DR. ALBERT ÁGOTA

ÜVEGES ANDRÁS JÓZSEF

ADATVÉDELEMRŐL ALAPFOKON

DR. ALBERT ÁGOTA LLM
ÜVEGES ANDRÁS JÓZSEF

Adatvédelemről alapfokon

Katonai Nemzetbiztonsági Szolgálat

Budapest, 2023.

Adatvédelemről alapfokon

Szerző:
dr. Albert Ágota LLM
Üveges András József őrnagy

Lektor:
dr. Báldy Péter

Olvasószerkesztő:
Farkasné dr. Nagy Katalin őrnagy

Tördelőszerkesztő: Nagy Gábor főhadnagy

A borító tervezője: Perényi Attila

Felelős kiadó: Tajti Norbert vezérőrnagy, főigazgató
Katonai Nemzetbiztonsági Szolgálat

A kiadó képviselője: Dr. Kenedli Tamás ezredes
Katonai Nemzetbiztonsági Szolgálat
Tudományos Tanács titkár

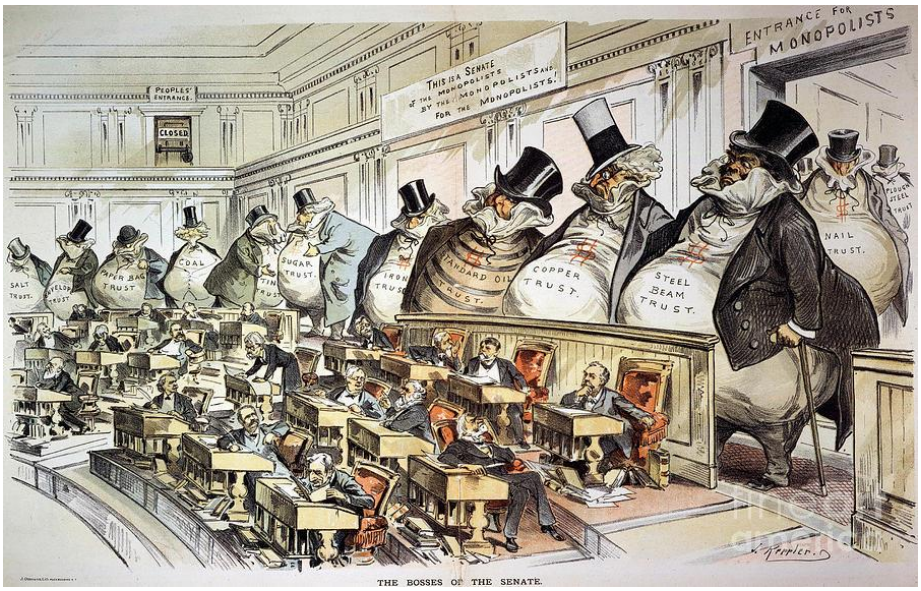
A kiadvány a Katonai Nemzetbiztonsági Szolgálat
Költségvetési Kutatóhely Tudományos Tanács támogatásával készült.

ISBN: 978-615-6128-14-0

Nyomdai kivitelező:
HM Zrínyi Geoinformációs és Toborzástámogató Közhasznú Nonprofit Kft.

ELŐSZÓ

Joseph Keppler 1889-es karikatúrájánál semmi sem ábrázolhatta volna szemléletesebben, hogy mely iparágak mágnásai tettek szert hatalomra a politikai vezetés felett. A mogorva mogulok hordóhasán a feliratok a stratégiai ipari ágazatokat[1] testesítik meg, azokat, amelyek Keppler korszakában a rohamos léptékű gazdasági fejlődésben nélkülözhetetlenek voltak. Napjainkban azonban a „hagyományos" monopóliumra törekvő ágazatok mellett új „nyersanyag" jelent meg, ez pedig az adat.



„Az adat az új olaj" halljuk mindenfelől, a jogalkotók és jogérvényesítő hatóságok-bíróságok pedig – a hatalmasra nőtt technológiai vállalatok lobbierejét ellensúlyozva – próbálják az újfajta piaci dominanciát megtörni. Azonban tudomásul kell vennünk, hogy az adat egyáltalán nem úgy viselkedik, mint az olaj, míg az olaj fizikailag megjelenik, az adat ugyan számszerűsíthető és minősíthető, de a fizikai világban nehezen értelmezhető, alapértelmezett funkciója nincs, miközben az áramlása úgy is megtörténhet, hogy akár mindvégig egyhelyben marad. Emellett az adatok feletti rendelkezés sem hasonlít az olaj feletti rendelkezéshez, ahogy az adatok előállítása sem – a nagyméretű adatállományok létrejöttéhez és növekedéséhez az adatokat szolgáltatók úgy járulnak hozzá, hogy gyakran nem rendelkeznek információval arról, hogy mindennapi tevékenységükkel kit gazdagítanak, kinek a piaci dominanciáját erősítik. Ráadásul az adatgyűjtés/előállítás új, innovatív technológiái intenzíven gyorsítják az eddig sem lassan haladó folyamatokat, a jogalkotók és jogérvényesítők pedig próbálják beérni az egyre inkább elszabaduló szereplőket. Ezen piaci szereplők tevékenységének volumene azonban emelkedő tendenciát mutat, és 2021-ben már

[1] réz, acél, olaj, szén

eljutottak odáig, hogy a legnagyobb cégek globális listáján[2] egyértelműen domináltak azok a vállalatok[3], amelyek szoros kapcsolatot ápolnak az adatokkal.

Hol tartunk ma, és mire számíthatunk a közeljövőben? Ha Keppler ma rajzolná meg híres karikatúráját a mindenre rálátó és a mindent felügyelő monopolistákkal, akkor a legnagyobb és a legdominánsabb az a piaci szereplő lenne, aki a legtöbb adatot birtokolja úgy, hogy azt bármikor hajlandó tisztességtelenül felhasználni, miközben a tevékenysége nemcsak az adatokat szolgáltató természetes személyek jogaira és szabadságaira, hanem a nemzetállamokra is hatalmas veszélyt jelentene.

Könyvünknek nem célja a napjainkban hatályos adatvédelmi jog teljeskörű ismertetése és arra sem vállalkoztunk, hogy az Európai Unió általános adatvédelmi rendeletét[4] cikkről cikkre megmagyarázzuk. A mi célunk az, hogy sok-sok példával közelebb hozzuk az adatvédelmet és olyan ismereteket adjunk át, amelyek egy „átlagos", az adatvédelemmel kényszerből találkozó olvasó is hasznosítani tud mindennapjai során.

A könyvünk írása során kérdőíves-interjús kutatást végeztünk annak érdekében, hogy a könyvünk valós adatokkal, a jelenlegi hazai gyakorlat és ismeretanyag tükrében készüljön. Kutatásunkhoz olyan kérdőív rendszert használtunk, amelynek része volt

- az alapismereteket mérő kérdőív (1/A) polgári és katonai személyek részére;
- a felhasználók (adatkezelők) ismereteit mérő kérdőív (1/B) polgári és katonai személyek részére;
- az adatvédelmi szakemberek részére készült kérdőív;
- a katonai vezetők részére készült kérdőív.

A téma érzékenysége, illetve komplexitása miatt volt szükség több kérdőív alkalmazására, mivel az alábbi elosztásban mértük a mutatókat:

- a megkérdezettek ismerik-e az adatvédelmi rendeletet, illetve az alapvető fogalmakat;
- ha ismerik, akkor milyen mélységben;
- a rendeletet mennyire találják használhatónak;
- a rendelet alkalmazandósága milyen módon hatott az adatvédelemre és kiberbiztonságra.

A kutatási eredményeinket a könyvünkben tematika szerint adjuk közre, kiegészítő információként.

[2] Jenna Ross: The Biggest Companies in the World in 2021, June 10, 2021, https://www.visualcapitalist.com/the-biggest-companies-in-the-world-in-2021/, *Data as of March 31, 2021.*

[3] Apple Inc, Microsoft Corp, Amazon.com Inc, Alphabet Inc, Facebook Inc, Tesla Inc

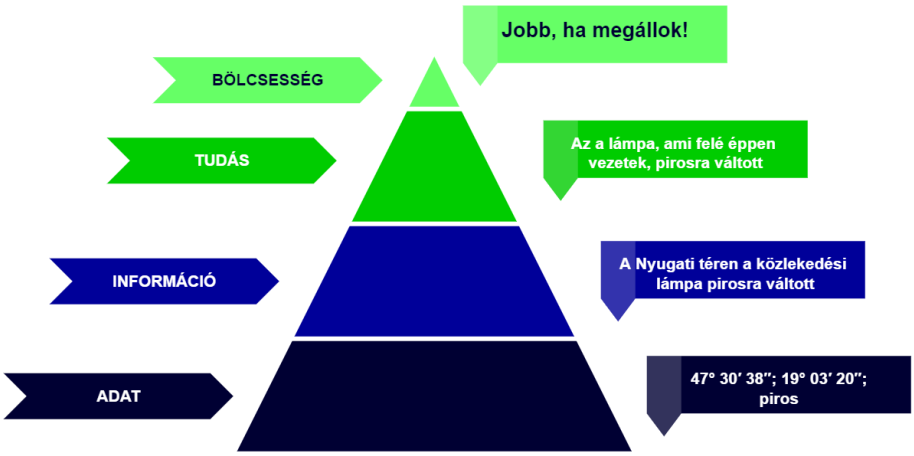
[4] az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet, továbbiakban: GDPR)

TARTALOMJEGYZÉK

MIÉRT VAN SZÜKSÉG ADATVÉDELEMRE, AVAGY MIT VÉD AZ ADATVÉDELEM?

Az első és legfontosabb, amit tudni kell az adatvédelemről az, hogy az adatvédelem nem az adatokat védi, hanem azoknak a jogait és szabadságát (az adataikon keresztül), akikre ezek az adatok vonatkoznak.

Álláspontunk szerint az adat olyan minta, amely rendelkezik kapcsolattal. Ismert az, hogy az adott digitális vagy fizikai minta kihez tartozik, minek a jellemzését adja, mit és hogyan ír le. Az adatoknak önmagukban nincs jelentésük, az adatok az értelmezéstől, azok feldolgozásának módjától, alkalmazásuktól nyernek értelmet. Ackoff az alábbiak alapján ábrázolta az adat, az információ, a tudás és a bölcsesség hierarchiáját:[5]



Az adat-bölcsesség piramisa

Elmondható, hogy napjainkban már a digitális adat a mérvadó (erre gondolunk, ha azt a szót halljuk, hogy „adat"), mivel „*az információk a kibertérben adatok formájában jelennek meg, áramlanak, érhetőek el. Az adatok által hordozott információk vonatkozhatnak a valós világ dolgaira, de leírhatnak a valóságban nem létező dolgokat is"*.[6]

[5] ACKOFF, R.L.: From data to wisdom. = Journal of Applied Systems Analysis, 16. köt. 1989. p. 3–9.
[6] MUNK S.: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései, HADITECHNIKA, DOI 10.17047/HADTUD.2018.28.1.113 121. o.

(1) Ez a rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg.

(2) Ez a rendelet a természetes személyek alapvető jogait és szabadságait és különösen a személyes adatok védelméhez való jogukat védi.

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), 1. cikk

Az adatvédelmet mint jogterületet több oldalról is megközelíthetjük különös tekintettel arra, hogy az érintettek jogainak és szabadságainak védelme nemcsak az Alaptörvényből[7] levezethető kiemelt állami feladat, hanem nemzetközi szintű kötelezettség is.

Hogyan védi meg az állam a polgárait?

- ✓ az idegen hatalmaktól például úgy, hogy a harmadik országokba történő adattovábbítások esetén speciális garanciákat követel meg,
- ✓ a piaci erőfölénnyel visszaélő multinacionális és hazai nagyvállalatokkal szemben (lásd például az óriás platformokat);
- ✓ a kiszolgáltatott élethelyzetekben fokozott védelmet biztosítva, például amikor munkavállalóként vagy az egészségügyben pácienskén szenvedik el az adataik kezelőinek tevékenységét;
- ✓ önmagától (az államtól magától), azaz a túlzott hatalom gyakorlásától, az „alattvalók" magánéletébe indokolatlan behatolástól is.

Az államnak sokféle eszköz áll rendelkezésére a védelem biztosítására, többek között

- ✓ jogalkotás keretében tagállami és uniós szinten alapvető, minden szereplőre egyformán érvényes és irányadó szabályokat fektethet le;
- ✓ kialakítja a jogérvényesítés rendjét (felügyeleti hatóságok és bíróságok működtetése, érdekvédelmi fórumok támogatása stb.);
- ✓ rászorítja az adatkezelőket, hogy a kezelésükben lévő személyes adatokat az adatvédelemre vonatkozó jogszabályoknak megfelelően kezeljék és az érintettek velük szemben képesek legyenek érvényesíteni az információs önrendelkezéssel kapcsolatos jogaikat;
- ✓ elősegíti az érintettek adatvédelmi tudatosságának megalapozását és növelését, például különféle adatvédelmi témákban kampányokat szervez.

Az államnak azonban nemcsak a személyes adatok védelmével kapcsolatban vannak feladatai, hanem az üzleti titkok, illetve a minősített adatok védelme területén is, ezen kívül az adatvédelmet (információs önrendelkezési jog védelmét) össze kell egyeztetni más jogokkal és szabadságokkal is. Ilyen szabadság például az Alaptörvényünkben garantált információszabadság, szólásszabadság, valamint a véleménynyilvánítás szabadsága is.

[7] https://net.jogtar.hu/jogszabaly?docid=a1100425.atv letöltve: 2022.04.22

TÖRTÉNELMI KITEKINTÉS, AVAGY HOGYAN JUTOTTUNK EL ODA, AHOL MA VAGYUNK?

Egyes vélemények szerint az adatvédelem a XX. század utolsó évtizedének találmánya, a célja pedig az adatkezelők munkájának támogatása/hátráltatása. A gyakorlatban azonban az adatvédelmi jog gyökerei nem pár évtizedre, hanem sokkal régebbre nyúlnak vissza, egészen az ókorba Aszklépiosz gyógyító papjaihoz, az aszklépidákhoz.

A titoktartás, mint szakmai kötelezettség

A történelmünk során mindig is voltak olyan „szakmák", amelyek képviselői a személyes adatokat (információkat) a titoktartás különleges szabályai szerint kezelték, ilyen például a hippokratészi eskü[8] vagy éppen a katolikus egyház gyónási titka[9] is. A későbbiek során ez a titoktartási kötelezettség más foglalkozásokra is kiterjedt, köztük a bankárokra, az ügyvédekre, a postai és távközlési dolgozókra, katonákra. Akik szakmai titoktartásra kötelezettek, azok tisztában voltak és vannak azzal, hogy azokat az információkat, amelyeket hivatalos (titoktartással terhes) minőségükben magánszemélyektől kaptak/kapnak, kötelesek bizalmasan kezelni.

A szakmai titoktartás nem öncélú tevékenység és nem is bizonyos „klubba tartozás" kelléke, hanem mind az egyént, mind a társadalmat szolgáló intézmény. Egyrészt a titkait és ezzel önmagát is kiszolgáltató egyén bízhat abban, hogy az a személy, akinek az információt átadta, bizalmasan kezeli azt, másrészt ez a bizalom a közjót szolgálja, hiszen a titoktartás hiánya például meggátolhatja az embereket abban, hogy segítséget merjenek kérni akkor, amikor arra lenne szükségük, például betegség kezelése vagy elterjedése érdekében.

Nemcsak a szakmai titoktartás, hanem egyéb helyzetekben is fontos a titkok megőrzése. A rendvédelmi és honvédelmi, valamint bűnüldözési és terrorelhárítási tevékenységek során, például a szélsőséges politikai vagy vallási csoportok terjeszkedésének megállítása, a korrupció, illetve az uniós jog megsértése elleni harc[10] érdekében a magánszemélyektől csak úgy várható el, hogy segítséget nyújtsanak

[8] A Hippokratész viselő eskü eredete feltehetőleg régebbre, Kr. e. VI. századra nyúlik vissza és a Kósz szigetén működő Aszklépiosz orvospapok fogadalmi szövege volt: *„(…) Amit kezelés közben látok vagy hallok (akár kezelésen kívül a társadalnú érintkezésben), nem fogom kifecsegni, hanem titokként megőrzöm."* (részlet a hippokratészi esküből, Magyar Katolikus Lexikon, http://lexikon.katolikus.hu/H/hippokrat%C3%A9szi%20esk%C3%BC.html)

[9] *„gyónási titok: a gyónást, a bűnbánat szentségét védő titoktartási fegyelem. – A szó szoros értelmében vett ~, a szentségi pecsét (sigillum sacramentale) a gyóntatót kötelezi, s azt jelenti, hogy tilos a gyónót szóval v. bármilyen más módon, bármi okból is, akár csak részben is elárulnia (983.k. 1.§)"* Magyar Katolikus Lexikon, http://lexikon.katolikus.hu/G/gy%C3%B3n%C3%A1si%20titok.html

[10] Például: Az Európai Parlament és a Tanács (EU) 2019/1937 irányelve (2019. október 23.) az uniós jog megsértését bejelentő személyek védelméről, (60) preambulumbekezés: *„Az uniós jog megsértésének hatékony felderítése és megelőzése megköveteli, hogy a visszaélést potenciálisan bejelentő személyek könnyen és teljes titoktartás mellett hozhassák a birtokukban lévő információt azon releváns illetékes hatóságok tudomására, amelyeknek módjában áll a probléma kivizsgálása és lehetőség szerint orvosolása."*

(például információforrásként), ha bízhatnak abban, hogy az ilyen tevékenységeket ellátó szervezetek megtartják a rájuk bízott titkokat (például nem fedik fel a forrás kilétét és a nyilvánosságra hozott információkkal sem teszik lehetővé a forrás személyének beazonosítását).

Példák a titoktartásra

- ✓ ***Banktitok*** *minden olyan, az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló tény, információ, megoldás vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik.*[11]
  *A pénzügyi intézmény ügyfelének tekintendő mindenki, aki (amely) a pénzügyi intézménytől pénzügyi szolgáltatást vesz igénybe. A banktitokra vonatkozó szabályokat alkalmazni kell arra a személyre is, aki szolgáltatás igénybevétele céljából lép kapcsolatba a pénzügyi intézménnyel, de a szolgáltatást nem veszi igénybe***.**
- ✓ ***Orvosi titok****: a gyógykezelés során az adatkezelő tudomására jutott egészségügyi és személyazonosító adat, továbbá a szükséges vagy folyamatban lévő, illetve befejezett gyógykezelésre vonatkozó, valamint a gyógykezeléssel kapcsolatban megismert egyéb adat.*[12]
- ✓ ***Ügyvédi titoknak*** *minősül minden olyan tény, információ és adat, amelyről az ügyvédi tevékenység gyakorlója e tevékenysége gyakorlása során szerzett tudomást.*[13]
- ✓ ***A kamarai tag könyvvizsgáló****, a könyvvizsgáló cég köteles a tevékenysége során tudomására jutott, a jogszabályi kötelezettségen alapuló könyvvizsgálói tevékenység ellátására irányuló megbízással összefüggő minősített adatot, hivatásbeli titkot és üzleti titkot megőrizni.*[14]
- ✓ *A* ***pedagógus****t, a nevelő és oktató munkát közvetlenül segítő alkalmazottat, továbbá azt, aki közreműködik a gyermek, tanuló felügyeletének az ellátásában, hivatásánál fogva harmadik személyekkel szemben titoktartási kötelezettség terheli a gyermekkel, a tanulóval és családjával kapcsolatos minden olyan tényt, adatot, információt illetően, amelyről a gyermekkel, tanulóval, szülővel való kapcsolattartás során szerzett tudomást.*[15]

[11] a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény 160.§
[12] az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény 3.§ d) pont
[13] az ügyvédi tevékenységről szóló 2017. évi LXXVIII. Törvény 9.§ (1) bekezdés
[14] a Magyar Könyvvizsgálói Kamaráról, a könyvvizsgálói tevékenységről, valamint a könyvvizsgálói közfelügyeletről szóló 2007. évi LXXV. Törvény 66.§ (1) bekezdés
[15] a nemzeti köznevelésről szóló 2011. évi CXC. törvény

Bár az adatvédelem gyökerei visszavezethetőek a titoktartásra, azt mindenképpen le kell szögezni, hogy az adatvédelem sokkal több (illetve más), mint „egyszerű" titoktartás. A titoktartási kötelezettségből ugyanis nem vezethető le az, hogy a betegek, az ügyfelek és egyéb személyek rendelkezzenek olyan, a személyes adataikkal kapcsolatos jogokkal, mint például a hozzáférés, a helyesbítés vagy a törlés joga, illetve a titoktartási szabályok azt sem határozzák meg, hogy hogyan, milyen feltételekkel lehet a személyes adatokat kezelni és mikor kell például azokat törölni/megsemmisíteni.

Az osztrák szövetségi közigazgatási bíróság gyakorlatából

A bíróság megállapította, hogy a könyvelők jogszabályban előírt titoktartási kötelezettsége nem zárja ki általában a GDPR 15. cikkének (4) bekezdése szerinti hozzáférési jogot, hanem azt eseti alapon kell értékelni.[16]

Előfordulnak azonban olyan esetek is, amikor egyetlen ügyben mind a szakmai titoksértés, mind az adatvédelmi jog megsértése megvalósul.

A román adatvédelmi hatóság (ANSPDCP[17]) gyakorlatából

Az ANSPDCP mintegy 1 000 eurós bírságot szabott ki a „Sabou, Burz & Cuc„ ügyvédi irodára, mert az egyik ügyfelének személyes adatait tartalmazó ügyiratot egy külső WhatsApp-csoportban más ügyvédekkel megosztott, megsértve ezzel a GDPR 6. cikkét és az 5. cikk (1) bekezdésének a), b), c) és f) pontját és (2) bekezdését.

Az egyik ügyfele panaszt nyújtott be a román adatvédelmi hatósághoz az ügyvédi iroda ellen, azt állítva, hogy a személyes adatait tartalmazó ügyirata a beleegyezése és előzetes tájékoztatása nélkül lett megosztva egy, az ügyvédi kamara jogászai által használt WhatsApp-csoportban.

A hatóság megállapította, hogy

- ✓ *az érintett személyes adatait (többek között a nevét, , lakcímét és a bíróság előtt folyamatban lévő ügyre vonatkozó információkat) tartalmazó ügyiratot valóban megosztották egy WhatsApp ügyvédi csoportban, amelynek 247 tagja volt.*
- ✓ *az adatkezelés érvényes jogalap nélkül történt*
- ✓ *az adatkezelés túlzott mértékű volt, mivel az összeegyeztethetetlen volt az adatgyűjtés eredeti céljával, és nem tartalmazta az adatok bizalmas kezelését biztosító szükséges technikai és szervezési intézkedéseket, megsértve a GDPR 6. cikkét és az 5. cikk (1) bekezdésének a), b), c) és f) pontját, valamint a (2) bekezdését.*

[16] Bundesverwaltungsgericht (BVwG) – W101 2218962-1 – https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20220728_W101_2218962_1_00/BVWGT_20220728_W101_2218962_1_00.pdf, utolsó letöltés 2022. 10. 21.

[17] The National Supervisory Authority for Personal Data Processing – Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Persona

A hatóság a bírság kiszabása mellett kötelezte az ügyvédi irodát, hogy

- ✓ *az ügyvédi kamara jogászai által használt WhatsApp csoport valamennyi tagját értesítse az e csoportban közzétett cím törlése érdekében,*
- ✓ *kérje a csoport adminisztrátorát, hogy törölje az ügyiratot,*
- ✓ *tanítsa meg az alkalmazottakat a GDPR rendelkezéseinek betartására és a jövőbeni jogellenes adatközlések elkerülésére.*[18]

„Privacy" – a magánélet tiszteletben tartása

Az adatvédelmi jog gyökerei között nemcsak a szakmai titoktartás, hanem a „privacy" intézménye is ott van. A „privacy" mint a magánélet fogalma magában foglalja egyrészt azt, hogy mi a magánélet és hogyan kell azt értékelni, másrészt a magánélethez való jogot, amely alapjogi védelmet élvez a mai modern társadalmakban.

Mérföldkövek a modern „privacy" kialakulásában

Az ókori görögök a „saját„ (idion) magányban eltöltött életet „idiótának„ tekintették. Hasonlóképpen gondolkodtak a rómaiak is, akik a magánéletet csupán ideiglenes menedéknek tekintették a „res publica"[19] élete elől. A magánélet magánjellege számukra azt az állapotot jelentette, hogy amikor az ember valamitől, sőt az ember legmagasabb és legemberibb képességeitől is meg van fosztva. Úgy vélték, az az ember, aki csak magánéletet él, aki a rabszolgához hasonlóan nem léphet be a közéletbe, vagy a barbárhoz hasonlóan úgy dönt, hogy nem hoz létre egy ilyen életteret, nem teljesen ember. Csak a kései Római Birodalomban lehet felismerni a magánélet, mint az intimitás zónája elismerésének kezdeti szakaszait.

A köz- és magánszféra modernkori elhatárolása egyrészt a 16. és 17. században a nemzetállam és a szuverenitás elméleteinek kialakulásának köszönhető, másrészt megjelent az igény az állam beavatkozásától mentes privát szférára is.

Történelmi kitekintés – főbb események, amelyek a mai közvélekedéshez vezettek

- ✓ ***1361 Anglia, békebírói törvény*** *– büntethetővé teszi a lehallgatást és a kukkolást.*
- ✓ ***1604 Semayne-eset***
  - *„a ház mindenki számára olyan, mint a vára és erődje„ (William Pitt)*
  - *„A legszegényebb ember is dacolhat a házában a nagyvilág minden erejével. Lehet, hogy törékeny – a teteje megremeghet – a szél átfújhat rajta – a vihar bejuthat – az eső bejuthat – de Anglia királya nem juthat be." (William Pitt, Chatham első grófja)*[20]

[18] Amendă pentru încălcarea RGPD, https://www.dataprotection.ro/?page=Comunicat_Presa_22_02_2022_2&lang=ro, utolsó letöltés 2022. 08. 20.

[19] köztársaság

[20] The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail – its roof may shake – the wind may blow through it – the storm may enter – the rain may enter – but the King of England cannot enter. – William Pitt, 1st Earl of Chatham

- ✓ ***1879 – Thomas Cooley amerikai bíró*** *a személyes biztonság kapcsán kiemeli a „háborítatlansághoz való jogot”*
- ✓ ***1890 – Samuel Warren és Louis Brandeis cikke az egyének magánélethez való jogáról****, amelyet úgy neveztek el: „háborítatlansághoz való jog”. Ez a cikk inspirálta a XX. században a magánélethez fűződő jogsértések elismerését („egyedül hagyatáshoz való jog”)*[21]

A magánélet Alan F. Westin (1967) szerint

„A magánélet az egyének, csoportok vagy intézmények azon igénye, hogy maguk határozzák meg, mikor, hogyan és milyen mértékben közölnek róluk információkat másokkal. Az egyénnek a társadalmi részvételhez való viszonyát tekintve a magánélet az egyén önkéntes és átmeneti visszavonulása az általános társadalomtól fizikai vagy pszichológiai eszközökkel, akár magányos vagy kiscsoportos intimitásban, akár nagyobb csoportok tagjaként a névtelenség vagy a tartózkodás („elvonulás”) állapotában. Az egyén magánélet iránti vágya sohasem abszolút, mivel a társadalomban való részvétel ugyanolyan erős vágy. Így minden egyén folyamatosan egy személyes alkalmazkodási folyamatban van, amelyben egyensúlyt teremt a magánélet iránti vágya és az önmagát másokkal való közlésre és kommunikációra irányuló vágya között, a környezeti feltételek és a társadalom által meghatározott társadalmi normák fényében, amelyben él. Az egyén mindezt a mások kíváncsiságából és a megfigyelési folyamatokból eredő nyomással szemben teszi, amelyet minden társadalom a társadalmi normák érvényesítése érdekében állít fel. (…)

„A magánélet első állapota a magány; itt az egyén elkülönül a csoporttól, és megszabadul más személyek megfigyelésétől. (…)

A magánélet második állapotában, az intimitásban az egyén egy olyan kis egység részeként cselekszik, amely igényli és gyakorolhatja a társas elzárkózást, hogy két vagy több egyén között szoros, nyugodt és őszinte kapcsolatot valósíthasson meg. Az intimitás tipikus egységei a férj és feleség, a család, egy baráti kör vagy egy munkahelyi csoport. (…)

A magánélet harmadik állapota, az anonimitás, akkor következik be, amikor az egyén nyilvános helyen tartózkodik vagy nyilvános cselekményeket hajt végre, de mégis keresi és meg is találja az azonosítás és a megfigyelés alóli mentességet. Lehet, hogy metróban utazik, egy meccsen vesz részt, vagy az utcán sétál; emberek között van, és tudja, hogy megfigyelik; de hacsak nem egy jól ismert híresség, nem várja el, hogy személyesen azonosítsák, és ne tartsák be a viselkedés és a szerep teljes szabályait, amelyek akkor működnének, ha a megfigyelők ismernék őt. Ebben az állapotban az egyén képes beleolvadni a „szituációs tájba". Az a tudat vagy félelem, hogy az ember nyilvános helyeken szisztematikus megfigyelés alatt áll, lerombolja a nyugalom és a szabadság érzését, amelyet az emberek a nyílt terekben és a nyilvános színtereken keresnek. (…)

[21] Samuel Warren & Louis Brandeis, A magánszférához való jog, Harvard Law Review 193 (1890)

Az anonimitásnak még egy másik fajtája a gondolatok névtelenül történő közzététele. Itt az egyén valamilyen eszmét nyilvánosan akar bemutatni a közösségnek vagy annak egy részének, de nem akarja, hogy azonnal általánosan azonosítják a szerzőt – különösen nem a hatóságok, amelyek kénytelenek lehetnek intézkedni, ha „ismerik" az elkövetőt.

Az anonim cselekvés minden ilyen típusának lényege az egyének vágya a „nyilvános magánéletre".

A tartózkodás („elvonulás"), a magánélet negyedik és legkifinomultabb állapota, a nem kívánt behatolással szembeni pszichológiai gát megteremtése; ez akkor következik be, amikor az egyénnek a saját magáról szóló kommunikáció korlátozására irányuló igényét az őt körülvevők készséges diszkréciója védi. Életünk nagy részét nem magányban vagy anonimitásban töltjük, hanem intim helyzetekben és csoportokban, ahol mások ismernek bennünket. Még a legintimebb kapcsolatokban is az önmagunkról másokkal való kommunikációnk mindig hiányos, és azon az igényen alapul, hogy önmagunk bizonyos részeit vagy túl személyesnek és szentnek, vagy túl szégyenletesnek és profánnak tartjuk ahhoz, hogy kifejezzük." [22]

A magánélt Roger Clarke magánélet szerint

„A magánszféra egy 'személyes tér' fenntartásával az egyének érdekét szolgálja, mely így mentes más emberek és szervezetek beavatkozásától."[23]

A magánélet Raymond Wacks szerint

„A legáltalánosabb szinten a magánélet eszméje azt a vágyat foglalja magában, hogy békén hagyjanak, hogy szabadon önmagunk lehessünk – gátlások és mások kíváncsiskodása által nem korlátozva. Ez túlmutat a kíváncsiskodáson és a kéretlen nyilvánosságon, és kiterjed a „térbe" való behatolásra, amelyre szükségünk van ahhoz, hogy intim, személyes döntéseket hozzunk az állam beavatkozása nélkül. (…)

(…) a privát szféra a kreativitás, a pszichológiai jólét, a szeretetre való képességünk, a társas kapcsolatok kialakításának, a bizalom, az intimitás és a barátság előmozdításának szféráját is kijelöli."[24]

A magánélet („privacy") védelme

Hazánkban mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát, kapcsolattartását (együttesen: magánélethez való jog) tiszteletben tartsák.

[22] Allan F. Westin: Privacy and Freedom, The Association of the Bar of the City of New York, 1967. fordította: dr. Albert Ágota
[23] Koops, B.-J. et al. (2016, 'A Typology of Privacy' (2017) 38 University of Pennsylvania Journal of International Law 483), https://scholarship.law.upenn.edu/jil/vol38/iss2/4/. fordította: dr. Albert Ágota
[24] Raymond Wacks: Privacy A Very Short Introduction, Oxford University Press, 2010. fordította: dr. Albert Ágota

„A magánélet, a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához fűződő jog együttesen az ember veleszületett méltóságából ered, amely mindenkit megillet. A magánélethez való jog az emberi lét és önazonosság kiteljesedéséhez elengedhetetlen, hiszen az az emberi személyiség érinthetetlen tartományát határolja körül.

Magánélethez való jog minden embert megillet, és azt a közügyek szabad vitatása során is tiszteletben kell tartani, erre figyelemmel a közéleti ügyek szabad megvitatása sem járhat a magán- és családi élet, valamint az otthon sérelmével. Az Alaptörvénnyel összhangban a közéleti szereplőt is megilleti a magánélet védelme és az otthon nyugalma. (…)

(…) a magánélet védelme kiterjed a fizikai és az interneten megvalósuló zaklatásra egyaránt. Az egyén méltóságát és magánélethez fűződő jogát biztosítani kell a közösségi médiatérben is."[25]

A **magánélethez való jog** a személyiségünk szabad kibontakoztatásához való jog része, amelynek értelmében az egyént szabadság illeti meg élete felelősségteljes, önálló alakítására, család, otthon, valamint emberi kapcsolatok létesítésére és megóvására. A magánszféra fokozott védelmét szolgáló alapvető szabályokat törvény állapítja meg és e jogunk csak:

- ✓ más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében,
- ✓ a feltétlenül szükséges mértékben,
- ✓ az elérni kívánt céllal arányosan,
- ✓ a magánélethez való jog lényeges tartalmának és az emberi méltóságnak a tiszteletben tartásával korlátozható.

A magánélethez való jogunk lényege, hogy azt – külön törvényben meghatározott kivételekkel – akaratunk ellenére mások ne sérthessék meg, illetve a magánélethez való jog gyakorlása során mi is kötelesek vagyunk mások jogait tiszteletben tartani.

A magánélethez való jog egyes kiemelt területei[26]és ezen területekkel kapcsolatos kockázati tényezők:

- ✓ **a magánélet tiszteletben tartásához való jog** célja, különösen a névviseléshez való jog, a személyes adatok, a magántitok, a képmás és hangfelvétel, a becsület és a jó hírnév védelme. A magánélet tiszteletben tartásához való jogunk megsértését jelentheti az általunk különösen a magánéletünkkel kapcsolatban megőrizni kívánt személyes adatunkkal, titkunkkal, képmásunkkal, hangfelvételünkkel való visszaélés, vagy a becsületünk és a jó hírnevünk megsértése.
    - A fentiekben említett adatok forrásai és eszközei lehetnek számos digitális térben elkövetett visszaélésnek. A hekkercsoportok tevékenységük során (illegális anyagi haszonszerzés céljából) előszeretettel tulajdonítják el és használják fel ezeket az adatokat.

[25] 2018. évi LIII. törvény a magánélet védelméről, preambulum
[26] Részletesen lásd: 2018. évi LIII. törvény a magánélet védelméről

Egyik leggyakoribb tevékenységük a személyiséglopás, közismertebb nevén az „identity theft[27]", amelynek a szakirodalomban nincs egységesen elfogadott definíciója, identitáslopásnak minősül például más személyes adatainak csalási szándékkal történő használata.

- Szigorúan tilos a háztartási céllal üzemeltett kamerarendszerrel a szomszédot megfigyelni és a rögzített felvételeket pedig nyilvánosságra hozni.

A belga adatvédelmi hatóság (APD/GBA[28]) gyakorlatából:

A hatóság megbüntette azt a személyt, aki olyan videókat tett közzé a YouTube-on, amelyeken fatüzelést használó helyi lakosok kandallója volt ábrázolva a szóban forgó ház lakójának nevével és címével együtt.
A hatóság véleménye szerint a kandallóról készült fénykép/film közzététele önmagában nem jár olyan személyes adatok feldolgozásával, amelyre a magánélet védelmére vonatkozó jogszabályok alkalmazandók lennének, azonban amint a filmet az érintett személy nevével és címével együtt teszik közzé, már személyes adatok kezeléséről beszélünk.

A hatóság egyértelművé tette, hogy bár a személyes adat fogalma tágan értelmezendő, és magában foglal minden olyan adatot, amely alapján egy természetes személy azonosítható, egy olyan videofelvétel, amelyen csupán egy kémény (füstkibocsátás) látható anélkül, hogy egy személy bármilyen módon azonosítható lenne, nem minősül személyes adatnak. A kandallóról készült videofelvétel viszont személyes adattá válik, amint a természetes személy azonosítása megemlítésre kerül.[29]

- ✓ **a családi élet tiszteletben tartásához való jog** alapján mindenkinek joga van arra, hogy családi életét, mint a magánélet közegét fokozott védelem illesse meg. A családi élet tiszteletben tartásához való jog az egyént és a családtagját együttesen is megilleti. A családi életünk tiszteletben tartásához való jogunk sérelmét jelenti különösen annak jogosulatlan megsértése, zavarása vagy abba való jogosulatlan beavatkozás. Ez igaz arra is, hogy ma már ehhez a szférához tartoznak az alábbi elemek is:
  - otthonunkban működő PAN rendszer[30]

[27] identitätsdiebstahl, vagy identity fraud
[28] Belgian Data Protection Authority (APD, Autorité de protection des données in French or GBA, Gegevensbeschermingsautoriteit in Dutch)
[29] APD/GBA – 71/2020, https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-71-2020.pdf utolsó letöltés: 2022. 07. 08.
[30] az otthonunkban működő PAN rendszer ("Personal Area Network", személyes hálózati terület) egy olyan hálózati rendszert, amely lehetővé teszi a különböző eszközök (például számítógépek, okostelefonok, nyomtatók, hangszórók stb.) közvetlen kommunikációját egymással az otthonunkban. Általában vezeték nélküli technológiákon alapul, például Wi-Fi vagy Bluetooth, és lehetővé teszi az eszközök közötti adatátvitelt, megosztást vagy együttműködést.

- személyes adatainkat tároló otthoni NAS[31]
- a lakásunkban működő IoT eszközök alkotta rendszer, amely számos személyes adatot kezel.

Ezeknek az eszközöknek és hálózatoknak az adatvédelme kiemelt fontosságú, mivel ezen eszközökön személyes adataink nagy része megtalálható (az ilyen otthoni rendszerek tárolhatják elektronikus formában számos személyes adatunkat, például mikor vagyunk otthon, mit nézünk a televíziónkon/számítógépünkön, kinek telefonáltunk és mikor nyitottuk ki utoljára az okos hűtőnket). Kiemelt kockázati tényező az is, hogy ezek az adatok egy helyen, koncentráltan fordulnak elő, és ezek között nagy mennyiségben lehet kép-, hang- és videótartalom is.

- ✓ **az otthon tiszteletben tartásához való jog** alapján az állam jogi védelemben részesíti az otthon nyugalmát. Az otthon nyugalma biztosítja a magán- és családi életünk kibontakozását, továbbá a magánszféránk szabad és teljes megélését. Ennek tiszteletben tartása érdekében az otthonunkat, mint magánéletünk, családi életünk színterét fokozott védelem illeti meg. Az otthon tiszteletben tartásához való jogunk sérelmét jelenti különösen az otthonunkba való jogosulatlan behatolás, vagy egyéb sértő, zavaró, zaklató módon történő jogosulatlan beavatkozás.

Ilyen beavatkozás lehet egy esetleges kibertámadás is, amelynek célja, hogy illetéktelen személyek hozzáférjenek személyes adatainkhoz, amelyek lehetnek például:

- NAS vagy otthoni informatikai hálózaton tárolt személyes adatok;
- személyes IoT[32] eszközökön tárolt érzékeny adatok;
- ház automatizálási rendszerek szenzor adatai.

- ✓ **a kapcsolattartás tiszteletben tartásához való jog** alapján a magánközlések, az élőszóban, telefonbeszélgetés, hagyományos vagy elektronikus levelezés során vagy egyéb kommunikációs eszközök segítségével átadott magánjellegű információk ezen jog védelme alá tartoznak, valamint az egyént fokozott védelem illeti meg mind a zaklatás hagyományos, mind valamennyi internetes formájával szemben is. A kapcsolattartás tiszteletben tartásához fűződő jogunk kiterjed a magánkommunikációnk bármely módon történő megfigyelésével szembeni védelemre is.

[31] az otthoni NAS („Network Attached Storage", hálózati csatolt tárolás) olyan tárolóeszköz, amelyet az otthoni hálózatban használunk a személyes adatok, például fájlok, képek, videók vagy dokumentumok biztonságos tárolására. A NAS rendszer általában egy különálló eszköz vagy számítógép, amelyben több merevlemez található, és amelyhez hálózati kapcsolaton keresztül csatlakozhatnak más eszközök, például számítógépek, okostelefonok vagy táblagépek.
[32] a személyes IoT eszközök („Internet of things", tárgyak internete) olyan intelligens eszközök, amelyeket egyénileg használunk mindennapi életünk során. Ezek az eszközök lehetnek viselhető eszközök (pl. okosórák, fitnesz nyomonkövetők), okostelefonok, okos otthoni eszközök (pl. okos világítás, okos zárak, okos termosztátok) és más olyan eszközök, amelyek kapcsolódnak az internethez és adatokat küldhetnek vagy fogadhatnak.

Az olasz adatvédelmi hatóság (Garante) gyakorlatából:

A hatóság 20 ezer eurós bírságot szabott ki a Gaypa s.r.l.-re azért, mert a vállalat saját érdekeinek védelme érdekében jogszerűtlenül ellenőrizte alkalmazottja munkahelyi e-mail fiókját. A panasz tárgya az volt, hogy a vállalat a munkavállalója elbocsátása után hozzáfért annak munkahelyi e-mail fiókjához, és az ellenőrzött e-mailek egy részét felhasználta egy ellene bizalmas információk eltulajdonítása miatt indított eljárás alátámasztására. A vállalat a bejelentett megőrzési időszak lejárta után és a volt munkavállalónak az adatkezelésről történő értesítése nélkül jutott hozzá ezekhez az adatokhoz.
A Gaypa s.r.l. azt állította, hogy az információkat kizárólag jogos érdekeinek bíróság előtti védelmére használta fel, illetve rendelkezik belső szabályzatokkal az érintettek személyes adatok kezeléséről történő tájékoztatására. [33]

Amennyiben magánéletünkhöz való jogunkban megsértenek, a jogsértés ténye alapján – az elévülési időn belül – az eset körülményeihez képest a Polgári Törvénykönyv szabályai szerint követelhetjük

a) a jogsértés megtörténtének bírósági megállapítását,
b) a jogsértés abbahagyását és a jogsértő eltiltását a további jogsértéstől,
c) azt, hogy a jogsértő adjon megfelelő elégtételt, és ennek biztosítson saját költségén megfelelő nyilvánosságot,
d) a sérelmes helyzet megszüntetését, a jogsértést megelőző állapot helyreállítását és a jogsértéssel előállított dolog megsemmisítését vagy jogsértő mivoltától való megfosztását,
e) azt, hogy a jogsértő vagy jogutódja a jogsértéssel elért vagyoni előnyt engedje át a javunkra a jogalap nélküli gazdagodás szabályai szerint.

Amennyiben a magánéletünkhöz való jogunkban megsértenek,

- ✓ a Polgári Törvénykönyv szabályai szerint sérelemdíjat követelhetünk a minket ért nem vagyoni sérelemért, illetve
- ✓ ha a magánéletünkhöz való jogunk megsértéséből eredően kárt szenvedünk, a fenti a)-e) pontokon túlmenően – a Polgári Törvénykönyvnek a jogellenesen okozott károkért való felelősség szabályai szerint – követelhetjük a jogsértőtől kárunk megtérítését, valamint külön törvényben meghatározottak szerint egyéb igényeinket is érvényesíthetjük.

[33] Ordinanza ingiunzione nei confronti di Gaypa s.r.l. – 29 ottobre 2020 [9518890], https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9518890, utolsó letöltés: 2022. 07. 08.

Európa – Európa Tanács[34] és a magánélet tiszteletben tartásához való jog

A magánélethez (a magánélet tiszteletben tartásához) való jog, mint az alapvető védett emberi jogok egyike jelenik meg az **Emberi Jogok Egyetemes Nyilatkozatá**ban (ENSZ, 1948). Az Európa Tanács szintén elismerte ezt a jogot az 1950-ben elfogadott **Emberi jogok európai egyezményé**ben (EJEE), mely 1953-ban lépett hatályba és jogilag kötelező érvényű a részes felekre nézve.

Az EJEE 8. cikke alapján

„1. Mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák.
2. E jog gyakorlásába a hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban a nemzetbiztonság, a közbiztonság vagy az ország gazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges."[35]

A 8.cikk

- ✓ a személyes adatok kezelésével szembeni védelemhez való jogot nem önálló jogként, hanem a magán- és családi élet, a lakás és a kapcsolattartás tiszteletben tartásához való jog részeként határozza meg;
- ✓ nemcsak arra kötelezi az egyezményben részes államokat, hogy tartózkodjanak az olyan magatartástól, amely sértheti ezt a jogot, hanem azt is tartalmazza, hogy az államokat – bizonyos körülmények fennállása esetén – pozitív kötelezettség terheli atekintetben, hogy ténylegesen is biztosítsák a magán- és családi élet tényleges tiszteletben tartását;
- ✓ elsődlegesen a hatalomnak az egyén magánéletébe való szükségtelen beavatkozásával szemben nyújt védelmet például a kommunikáció állami szervek általi lehallgatása vagy a szexuális magánéletet kriminalizálása esetén.

Az egyezményben foglaltak érvényesítése érdekében 1959-ben Strasbourgban létrejött az Emberi Jogok Európai Bírósága (EJEB).

Az Emberi Jogok Európai Bíróságának gyakorlatából *(Copland kontra Egyesült Királyság[36])*

C-t egy továbbképző főiskolán való munkaviszonya alatt az igazgatóhelyettes kezdeményezésére több hónapon keresztül megfigyelték, így a telefonhívásait, az e-mail- és internethasználatát is. A főiskola szerint a megfigyelésre annak

[34] Az Európa Tanács regionális nemzetközi szervezet, székhelye Strasbourg, jelenleg 47 tagja van, A szervezethez bármely olyan európai állam csatlakozhat, amely elfogadja a jogállamiság intézményét és garantálja állampolgárai számára az alapvető szabadság és emberi jogokat.
[35] https://www.echr.coe.int/documents/convention_hun.pdf
[36] Hivatkozás: 62617/00, az ítélethozatal időpontja: 2007 április 3., https://www.5rb.com/wp-content/uploads/2013/10/Copland-v-UK-ECHR-3-Apr-2007.pdf, utolsó letöltés: 2022. 07. 08.

megállapítása miatt került sor, hogy C. nem használja-e túlzott mértékben a főiskola eszközeit személyes célokra. A telefonhasználat ellenőrzése a főiskola telefonszámláinak elemzéséből állt, amely a hívott telefonszámokat, a hívások időpontját, hosszát és költségét mutatta. Az internethasználat nyomon követése a meglátogatott weboldalak, a látogatások időpontjának és időtartamának elemzéséből állt. Az e-mailek nyomon követése az e-mail címek, valamint az e-mailek küldésének dátumai és időpontjai elemzésének formájában történt. A főiskolán nem volt hatályos szabályzat az alkalmazottak telefon-, e-mail- vagy internethasználatának nyomon követésére vonatkozóan.

A bíróság megállapította a 8. cikk megsértését:
(1) A 8. cikk értelmében a telefonhívások, az e-mailek és a személyes internethasználat az üzleti helyiségekben prima facie[37] „magánéletnek" és „levelezésnek„ minősül. Mivel C-t nem figyelmeztették a megfigyelésre, észszerű elvárása volt a magánélethez való joggal kapcsolatban. C. telefonbeszélgetéseire, valamint e-mail- és internethasználatára vonatkozó személyes adatoknak a C tudta nélkül történő gyűjtése és tárolása a 8. cikk értelmében a magánélet és a magánlevelezés tiszteletben tartásához való jogába való beavatkozásnak minősült.
(2) A főiskolának nem volt hatásköre arra, hogy „mindent megtegyen, ami szükséges vagy célszerű az oktatás biztosítása érdekében. Sem az általános nemzeti jogban, sem a főiskola irányadó dokumentumaiban nem léteztek olyan rendelkezések, amelyek szabályozták volna, hogy a munkáltató milyen körülmények között ellenőrizheti a munkavállaló telefon-, e-mail- és internethasználatát. Ennek megfelelően a beavatkozás nem volt „a joggal összhangban".

Ezen szabályozásnak hiányossága, hogy az EJEE-ből levezethetően az egyéneket nem illette meg kereseti jog más egyénekkel szemben és csak az állammal szemben tudtak fellépni arra hivatkozva, hogy az nem védi meg őket a nemzeti jog segítségével. A fenti, Copland kontra Egyesült Királyság perben az EJEB úgy ítélte meg, hogy a megfigyelés sérti a 8. cikket, ezért kötelezte az államot, hogy fizessen C-nek 3 000 eurót a nem vagyoni kárai (stressz, szorongás, rossz hangulat és alvásképtelenség), valamint 6 000 eurót a költségei és kiadásai megtérítése címén.

Összességében elmondható tehát, hogy sem a titoktartásra vonatkozó szabályozások, sem a magánélet tiszteletben tartásával kapcsolatos jogok és garanciák nem tudták megvédeni az egyéneket azzal szemben, hogy a személyes adataik visszaélésszerű gyűjtésére és felhasználására sor kerülhessen, így a társadalmi fejlődés óhatatlanul magával hozta egy új szabályrendszer kialakításának igényét.

Európában a válasz erre a problémára a személyes adatok védelméhez való jog (információs önrendelkezési jog) mint önálló jog elismerése volt. Ez azonban nem azt jelenti, hogy ez az új jog egy teljesen új, elkülönült jog – ezen „új" jogot mindig a többi, „hagyományos" joghoz szorosan kapcsolódva kell vizsgálnunk és értelmeznünk.

[37] első látásra, azonnal felismerhető módon (lat.)

Az adatvédelmi / információs önrendelkezési jog kialakulása

Az első számítógépeket a második világháború alatt építették katonai célokra és csak az 1960-as évekre jutott el odáig a fejlődés, hogy ezen eszközöket személyes adatok automatizált feldolgozására is használják. Az első számítógépek – magas áruk és helyigényük miatt – először a kormányzati hivataloknál és nagyvállalatoknál álltak hadrendbe, jellemzően kifizetések menedzselése, kórházi betegek nyilvántartása, népszámlálás és statisztikák készítésének céljára, valamint rendőrségi adatok tárolása érdekében.

A ’60-as évek végén és a ’70-es évek elején ez a számítástechnikai (adatgyűjtési és adatkezelési) fejlődés Európa-szerte számtalan vitát generált. Németországban Hessen tartományban például a rendőrségi akták léte, míg Norvégiában, Svédországban és Franciaországban a második világháborús náci megszállók lakossági és egyéb közhiteles nyilvántartásokkal való visszaéléseinek emléke idézett elő nagyfokú bizalmatlanságot.

A ’70-es évek végén és a ’80-as évek elején a kételyek és viták szélesebb körben is elterjedtek:

- ✓ Franciaországban 1974-ben kiszivárgott, hogy a kormány olyan nemzeti adatbázist kíván létrehozni, amelyben minden francia állampolgár és lakos benne lesz, ráadásul mindenki egyedi azonosító számot kap és napvilágra került az addig vitatott rendőrségi akták létezése is,
- ✓ Németországban az 1983-ra tervezett nemzeti népszámlálás váltott ki széles körű ellenállást.

Ezen viták központi témái:

- ✓ az új technológiák alkalmazása miatt megnő a magánélet sérülésének kockázata,
- ✓ aggódás a hibás adatok lehetséges következményei miatt
- ✓ a különböző célokra gyűjtött adatok központosítása és/vagy az egyedi azonosító segítségével az adatbázisok összekapcsolása révén önkényuralom kiépítésére is lehetőség nyílik.

Az első adatvédelmi törvény a németországi Hessen tartományban 1970-ben elfogadott törvény volt[38], melynek címe[39] „ragadt rá” az új jogágra mint elnevezés annak ellenére, hogy a kifejezés valójában félrevezető, mivel a törvény nem az adatokat, hanem azon személyek jogait védte, akiknek az adatait kezelték. Az „adatvédelem” kifejezés ennek ellenére széleskörben elterjedt, az 1995-ös EK

[38] HessischesDatenschutzgesetz (HDSG) 1970, hatályos 1970. október 13-től, http://starweb.hessen.de/cache/GVBL/1970/00041.pdf
[39] „Datenschutzgesetz”; Datenschutz – „adatvédelem”

adatvédelmi irányelv[40] és a 2016-os uniós általános adatvédelmi rendelet (GDPR)[41] is ezt használja.
A jogág fejlődésének újabb nagy mérföldköve az volt, amikor a német Szövetségi Alkotmánybíróság egy 1983-as ítéletében megerősítette az információs önrendelkezési jogot[42].

„1. A modern adatkezelés körülményei között az egyén védelmét személyes adatainak korlátlan gyűjtése, tárolása, felhasználása és nyilvánosságra hozatala ellen a GG[43] (...) szerinti általános személyiségi jog foglalja magában (...). Ebben a tekintetben az ***alapvető jog garantálja az egyén azon jogát, hogy maga dönthessen személyes adatainak nyilvánosságra hozataláról és felhasználásáról.***

2. ***Az „információs önrendelkezési jog" korlátozása csak nyomós közérdekből megengedett****. Ez alkotmányos jogalapot igényel, amelynek meg kell felelnie a normák egyértelműsége alkotmányos követelményének. A jogalkotónak a szabályozásában az arányosság elvét is tiszteletben kell tartania. Olyan szervezeti és eljárási óvintézkedéseket is meg kell tennie, amelyek ellensúlyozzák a személyiségi jog megsértésének veszélyét."*[44]

A bíróság tehát úgy ítélte meg, hogy az információs önrendelkezési jog a német alkotmány által védett, a személyiség tiszteletben tartásához fűződő alapvető jogból ered.

„Az egyéni önrendelkezés *(...)* ***feltételezi*** *– még a modern információfeldolgozási technológiák körülményei között is -,* ***hogy az egyén szabadon dönthet a meghozandó vagy mellőzendő cselekedetekről, beleértve annak lehetőségét, hogy ténylegesen e döntésnek megfelelően viselkedjen. Az a személy, aki nem képes kellő biztonsággal előre látni, hogy a társadalmi környezetének egyes területein milyen őt érintő információk ismertek, és aki nem képes bizonyos mértékig megbecsülni a lehetséges kommunikációs partnerek ismereteit, jelentősen korlátozható abban, hogy saját önrendelkezése alapján tervezzen vagy döntsön.***

Az információs önrendelkezési jog nem lenne összeegyeztethető egy olyan társadalmi renddel és az azt lehetővé tevő jogrenddel, amelyben a polgárok már nem tudhatják, hogy ki, mit, mikor és milyen alkalommal tud róluk. *Azok, akik bizonytalanok abban, hogy a deviáns viselkedést bármikor megjegyzik-e, és*

[40] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (továbbiakban: adatvédelmi irányelv)
[41] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatokszabad áramlásáról, valamint a 95/46/EK hatályon kívül helyezéséről (általános adatvédelmi rendelet), továbbiakban: GDPR
[42] Volkszählungsurteil, BVerfGE Bd. 65, S. 1skk.
[43] GrundGesetz, Németország Alaptörvénye
[44] Volkszählungsurteil, BVerfGE Bd. 65, S. 1skk. Leitsätze zum Urteil des Ersten Senats vom 15. Dezember 1983, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. fordította: dr. Albert Ágota

tartósan tárolják-e, felhasználják-e vagy információként továbbítják-e, igyekeznek nem felhívni magukra a figyelmet az ilyen viselkedéssel. Azok, akik arra számítanak, hogy például egy gyűlésen vagy egy polgári kezdeményezésben való részvételt a hatóságok nyilvántartásba vesznek, és hogy ennek következtében ez kockázatot jelenthet számukra, esetleg tartózkodni fognak a megfelelő alapvető jogaik gyakorlásától (...). Ez nemcsak az egyén fejlődési esélyeit rontaná, hanem a közjót is, hiszen ***az önrendelkezés egy szabad demokratikus közösség elemi működési feltétele, amely a polgárok cselekvőképességén és részvételi képességén alapul.***"[45]

Az évek során az adatvédelem/információs önrendelkezési jog immár nem a magánélet tiszteletben tartásához való jog része volt, hanem önálló joggá vált, azonban a magánélet tiszteletben tartásához való jog[46] és a személyes adatok védelméhez való jog[47] mind a mai napig szorosan kapcsolódnak egymáshoz. Mindkét jog célja az egyén önállóságának és emberi méltóságának megvédése olyan személyes (privát) szféra biztosításával, amelyben szabadon kiteljesedhet, gondolkodhat és véleményt alkothat – éppen ezért elmondható, hogy a többi alapvető szabadság, így a véleménynyilvánítás[48] és a békés gyülekezés[49], valamint a gondolat, a lelkiismeret és a vallás szabadsága[50] elengedhetetlen előfeltételét képezik.

A személyes adatok védelme tehát modern és aktív jog, amely a fékek és ellensúlyok rendszerét vezette be annak érdekében, hogy védelmet biztosítson az egyének számára személyes adataik kezelése esetén.

> A hesseni törvényt számos európai, az adatvédelem kérdéskörét rendező törvény követte, így a svéd (1973), a német szövetségi (1977), a francia, osztrák, dán, norvég (1978) és a luxembourgi (1978) törvények.

Az európai államok adatvédelemmel kapcsolatos szabályozásának főbb elemei:

- ✓ a személyes adatok gyűjtését, további felhasználását és nyilvánosságra hozatalát törvények szabályozzák, nem pedig irányelvek és egyéb, kötelező erővel nem bíró magatartási kódexek, iránymutatások stb.
- ✓ ezeknek a jogszabályoknak olyan gyűjtőjogszabályoknak kell lenniük, amelyek elviekben minden köz- és privátszférában tevékenykedő adatkezelőre vonatkoznak (meghatározva az eltéréseket úgy, hogy mindeközben az alapelvek tiszteletben tartása töretlen maradjon)
- ✓ ezeknek a törvényeknek magukban kell foglalniuk olyan alapvető anyagi jogi szabályokat is, amelyek lefektetik az alapvető adatvédelmi elveket, illetve az adatkezelésekben érintett személyek jogait, valamint
- ✓ e jogszabályok betartása felett speciális felügyeleti hatóságoknak kell őrködniük.

[45] Volkszählungsurteil, BVerfGE Bd. 65, S. 1skk. Gründe 145-146. Dezember 1983, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. fordította: dr. Albert Ágota
[46] Magyarország: Alaptörvény VI. cikk (1) bekezdés
[47] Magyarország: Alaptörvény VI. cikk (3) bekezdés
[48] Magyarország: Alaptörvény IX. cikk (1) bekezdés
[49] Magyarország: Alaptörvény VIII. cikk (1) bekezdés
[50] Magyarország: Alaptörvény VII. cikk (1) bekezdés

Adatvédelmi irányelvek (EK)

Az Európai Közösség eredeti szerződései nem tartalmaztak hivatkozást az emberi jogokra vagy azok védelmére, hiszen a regionális szervezet eredeti célja gazdasági integráció és közös piacra létrehozás volt, azonban elérkezett az, amikor a tagállamok diverzitása a fejlődés gátjává vált. 1990-ben az Európa Bizottság beterjesztett egy olyan javaslatot, amelynek célja a személyes adatok védelme volt:

- ✓ egy általános EK-irányelv az egyének védelméről a személyes adatok feldolgozása tekintetében (elfogadva: **95/46/EK adatvédelmi irányelv**)
- ✓ kiegészítő EK-irányelv a nyilvános digitális távközlési hálózatokkal összefüggésben az adatok védelméről, különös tekintettel az integrált szolgáltatású digitális hálózatra (ISDN[51]) és a nyilvános digitális mobilhálózatokra (elfogadva: 97/66/EK **távközlési adatvédelmi irányelv**, **utódja** a 2002/58/EK **elektronikus hírközlési irányelv**[52]).

Az EK (későbbiekben uniós) irányelvek jellegzetessége, hogy

- ✓ csakis közösségi jog alá tartozó területek szabályozására korlátozódnak,
- ✓ nem rendelkeznek közvetlen jogi hatállyal, azaz a tagállamoknak implementálni kell saját jogrendszerükbe, és
- ✓ ezen átültetés kapcsán a tagállamok akár jelentős mozgástérrel is rendelkezhetnek.

Adatvédelmi irányelv[53]

Az adatvédelmi irányelv rögzítette az adatvédelmi elveket és egyéb szabályokat, így például a jogalapok rendszerét, a különleges adatok körét és – az irányelvben tételesen meghatározott kivételek hiányában – a kezelési tilalmakat, az érintettek tájékoztatási kötelezettségét, az érintetti jogokat, az adatbiztonság követelményét, a felügyeleti hatóságokat, illetve a harmadik országba adattovábbítás garancia-rendszerét.

Az adatvédelmi irányelv létrehozta a **29. cikk szerinti Adatvédelmi Munkacsoport**ot („WP29”), mely tevékenységével jelentősen hozzájárult az irányelv tagállami szinten harmonizáltabb alkalmazásához, ajánlásaival és véleményeivel pedig nagymértékben befolyásolta az irányelv értelmezését. A WP29 dokumentumai mind a mai napig irányadóak.

Bár az adatvédelmi irányelv célja az volt, hogy teljeskörű harmonizációt és védelmet biztosítson, a tagállamok a gyakorlatban eltérő módon ültették át a rendelkezéseit, mely mind fogalommeghatározásokban, mind a gyakorlatban (például a jogérvényesítés szintjei és szankciók súlyossága terén) jelentős eltéréseket eredményezett. További problémát okozott az ugrásszerű technológiai fejlődés, amely szintén sürgette a reformot, amelynek eredményeképpen az adatvédelmi irányelvet 2018. május 25-i alkalmazással felváltotta **az általános adatvédelmi rendelet (GDPR)**.

[51] Az ISDN telefon a 20. sz. végétől használt digitális távközlési technológia – Integrated Services Digital Network
[52] „ePrivacy” irányelv
[53] Magyarországon az adatvédelmi irányelv rendelkezései az Infotv-be kerültek bele.

A GDPR létrehozta az **Európai Adatvédelmi Testület**et, amely a 29. cikk szerinti Adatvédelmi Munkacsoport örökösének tekinthető.

Elektronikus hírközlési adatvédelmi irányelv[54]

A távközlési adatvédelmi irányelv részletezte és kiegészítette az adatvédelmi irányelvet, azaz speciális szabályokat tartalmazott (tételes számlázás, hívóvonal-azonosítás, telefonkönyvek stb.). Az irányelv tagállami átültetése késett, majd a felváltására 2002-ben elfogadták a magánélet és az elektronikus hírközlés védelméről szóló 2002/58/EK irányelvet (ePrivacy irányelv)[55], amely ugyanolyan kiegészítő jellegű, mint az elődje. Az irányelvet a „sütitörvény"[56] módosította. Az irányelv rendeletté alakítása évek óta napirenden van, ez azonban még nem történt meg.

„(1) Ez az irányelv előírja azon nemzeti rendelkezések összehangolását, amelyekre azért van szükség, hogy biztosítsák az elektronikus hírközlési ágazatban a személyes adatok kezelése vonatkozásában az alapvető jogok és szabadságok védelmének egyenértékű szintjét – különös tekintettel a magánélethez és a bizalmas adatkezeléshez való jogra –, valamint biztosítsák az ilyen adatoknak, az elektronikus hírközlő berendezéseknek és az elektronikus hírközlési szolgáltatásoknak a Közösségen belüli szabad mozgását." [57]

Az irányelv rendelkezései pontosítják és kiegészítik az adatvédelmi irányelvet, illetve rendelkeznek a jogi személyiséggel rendelkező előfizetők jogos érdekeinek védelméről.

Az ePrivacy irányelv és a 95/46/EK irányelvet felváltó GDPR hatályának kérdéseit az Európai Adatvédelmi Testület 6/2021. számú véleménye[58] részletesen tárgyalja. A problémakört az teszi különösen fontossá, hogy az is előfordulhat, hogy a GDPR és az ePrivacy irányelvek rendelkezéseit tartalmazó tagállami jogszabály betartása feletti felügyelet két különböző hatóság alá tartozik[59]. A sokszor szinte feloldhatatlannak tűnő hatály-kérdést az ePrivacy rendelet jövőbeni hatályba lépése rendezni fogja, mivel a rendelet felügyeletét és végrehajtását – tervek szerint – az általános adatvédelmi rendelet tekintetében illetékes felügyeleti hatóságokra bízza, figyelemmel az általános adatvédelmi kérdések és a hírközlés titkossága közötti nagymértékű szinergiákra.[60]

[54] Magyarországon az elektronikus hírközlési irányelv rendelkezései az elektronikus hírközlésről szóló 2003. évi C. törvénybe (Eht.) kerültek bele.
[55] "elektronikus hírközlési adatvédelmi irányelv", „ePrivacy", Egységes szerkezetben: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:02002L0058-20091219&from=EN
[56] 2009/136/EK irányelv
[57] ePrivacy irányelv 1. cikk
[58] 5/2019. számú vélemény az elektronikus hírközlési adatvédelmi irányelv és az általános adatvédelmi rendelet
közötti kölcsönhatásról, különösen az adatvédelmi hatóságok illetékessége, feladatai és hatásköre tekintetében, elfogadás időpontja: 2019. március 12.,
https://www.naih.hu/files/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_hu.pdf
[59] Lásd pl. Magyarország NAIH és NMHH
[60] Javaslat AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet), Indoklás 5.2. pont, Brüsszel,

Az olasz adatvédelmi hatóság (Garante per la protezione dei dati personali) gyakorlatából

Az olasz adatvédelmi hatóság figyelmeztette a TikTokot, amiért az adatvédelmi tájékoztatójának frissítése szerint az a felhasználók hozzájárulása nélkül kívánta kezelni a sütiket.

A hatóság a vizsgálata során megállapította, hogy

- *az új adatkezelési tájékoztató szerint a TikTok csak 18 év feletti felhasználók számára és a TikTok jogos érdekére hivatkozva szolgáltatna személyre szabott reklámot [(GDPR 6. cikk (1) bekezdés f) pontja)]. Az olasz adatvédelmi hatóság álláspontja szerint a személyre szabott reklámok valószínűleg sütiket vagy más nyomonkövetési mechanizmusok használatával járnának.*
- *az elektronikus hírközlési adatvédelmi irányelv alkalmazandó az adatkezelő süti-kezelésére,*
- *a TikTok új adatkezelési tájékoztatójában foglalt gyakorlat sérti az elektronikus hírközlési adatvédelmi irányelvet, mivel az irányelv csak a felhasználó beleegyezésével engedélyezi az adatkezelő számára sütik és hasonló nyomon követési mechanizmusok használatát [2002/58/EK irányelv) 5. cikkének (3) bekezdése], emiatt a jogos érdek nem lehet jogszerű jogalap a sütik feldolgozására [GDPR 6. cikke (1) bekezdésének f) pontja].*[61]

Az ePrivacy irányelv számos speciális szabályt tartalmaz, például

- ✓ az elektronikus hírközlési szolgáltatásokat nyújtók kötelesek többek között biztosítani, hogy a személyes adatokhoz való hozzáférés kizárólag arra feljogosított személyekre korlátozódjon, valamint kötelesek megtenni minden szükséges intézkedést az adatok megsemmisülésének, elvesztésének vagy részleges sérülésének megelőzése érdekében.
- ✓ a hálózati biztonság megsértésének konkrét kockázata esetén a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyújtó szolgáltatónak tájékoztatnia kell az előfizetőket az ilyen kockázatról. Ha a végrehajtott biztonsági intézkedések ellenére a biztonság megsértése következik be, a szolgáltatók kötelesek értesíteni az irányelvben foglaltak végrehajtásával és érvényesítésével megbízott illetékes nemzeti hatóságot a személyes adatok megsértéséről.
- ✓ amikor a jogsértés valószínűleg hátrányosan befolyásolja az egyének személyes adatait vagy magánéletüket, a szolgáltatóknak értesíteniük kell az egyéneket is a személyes adatok megsértéséről,
- ✓ a közlések bizalmassága előírja, hogy elvben tilos a közlések és a metaadatok meghallgatása, lehallgatása, tárolása vagy bármilyen módon történő elfogása vagy megfigyelése.

2017.1.10. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52017PC0010&from=HU

[61] Provvedimento del 7 luglio 2022 [9788429].
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9788429

- ✓ tiltja a nem kívánt tájékoztatást („spameket” vagy „levélszemetet”), kivéve, ha a felhasználók ehhez hozzájárultak.

Az irányelv szabályokat tartalmaz a számítógépeken és más eszközökön tárolt sütikre vonatkozóan is, valamint a rendelkezései az IoT-eszközökre[62] is vonatkoznak, miszerint egy előfizető vagy felhasználó végberendezésében történő adattárolás, illetve az ott tárolt adatokhoz való hozzáférés csak azzal a feltétellel megengedett, ha az érintett előfizető vagy felhasználó egyértelmű és teljes körű tájékoztatás alapján ehhez előzetes hozzájárulását adta. Ez a rendelkezés nem akadályozza az olyan műszaki tárolást, illetve műszaki hozzáférést, amelynek kizárólagos célja az elektronikus hírközlő hálózaton keresztül történő közléstovábbítás, vagy amelyre az előfizető vagy felhasználó által kifejezetten kért, az információs társadalommal összefüggő szolgáltatás nyújtásához a szolgáltatónak feltétlenül szüksége van.[63]

A francia adatvédelmi hatóság (CNIL[64]) gyakorlatából

2020. december 7-én a CNIL két, összesen 100 millió eurós bírságot szabott ki a Google LLC-re és a Google Ireland Ltd-re a francia adatvédelmi törvény 82. cikkének megsértése miatt (amely az elektronikus hírközlési adatvédelmi irányelvet ülteti át). A CNIL szerint a Google

- ✓ *nem szerezte be a felhasználó hozzájárulását, mielőtt reklámsütiket helyezett el a felhasználó végberendezésében,*
- ✓ *elmulasztotta a tájékoztatást, és*
- ✓ *nem vezetett be a sütik elutasítására szolgáló mechanizmust.*

A Google nem értett egyet a CNIL döntésével, és bírósághoz fordult az ügyben. Az Államtanács elutasította a Google fellebbezését és – többek között – megerősítette az adatvédelmi törvény 82. cikkének három jogsértését, illetve azt is megállapította, hogy a bírságok nem voltak aránytalanok a „két„ vállalat pénzügyi kapacitására tekintettel [a Google több mint 90%-os piaci részesedése, (becslések szerint) 47 millió franciaországi felhasználó, a célzott online hirdetésekből származó nagy nyereség]. Ezen kívül a Google nem működött együtt ténylegesen a CNIL-lel, mivel nem szolgáltatott adatokat a reklámbevételekről és a jogsértések súlyosak voltak.[65]

[62] „tárgyak internete (Internet of Things) olyan infrastruktúrára utal, amelyben a mindennapi eszközökbe (önálló „dolgokba” vagy egyéb tárgyakhoz vagy személyekhez kapcsolódó dolgokba) beépített érzékelők milliárdjait arra tervezik, hogy adatokat rögzítsenek, kezeljenek, tároljanak és továbbítsanak, és – mivel egyedi azonosítóval rendelkeznek – a hálózati szolgáltatások segítségével együttműködjenek más eszközökkel vagy rendszerekkel.” 29. cikk szerinti Adatvédelmi Munkacsoport: 8/2014. számú vélemény a tárgyak internetének legújabb fejleményeiről, WP223, elfogadás: 2014. szeptember 16. (továbbiakban WP223) 4.o.

[63] ePrivacy irányelv 5. cikk (3) bekezdés

[64] Commission nationale de l'informatique et des libertés

[65] Conseil d'État, 10ème – 9ème chambres réunies, 28/01/2022, 449209, Publié au recueil Lebon, https://www.legifrance.gouv.fr/ceta/id/CETATEXT000045084087?init=true&page=1&query=&searchField=ALL&tab_selection=cetat, utolsó letöltés 2022. 07. 08.

Európai Unió Alapjogi Charta

Az EU **2000**-ben kihirdette az **Európai Unió Alapjogi Chartá**ját („Charta")[66], amelyben a magán- és családi élet tiszteletben tartása (7. cikk) mellett az adatvédelemhez való jog (8. cikk) különálló alapjog formájában jelenik meg. Az adatvédelemhez való jogot az EU működéséről szóló szerződés[67] is megerősíti.

Alapjogi Charta 8. cikk
(1) Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.
(2) Az ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni.
(3) E szabályok tiszteletben tartását független hatóságnak kell ellenőriznie.

EUMSZ 16. cikk *(az EKSz. korábbi 286. cikk)*
(1) Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.
(2) A természetes személyeknek az uniós intézmények, szervek és hivatalok által, illetve az uniós jog alkalmazási körébe tartozó tevékenységeik során a személyes adataiknak a tagállamok által végzett feldolgozása tekintetében történő védelmére, valamint az ilyen adatok szabad áramlására vonatkozó szabályokat rendes jogalkotási eljárás keretében az Európai Parlament és a Tanács állapítja meg. E szabályok tiszteletben tartását független hatóságok ellenőrzik.

Eredetileg a Charta csupán politikai dokumentum volt, a **Lisszaboni Szerződés**[68] **2009. december 1**-jei hatálybalépésével elsődleges uniós joganyagként jogilag kötelező erejűvé vált.

A Charta 8. cikke nemcsak a személyes adatok védelméhez való jogot tartalmazza, hanem pontosan meghatározza az e joghoz kapcsolódó alapvető értékeket is:

- ✓ a személyes adatokat tisztességesen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogalapon lehet kezelni,
- ✓ az egyének számára biztosítani kell a jogot, hogy a róla gyűjtött személyes adatokat megismerje és azokat kijavíttassa, valamint
- ✓ e jog tiszteletben tartását független hatóságnak kell ellenőriznie.

A Charta alapján a védelem a személyes adatok minden fajtájára és az adatkezelés minden fajtájára kiterjed függetlenül attól, hogy az adott esetnek milyen kapcsolata van a magánélettel, illetve a magánéletre gyakorolt hatással.

[66] [66] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:12012P/TXT&from=HU
[67] Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata (2012/C 326/01) itt található meg: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:12012E/TXT&from=HU
[68] https://www.europarl.europa.eu/factsheets/hu/sheet/5/a-lisszaboni-szerzodes

Általános adatvédelmi rendelet (GDPR)

2018. május 25-én vált alkalmazandóvá az új uniós Általános Adatvédelmi Rendelet,[69] amely az 1995-ös adatvédelmi irányelv[70] helyébe lépett.

A GDPR – mint általános érvénnyel használandó uniós jogszabály – számos változást hozott, különösen a tagállamok adatvédelmi jogának harmonizációja, az érintettek erősebb jogai, az adatvédelmi hatóságok közötti szorosabb, határokon átnyúló együttműködése tekintetében.

A GDPR minden tagállamban egyenszilárdságú védelmet biztosít az adatok tekintetében, melynek köszönhetően az Unió minden tagállamában ugyanaz a védelem jár, bármelyik állam polgárai is vagyunk.

A holland bírósági gyakorlatból

Az Államtanács közigazgatási kollégiuma úgy ítélte meg, hogy a GDPR (hollandul: AVG) 17. cikke (3) bekezdésének e) pontjában foglalt „elfeledtetéshez való jog" alóli kivétel magában foglalja a jogi igényekkel szembeni védekezés céljából történő megőrzést még akkor is, ha a holland szöveg nem használja kifejezetten a „védelem„ szót.

A kollégium megjegyezte, hogy az uniós jogszabályok értelmezésekor nemcsak a szövegezést, hanem a kontextust és a célt is figyelembe kell venni, ehhez pedig a különböző nyelvi változatok összehasonlítására is szükség lehet.
A kollégium megállapította, hogy a GDPR 17. cikk (3) bekezdés e) pontjának angol, német és francia nyelvű változata mind sokkal tágabb hatályú, mint a holland szöveg. Ezekben a „védelem„ (defence; Verteidigung; défense) szó valamilyen fordításában szerepeltek, míg a holland változat csupán az „alátámasztó" (onderbouwing) szót használta.

A kollégium véleménye, hogy a fordítások ilyen eltérései esetén a jogszabály célját és rendeltetését kell figyelembe vennie az egységes értelmezés érdekében (lásd EUB[71] Kraaijveld-ügy[72]). A GDPR célja a természetes személyek védelme a személyes adatok kezelése során[73], azonban ezt egyensúlyba kell hozni az Unió

[69] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, továbbiakban „GDPR")
[70] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról
[71] Európai Unió Bírósága
[72] C-72/95. sz. ügy, https://curia.europa.eu/juris/showPdf.jsf;jsessionid=F7EA6B014B1CFAA678AEE0F8203DAFB5?text=&docid=100313&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=445090, utolsó letöltés 2022. 07. 29.
[73] Lásd GDPR (1) és (2) preaambulumbekezdés

Alapjogi Chartájában elismert egyéb alapvető jogokkal[74], így a Charta 47. cikkével, amely magában foglalja a védelemhez való jogot (EUB Otis[75]), mindezekre tekintettel a kollégium megállapította, hogy a 17. cikk (3) bekezdésének e) pontjának német, angol és francia nyelvű változata jobban összhangban van a GDPR céljával, mint a holland változat.

A kollégium véleménye szerint az AVG 17. cikk (3) bekezdésének e) pontja magában foglalja a jogi igénnyel szembeni védekezést.[76]

Ez persze nem azt jelenti, hogy Máltán pontosan ugyanolyan szabályok vonatkoznak a személyes adatok adatkezelésére, mint Litvániában vagy Ausztriában, mivel a közvetlenül alkalmazandó rendeletet a nemzeti sajátosságoknak megfelelően törvények sora egészítheti ki, a keretszabályok azonban mindenhol ugyanazok, különösen az alapelvek, az érintettek jogai, valamint a felügyeleti hatóságok együttműködése és a szankcionálási gyakorlat tekintetében. És bár a rendelet ugyanúgy érvényes minden tagállamban, nem szabad meglepődnünk azon, hogy előfordulhat, ami az egyik tagállamban ajánlott eljárás, az egy másikban kifejezetten tilos.

Példa a tagállami eltérésre

Magyarországon a hatályos jogszabály[77] alapján a csomagellenőrzés során a random generátor alkalmazása kifejezetten tilos, azaz senkinek a táskáját sem lehet csak azért ellenőrizni, mert egy véletlenszerűen működő rendszer kiválasztotta. Németországban viszont van olyan büntetésről szóló határozat, amelynek indoklásában a felügyeleti hatóság kifejtette, hogy az adatkezelő által használt elektronikus megfigyelés helyett a privát szférába sokkal kevesebb beavatkozást jelentett volna a csomagok szúrópróbaszerű ellenőrzése[78].

Ez esetben azonban nem a GDPR eltérő értelmezéséről van szó, hanem a tagállami szabályozás eltéréséről.

---

[74] Lásd GDPR (4) preaambulumbekezdés

[75] C-435/18. sz. ügy, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:62018CJ0435&from=hu, utolsó letöltés 2022. 07. 29.

[76] ECLI:NL:RVS:2022:2065, https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RVS:2022:2065, utolsó letöltés: 2022. október 23.

[77] a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény

28. § (1) A vagyonőr a csomag tartalmának, jármű és szállítmány bemutatására a szerződésből fakadó kötelezettségei érvényesítése céljából, a tervezett intézkedése okának és céljának közlése mellett akkor hívhat fel, ha

a) megalapozottan feltehető, hogy az érintett bűncselekményből vagy szabálysértésből származó olyan dolgot tart magánál, amelynek őrzése a vagyonőrnek szerződésből fakadó kötelezettsége;

b) e dolgot a felszólítás ellenére sem adja át; és

c) az intézkedés a jogsértő cselekmény megelőzése, megszakítása érdekében szükséges.

[78] State Commissioner for Data Protection in Lower Saxony imposes € 10.4 million fine against notebooksbilliger.de, https://edpb.europa.eu/news/national-news/2021/state-commissioner-data-protection-lower-saxony-imposes-eu-104-million-fine_en

Bűnügyi adatvédelmi irányelv (LED[79])

Az általános adatvédelmi rendelettel együtt elfogadásra került a személyes adatok állami hatóságok által bűnüldözési célokra történő kezeléséről szóló irányelv (továbbiakban: **LED**)[80] is.

A LED a bűnüldözéssel összefüggésben létrehozta a személyes adatok védelmének átfogó rendszerét úgy, hogy elismerte a közbiztonsággal kapcsolatos adatkezelések sajátosságait és konkrét adatvédelmi szabályokat határozott meg a büntetőügyekben folytatott rendőrségi és igazságszolgáltatási terén. Az irányelv rendelkezéseit hazánkban az Infotv.[81] ülteti át.

A LED lényeges elemei:

- ✓ az irányelvre a nemzeti bíróságok, illetve az Európai Unió Bírósága előtt hivatkozhatnak az egyének az állam ellen indított keresetekben,
- ✓ szabályokat állapít meg a természetes személyek védelmére a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása – így többek között a közbiztonságot fenyegető veszélyekkel szembeni védelem és e veszélyek megelőzése – céljából végzett kezelése tekintetében.[82]
- ✓ az irányelv nem akadályozza meg a tagállamokat abban, hogy az érintettek jogainak és szabadságainak védelme érdekében a személyes adatok illetékes hatóságok által végzett kezelésére az irányelvben megállapítottnál magasabb védelmi szintet biztosító garanciákról rendelkezzenek.[83]
- ✓ Az irányelvben meghatározott adatkezelési célok esetében az irányelvben foglaltakat kell alkalmazni a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni.[84]
- ✓ az irányelv hatálya alá tartozó szervezeteknek is meg kell felelniük az elszámoltathatóság elvének.[85]

[79] Law Enforcement Directive
[80] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/680 IRÁNYELVE (2016. április 27) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv, „LED”), https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L0680&from=EL
[81] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)
[82] LED 1. cikk (1) bekezdés
[83] LED 1. cikk (3) bekezdés
[84] LED 2. cikk (2) bekezdés
[85] LED 4. cikk (4) bekezdés

- ✓ meghatározza az „illetékes hatóság” fogalmát, mely szerint az illetékes hatóság
  - ✓ olyan közhatalmi szerv, amely a bűncselekmények megelőzését, nyomozását, felderítését vagy üldözését, illetve büntetőjogi szankciók végrehajtását illetően eljárni jogosult beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését; vagy
  - ✓ bármely egyéb, olyan szerv vagy más jogalany, amely a tagállami jog alapján közfeladatokat lát el és közhatalmi jogosítványokat gyakorol a bűncselekmények megelőzése, nyomozása, felderítése vagy a vádeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása céljából, beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését.[86]
- ✓ a fogalmak[87] sok esetben gyakorlatilag a GDPR fogalmaival azonosak
- ✓ széles körű korlátozásokat tesz lehetővé az érintetti jogokkal kapcsolatban, így többek között atéren, hogy tájékoztatást kapjanak az adatkezelésről, hozzáférhessenek az adataikhoz, valamint, hogy helyesbítsék vagy törölhessék azokat az adatokat, amelyek nem felelnek meg a vonatkozó adatminőségi előírásoknak, vagy amelyeket egyébként az irányelvben meghatározott szabályokkal ellentétesen kezelnek. Azonban ezeket a korlátozásokat a demokratikus társadalomban szükséges és arányos mértékre kell korlátozni.[88] Az irányelv lehetővé teszi azt is, hogy az érintetti jogokat közvetve, az illetékes felügyeleti hatóságon keresztül is lehessen gyakorolni.[89]
- ✓ Az irányelv meghatározza a harmadik országba történő adatátadás előfeltételeit, illetve rendelkezik az adatátadással kapcsolatos garanciákról is.[90]

Azokban az esetekben, amikor egy illetékes hatóság a személyes adatokat bűncselekmények megelőzése, nyomozása, felderítése, büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából kezeli, a LED rendelkezéseit kell alkalmazni. Amennyiben ezek a hatóságok ettől eltérő célú adatkezeléseket végeznek, a tevékenységükre a GDPR szabályai az irányadóak.

Az EDPB a LED alkalmazásával kapcsolatban is jogosult kiadni iránymutatásokat.

Az EDPB 2022. májusában társadalmi egyeztetésre bocsátotta az arcfelismerőrendszerek LED-relevanciájú alkalmazásával kapcsolatos iránymutatásának 1.0 verzióját.[91] Ebben az EDPB emlékeztet az EDPB és az

[86] LED 3. cikk 7. pont
[87] LED 3. cikk
[88] LED 12-16. cikk, különösen: a hozzáférési jog korlátozása, 15. cikk
[89] LED 17. cikk
[90] LED 35-39. cikk
[91] Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 1.0 Adopted on 12 May 2022, https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf, Utolsó letöltés 2022. 07. 09.

európai adatvédelmi biztos (EDPS) közös felhívására, amely szerint be kell tiltani bizonyos típusú feldolgozási eljárásokat az alábbi eljárásokkal kapcsolatban:
(1) személyek távoli biometrikus azonosítása nyilvánosan hozzáférhető helyeken,
(2) mesterséges intelligenciával támogatott arcfelismerő rendszerek, amelyek a biometrikus adatok alapján etnikai hovatartozás, nem szerint csoportosítják a személyeket, illetve politikai vagy szexuális irányultság vagy más megkülönböztetés alapján,
(3) arcfelismerő vagy hasonló technológiák használata egy természetes személy érzelmeire való következtetés céljából, és
(4) személyes adatok bűnüldözési célú kezelése, amely személyes adatok tömeges és megkülönböztetés nélküli gyűjtésével feltöltött adatbázisra támaszkodik, pl. az interneten hozzáférhető fényképek és arcképek „lekérdezésével”.

A LED hatálya alá tartozó szervezeteknek figyelemmel kell lenniük arra, hogy olyan adatkezelések esetén, mint például szervezett bűnözés és a terrorizmus megelőzése, nyomozása, felderítése és büntetőeljárás alá vonása céljából biometrikus adatok kezelése során is minden esetben tiszteletben kell tartani az alapvető jogokat, így különösen a Charta 7. cikke szerinti magánélet és kommunikáció tiszteletben tartását, valamint a Charta 8. cikke szerinti személyes adatok védelméhez való jogot.

Példák az Infotv. (LED) alkalmazására

- ✓ *igazoltatás*
- ✓ *büntetőeljárás keretében a gyanúsított adatainak kezelése*
- ✓ *nemzetbiztonsági szolgálatok műveleti tevékenységének keretében a megfigyelt személy adatainak kezelése*
- ✓ *térfigyelő kamerák üzemeltetése*

Példák a GDPR alkalmazására

- ✓ *rendőrség/honvédség hivatásos állományba tartozó személy (mint alkalmazott) adatainak kezelése*
- ✓ *rendőrség által lefolytatott, nem bűnüldözéssel összefüggő eljárások keretében történő adatkezelés (pl. járványügyi intézkedéssel, fegyvertartási engedéllyel kapcsolatos ügyek[92])*

Az irányelv alapján a tagállamok megállapítják az irányelv alapján elfogadott rendelkezések megsértése esetén alkalmazandó szankciókra vonatkozó szabályokat, és meghoznak minden szükséges intézkedést ezek végrehajtására. Az előírt szankcióknak hatékonynak, arányosnak és visszatartó erőjűnek kell lenniük.

[92] https://ugyintezes.police.hu/web/guest/uj-ugy-inditasa/

Magyar szabályozás

Alaptörvény[93]

Alaptörvényünk VI. cikke alapján

- ✓ mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát, kapcsolattartását és jó hírnevét tiszteletben tartsák,
- ✓ a véleménynyilvánítás szabadsága és a gyülekezési jog gyakorlása nem járhat mások magán- és családi életének, valamint otthonának sérelmével,
- ✓ az állam jogi védelemben részesíti az otthon nyugalmát, valamint
- ✓ mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez.

Infotv.[94]

Az Infotv. alapvetően a személyes adatok bűnüldözési, nemzetbiztonsági és honvédelmi célú kezelésére kell alkalmazni[95], illetve bizonyos szakaszait[96] a GDPR kiegészítéseként.

Az Infotv. alapján

- ✓ **bűnüldözési célú adatkezelés**: a jogszabályban meghatározott feladat- és hatáskörében a közrendet vagy a közbiztonságot fenyegető veszélyek megelőzésére vagy elhárítására, a bűnmegelőzésre, a bűnfelderítésre, a büntetőeljárás lefolytatására vagy ezen eljárásban való közreműködésre, a szabálysértések megelőzésére és felderítésére, valamint a szabálysértési eljárás lefolytatására vagy ezen eljárásban való közreműködésre, továbbá a büntetőeljárásban vagy szabálysértési eljárásban megállapított jogkövetkezmények végrehajtására irányuló tevékenységet folytató szerv vagy személy (a továbbiakban együtt: bűnüldözési adatkezelést folytató szerv) ezen tevékenység keretei között és céljából – ideértve az ezen tevékenységhez kapcsolódó személyes adatok levéltári, tudományos, statisztikai vagy történelmi célból történő kezelését is – (a továbbiakban együtt: bűnüldözési cél) végzett adatkezelése[97]
- ✓ **nemzetbiztonsági célú adatkezelés**: a nemzetbiztonsági szolgálatok jogszabályban meghatározott feladat- és hatáskörében végzett adatkezelése, valamint a rendőrség terrorizmust elhárító szervének jogszabályban meghatározott feladat- és hatáskörében végzett, a nemzetbiztonsági szolgálatokról szóló törvény hatálya alá tartozó adatkezelése[98]
- ✓ **honvédelmi célú adatkezelés**: a honvédségi adatkezelésről szóló törvény, továbbá a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló törvény, és a Magyar

[93] https://net.jogtar.hu/jogszabaly?docid=a1100425.atv
[94] az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
[95] Infotv. 2.§ (3) bekezdés
[96] Infotv. 2.§ (2) bekezdés
[97] Infotv. 3.§ 10a. pont
[98] Infotv. 3.§ 10b. pont

Köztársaság területén szolgálati céllal tartózkodó külföldi fegyveres erők, valamint a Magyar Köztársaság területén felállított nemzetközi katonai parancsnokságok és állományuk nyilvántartásáról, valamint jogállásukhoz kapcsolódó egyes rendelkezésekről szóló törvény hatálya alá tartozó adatkezelés.[99]

Példa a GDPR és az Infotv. alkalmazására

A helyi tankerület (iskola) a GDPR alapján oktatási célokra gyűjthet személyes adatokat az iskolásokról, amely adatok egy részéhez a rendőrség kérhet hozzáférést, mert a gyerekeket meg szeretné hívni egy, a rendőrök által tartott karácsonyi ünnepségre. Ebben az esetben mindkét szervezet adatkezelése a GDPR hatálya alá tartozik.

A helyi tankerület (iskola) a GDPR alapján oktatási célokra gyűjthet személyes adatokat az iskolásokról, amely adatokhoz (vagy az adatok egy részéhez) a rendőrség kérhet hozzáférést bűncselekmény felderítése céljából. Ilyen lehet például az, amikor egy bűncselekmény esetén felmerül az, hogy kiskorú követte el, a rendőrség pedig információt szeretne arról, hogy az elkövetés idején melyik – gyanú alá vont – gyermek hiányzott az iskolából. Míg az iskola a GDPR alapján kezeli és továbbítja az adatokat, a rendőrség már az Infotv. (LED) alapján.

A telefontársaság a hívások adatait a GDPR alapján kezeli (gyűjti és tárolja), azonban a nemzetbiztonsági szolgálatok ezeket az adatokat (pl. cellainformációkat, híváslistákat) kikérhetik nemzetbiztonsági célból. Ez esetben a telefontársaság a GDPR szabályai alapján továbbíthatja az adatokat, a nemzetbiztonsági szolgálatok (mivel nem tartoznak az uniós jog hatálya alá) nemzetbiztonsági célból az Infotv. alapján kezelik az adatokat.

Ágazati szabályok

Számtalan ágazati jogszabályunk tartalmaz adatvédelmi rendelkezéseket, így például

- ✓ a munka törvénykönyve (Mt.)[100]
- ✓ a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló törvény[101]
- ✓ az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló törvény[102]
- ✓ a panaszokról és a közérdekű bejelentésekről szóló törvény[103]
- ✓ a nemzeti köznevelésről [104] és a nemzeti felsőoktatásról szóló törvény[105]
- ✓ az elektronikus hírközlésről szóló törvény[106]
- ✓ a személyszállítási szolgáltatásokról szóló törvény[107] stb.

[99] Infotv. 3.§ 10c. pont
[100] https://net.jogtar.hu/jogszabaly?docid=a1200001.tv
[101] https://net.jogtar.hu/jogszabaly?docid=a0500133.tv
[102] https://net.jogtar.hu/jogszabaly?docid=a0100108.tv
[103] https://net.jogtar.hu/jogszabaly?docid=a1300165.tv
[104] https://net.jogtar.hu/jogszabaly?docid=a1100190.tv
[105] https://net.jogtar.hu/jogszabaly?docid=a1100204.tv
[106] https://net.jogtar.hu/jogszabaly?docid=a0300100.tv
[107] https://net.jogtar.hu/jogszabaly?docid=a1200041.tv

Amennyiben az ágazati törvény adatkezelésre vonatkozó szabálya ütközik a GDPR előírásaival, az uniós rendeletben megfogalmazottak az irányadók.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A Kérelmezett a felvételek törlésének indokaként az akkor hatályos Szvtv. 31. § (6) bekezdésére hivatkozott, mely rendelkezés alapján a jogalkotó alapvetően annak lehetőségét biztosította az érintett számára, hogy joga vagy jogos érdekének igazolásával a felvételek zárolását kérje. Ekkor az adatkezelőnek a felvételt zárolnia kellett, majd amennyiben bíróság vagy valamely hatóság az eljárása során a felvételt igényelte, akkor azt meg kellett küldeni. Amennyiben a bíróság vagy a hatóság harminc napon belül a felvételeket nem kérte ki, akkor az adatkezelőnek a felvételt meg kellett semmisítenie, ezért célszerű volt a bírósági, illetve a hatósági eljárás megindításakor kifejezetten utalni erre a speciális körülményre, és felhívni az eljáró bíróság vagy hatóság figyelmét arra, hogy a felvételt e határidőn belül kérje ki. Ha a bíróság vagy a hatóság nem kereste meg az adatkezelőt a felvétel kiadása érdekében, akkor a felvételeket törölni kellett.

Az Szvtv. ezen rendelkezésére tekintettel tehát a Kérelmezett törölte a felvételeket a zárolást követő harminc nap elteltével, mivel a rendőrségtől és a Kérelmezőtől sem érkezett megkeresés.

Ezen 2018. novemberi és decemberi időszakban azonban már alkalmazandó volt az általános adatvédelmi rendelet – 2018. május 25. napjától. Ugyanakkor a 2019. évre maradt számos (szektorális) adatvédelmi előírást tartalmazó jogszabály, mint például az Szvtv. általános adatvédelmi rendelethez való „igazítása", amelynek változásai csak 2019. április 26. napján léptek hatályba. Ezen időszakig azonban az Szvtv. szabályait az általános adatvédelmi rendeletre tekintettel kellett értelmezni. Ebből kifolyólag az Szvtv. 31. § (6) bekezdése bár előírta azt, hogy amennyiben bíróság vagy a hatóság harminc napon belül a felvételeket nem kérte ki, akkor az adatkezelő semmisítse meg a zárolt felvételeket, az általános adatvédelmi rendelet adatkezelés korlátozásához való jog gyakorlására vonatkozó rendelkezései nem támasztanak ilyen feltételt, ebből pedig az következik, hogy a jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez szükséges időtartamig, például az adott jogi eljárás végéig zároltan kell tárolni a felvételeket, azokat nem lehet törölni.

Az általános adatvédelmi rendelet előírásai a magyar jogalanyokra 2018. május 25. napjától közvetlenül alkalmazandók, kivéve azokat, amelyek teljes körű alkalmazásához, végrehajtásához az egyes tagállamok nemzeti jogszabályaiban előírt további rendelkezések szükségesek. Emellett az általános adatvédelmi rendelet bizonyos – korlátozott – körben lehetőséget ad a tagállamoknak kiegészítő vagy ahhoz képest meghatározott irányban eltérő szabályok megalkotására, azonban az érintetti jogok gyakorlása nem tartozott ebbe a körbe, a tagállamok, így Magyarország sem kapott arra felhatalmazást, hogy az érintetti jogok gyakorlását korlátozza, ezért az Szvtv. 31. § (6)

bekezdését nem lehetett alkalmazni, ha az érintett kérte az adatkezelőtől a kamerafelvételek törlésének, megsemmisítésének mellőzését.

Ebből következően a Hatóság megállapítja, hogy a Kérelmezett az általános adatvédelmi rendelet szabályaival ellentétesen törölte a Kérelmező által kért, és a Kérelmezett által zárolt kamerafelvételeket a Kérelmező zárolásra irányuló kérelmét követő harminc nap elteltét követően. A Hatóság ebből adódóan megállapítja, hogy a Kérelmezett megsértette az általános adatvédelmi rendelet 18. cikk (1) bekezdés c) pontját." [108]

Az Európai Unió Bírósága (EUB, Luxembourg)[109]

Az Európai Unió Bíróságának 1952-ben történt alapítása óta az a feladata, hogy biztosítsa az európai jog tiszteletben tartását a Szerződések értelmezése és alkalmazása során. Ezen tevékenysége során:

- ✓ felülvizsgálja az Európai Unió intézményei jogi aktusainak jogszerűségét,
- ✓ gondoskodik arról, hogy a tagállamok teljesítsék a Szerződésekből eredő kötelezettségeiket és
- ✓ a nemzeti bíróságok kérelmére értelmezi az uniós jogot, azaz az EUB a tagállami bíróságokkal együttműködve gondoskodik az uniós jog egységes értelmezéséről és alkalmazásáról.

Az adatvédelmi irányelv 1995-ös elfogadása óta széles körű ítélkezési gyakorlat alakult ki a Bíróságon. Annak ellenére, hogy az irányelv hatályát veszítette és mára már a GDPR van érvényben, az előzetesen meglévő ítélkezési gyakorlat továbbra is releváns és érvényes marad az uniós adatvédelmi elvek értelmezése és alkalmazása tekintetében.

Jogszabályok

- ✓ AZ EURÓPAI UNIÓ ALAPJOGI CHARTÁJA 2012/C 326/02[110]
- ✓ Magyarország Alaptörvénye (2011. április 25.)[111]
- ✓ AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2002/58/EK IRÁNYELVE (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv, „**ePrivacy**")[112]
- ✓ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról,

[108] NAIH/2020/200/5, Budapest, 2020. március 19, https://naih.hu/files/NAIH-2020-200-hatarozat.pdf, utolsó letöltés: 2022. 07. 09.
[109] https://curia.europa.eu/jcms/jcms/j_6/hu/
[110] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:12012P/TXT&from=HU
[111] https://net.jogtar.hu/jogszabaly?docid=a1100425.atv
[112] Egységes szerkezetben: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:02002L0058-20091219&from=EN#tocId3

valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, „**GDPR**”)[113]

- ✓ AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/680 IRÁNYELVE (2016. április 27) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről („**LED**”)[114]
- ✓ 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (**Infotv**.)[115]
- ✓ 2003. évi C. törvény az elektronikus hírközlésről (**Eht**.)[116]
- ✓ 2018. évi LIII. törvény a magánélet védelméről[117]

[113] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679#d1e40-1-1
[114] https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L0680&from=EL
[115] https://net.jogtar.hu/jogszabaly?docid=a1100112.tv
[116] https://net.jogtar.hu/jogszabaly?docid=a0300100.tv
[117] https://net.jogtar.hu/jogszabaly?docid=A1800053.TV

AZ ADATVÉDELEM ÉS A NEMZETBIZTONSÁGI KOCKÁZAT

Resperger István szerint[118] a nemzetbiztonsági kockázatok az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége, a lehetséges veszélyek olyan megnyilvánulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek. A kihívás alacsonyabb szintű állapot, míg a fenyegetés a legmagasabb szintű, amikor már nemzeti érdekek sérülhetnek.

Melyek ezek a kockázatok és hogyan jelennek meg az adatvédelem és adatbiztonság területén?

Nemzetbiztonsági kockázatok lehetnek:

- ✓ az eltérő társadalmi fejlődésből fakadó, országok és csoportok közötti, átmeneti vagy tartós ellentétek,
- ✓ a gazdasági, pénzügyi és társadalmi válságok,
- ✓ az etnikai és vallási feszültségek,
- ✓ a terrorizmus,
- ✓ a szervezett bűnözés és a közbizalmat aláásó bűncselekmények (pl. a korrupció, rémhírterjesztés stb.),
- ✓ az illegális kábítószer- és fegyverkereskedelem, valamint embercsempészet,
- ✓ a tömeges migráció,
- ✓ a környezeti szennyezések és egyéb környezeti hatások,
- ✓ a tömegpusztító fegyverek és azok hordozóeszközeinek elterjedése,
- ✓ az információs rendszerek elleni kibertámadások, valamint
- ✓ a járványok (pl. COVID19) nemzetbiztonsági kockázatai.

Itt fontos még megjegyezni a fenti felsorolás mellett, hogy az információs térben számos területen jelentkeznek új kockázatok, amelyek új kihívásokat is hoznak magukkal az alábbi területeken:

- ✓ kriptopénzek (kriptoeszközök) és a személyes adatok paradigmái,
- ✓ az anonimizálás kérdései, különös tekintettel a nagy adat és a mesterséges intelligencia kihívásaira (például telematikai rendszerekből származó „anonim” adatok személyhez kötődésének visszaállítása stb.);
- ✓ a blokklánc technológia (okosszerződések stb.) és a személyes adatok összefüggései;
- ✓ „civil” alkalmazásokban található személyes adatok felhasználása a katonai műveletek során (orosz-ukrán válság).

A kockázatok felsorolásából egyértelmű, nemzetbiztonsági kockázattal nemcsak a közigazgatás, a rend- és honvédelem, valamint a nemzetbiztonsági szolgálatok területén kell számolni, hanem a létfontosságú infrastruktúrák területén is. Azonban a

[118] Resperger István: Biztonsági kihívások, kockázatok, fenyegetések és ezek hatása Magyarországra 2030-ig.
Felderítő Szemle, 12. (2013), 3. 5–36. 5.; Resperger István*: A fegyveres erők megváltozott feladatai a katonai jellegű fegyveres válságok kezelése során.* Doktori értekezés. Budapest, Zrínyi Miklós Nemzetvédelmi
Egyetem, 2002. 45.

közelmúlt eseményei bemutatták, szinte nincs egyetlen olyan szektor sem, amely ne szembesülne olyan kihívásokkal, amelyek nemzetbiztonsági kockázatot hordoznak. Ráadásul a kockázatkezelés során a folyamatok minden szintjét meg kell vizsgálni mind a tevékenység, mind a humán erőforrás szempontjából.

Egy nemzetbiztonsági szolgálat kezeli

- ✓ *a saját állományának személyes adatait (nyílt és fedett állomány, ki hova van beosztva, mi tartozik a munkakörébe, milyen feladatok végrehajtásában vett részt és milyen eredménnyel, mikor volt beteg, hogyan alakulnak a juttatásai, hozzátartozóinak adatai stb.);*
- ✓ *a látókörébe került személyek személyes adatait (szervezet üzleti partnereinek, társszervezetek képviselőinek, társadalmi kapcsolatainak személyes adatai stb.);*
- ✓ *az együttműködők személyes adatait;*
- ✓ *ellenérdekeltségű szervezetek és személyek adatait;*
- ✓ *egyéb műveleti adatokat;*
- ✓ *beszállítók adatai;*
- ✓ *alvállalkozók adatai;*
- ✓ *egyéb be nem sorolható személyek adatai (oktatók, óraadók, szakértők stb.)*

Az adatvédelemmel kapcsolatos szabályok be nem tartása számtalan olyan „eredményt" hozhat, amely nemkívánatos a szervezet szempontjából, például:

- ✓ személyi állomány alapjogainak megsértése
  - megnövekvő fluktuáció,
  - adatvédelmi hatósági vizsgálatok,
  - munkaügyi perek,
  - negatív érzéssel távozó alkalmazottak bosszújának szinte beláthatatlan következményei,
  - szervezet működési hatékonyságának drasztikus csökkenése stb.
- ✓ személyes állomány adatai kiszivárognak („adatvédelmi incidens")
  - pszichikai manipuláció („social engineering") esélye exponenciálisan megnő,
  - fedett hírszerzők dekonspirálódhatnak,
  - operatív műveletek sérülnek stb.
- ✓ azoknak a személyeknek az alapjogai sérülnek, akik a szolgálatok látókörébe kerülnek;
  - törvénytelen eszközök használata miatti negatív kritika
  - perek,
  - nemzetközi szintű negatív visszhang stb.
- ✓ azoknak az adatai szivárognak ki, akik látókörbe kerültek
  - kudarcba fulladó küldetés,
  - diplomáciai vagy belföldi politikai incidens,
  - szélsőséges esetben tüntetések,
  - bojkott stb.
- ✓ kockázatok növekedése
  - általános szokássá válik a szabályok megszegése,
  - a hanyag ügykezelés elfogadott normává válik

- kiberterroristák kezére játszás a védelmi eszközök gyengesége miatt stb.

✓ szervezet reputációjának sérülése
- szakmai inkompetencia,
- jogsértő tevékenység,
- személyi állomány demoralizálódása stb.

✓ anyagi kihatások
- adatvédelmi hatósági bírságok,
- kártérítési fizetési kötelezettség,
- kiszivárgott adatok miatti azonnali elhárító tevékenység költségei (fedett ügynöki rendszer átszervezése, műveletek félbeszakítása stb.)
- megnövekedett költségek a nagy sajtóvisszhang miatt (a hírnév visszaállítása érdekében) stb.

Ezekben és más, hasonló esetekben mindig a körülmények ismeretében kell eldönteni, hogy a GDPR vagy az Infotv. hatálya alá tartozik az adott ügy. Ez különösen azért fontos, mert a két jogszabály eltérő jogosultságokat ad az érintetteknek és az alapelvek szempontjából is más követelményeket kell az adatkezelőnek teljesítenie például az átláthatóság területén.

A nemzetbiztonsági kockázatok és a személyes adatok összefüggésére a legjobb példa az ukrán-orosz katonai konfliktus során tapasztalható jelenség, mely során a szembenálló felek nagy mennyiségű személyes adatot hoznak nyilvánosságra az interneten. Tevékenységük során az ellenérdekelt felek a személyi állomány adatait (például név, lakcím stb.) publikálják, amelyek az alábbi kockázatokat rejtik:

- a konfliktus békés rendezése után a megszerzett adatokkal lehetősége nyílik arra egyes személyeknek, hogy vélt vagy valós sérelmükért bosszút álljanak;
- kiberbűnözői csoportok a megszerzett adatokkal további bűncselekményeket kövessenek el;
- a konfliktus békés rendezése után a megszerzett adatok segítésesével hatékonyabban lehet beszervezni ellenérdekeltségű személyeket stb.;
- a megszerzett nagymennyiségű adat segítségével célirányos katonai propagandát lehet végrehajtani a szembenálló fél személyi állománya ellen.

Ha a digitalizációs folyamatok közül ki szeretnénk ragadni egy példát az Infotv. és a GDPR elhatárolására, akkor erre kiválóan alkalmas a rendvédelmi szervezeteknél rendszeresített mobiltelefonokra telepített elektronikus levél kliensek.

Ebben az esetben az a helyes eljárás, ha a személyes elektronikus postafiókunkat (például Gmail) nem telepítjük a szolgálati telefonunkra, illetve a szervezetek által alkalmazott Exchange kiszolgálót egy másik készülékre telepítjük. Gyakorlatban viszont egyes esetekben az Android operációs rendszerrel ellátott eszközök csak Gmail-fiók telepítésével működnek üzemszerűen, így ezek alkalmazása nem kívánatos a rendvédelmi szervezeteknél. Megoldás lehet, ha ilyen esetben egy kizárólag erre a célra elkülönített Gmail-fiókkal hajtjuk végre a készülékregisztrációt, ennek azonban hátránya, hogy ilyen esetben egy rendvédelmi

dolgozóhoz minimálisan két privát fiók (GDPR) és egy szolgálati fiók (Infotv.) tartozik.

Kockázatcsökkentési módszerek

Az egyik legkézenfekvőbb kockázatcsökkentési módszer az, ha az adatkezelő nevében adatkezelést végző személyek ismerik azokat a szabályokat, amelyek (elviekben) meghatározzák a tevékenységüket. Adatvédelmi és adatbiztonsági tudatossággal, azaz a szabályok ismeretével és betartásával, valamint a változó körülményekre odafigyeléssel jelentősen csökkenthető az általános kockázat. Ennek természetesen előfeltétele, hogy a szervezetek körültekintően, saját jellegzetességeiket figyelembe véve alakítsák ki belső szabályzataikat és eljárásrendjeiket, szem előtt tartva olyan jogszabályok előírásait, mint például az Ibtv.[119] illetve a végrehajtására kiadott BM rendelet.[120] A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete egy Kézikönyvet[121] adott ki a BM rendelet alkalmazásához, melyben iparági jó gyakorlatokkal, illetve előremutató példákkal segíti az információbiztonsági felelősök munkáját. A Kézikönyvhöz van egy kiegészítés is, amely részletes védelmi intézkedések gyűjteménye.

A Kézikönyv és kiegészítése nemcsak az Ibtv. hatálya alá tartozó szervezeteknek képes segítséget nyújtani, hanem bárkinek, aki meg szeretné erősíteni a szervezete információbiztonságát, ezzel is csökkentve tevékenységének adatvédelmi és adatbiztonsági kockázatait.

[119] az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
[120] az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet
[121] Kézikönyv a 41/2015. BM rendelet alkalmazásához, https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/kezikonyv-a-41-2015-bm-rendelet-alkalmazasahoz/, utolsó letöltés 2022. 07. 09.

AZ ADATKEZELÉS ALAPJAI – AVAGY MIÉRT VAN SZÜKSÉGÜNK AZ ADATVÉDELMI JOG ISMERETÉRE?

Nem azért, mert még egy tantárgy, amit le kell sajátítani egy képzés során.

Nem azért, mert manapság divatos lelkes adatvédőnek lenni, mert erre fogékony környezetben lehet vele dicsekedni.

Nem azért, mert munkaköri kötelezettség és nem is azért, mert időnként felrémlik, mintha az Alaptörvényben lenne valami passzus az információs önrendelkezési jogról is.

Amikor a mi adatainkat kezelik

Napjainkban nincs se a privát, se a szakmai életünknek olyan szegmense, amelyben ne kezelnék mások az adatainkat. A „régen" megszokott papír alapú adatkezelések mellett a digitalizációs transzformáció hatása is elért minket, így lassan szinte minden mozdulatunk legalább egy digitális adatbázisban megjelenik, gyakran a saját kezdeményezésünkre még akkor is, ha erről fogalmunk sincs. Azonban a digitális eszközök mellőzése sem jelenthet megoldást, hiszen ezen eszközök nélkül jelentős hátrányt szenvednénk mind a magán, mind a szakmai életünkben.

Hol és kik kezelik az adatainkat?

Magánemberként

- ✓ *a szervízben kiolvastatjuk az autónk fedélzeti számítógépét;*
- ✓ *bekapcsoljuk a mobil telefonunkat és feljelentkezünk a szolgáltató hálózatára*
- ✓ *böngészőnk süti „cooki" beállításaiban;*
- ✓ *böngészőnkben tárolt sablonokban és jelszó kulcskarikákon;*
- ✓ *a különböző szolgáltatók jelszó kulcskarikáin (Apple vagy Google);*
- ✓ *iskolába járunk és/vagy gyermekünk jár iskolába,*
- ✓ *bejelentkezünk egészségügyi szolgáltatásokba,*
- ✓ *egészségmegőrzést segítő alkalmazást telepítünk az okos telefonunkra*
- ✓ *megállít bennünket a rendőr és erőteljesen érdeklődik alkoholos befolyásoltságunk mértékéről*
- ✓ *a háziállat tartáshoz szükséges eszközökön (okos nyakörv stb.)*
- ✓ *a COVID19 járvány vonatkozásában kezelt rendszereken (appokban),*
- ✓ *kormányzati ügyintézés során,*
- ✓ *vizet/gázt/villanyt fogyasztunk,*
- ✓ *hibás tartalmú igazolást állít ki számunkra a közműszolgáltató (ez is adatkezelés, még ha a nem túl jól sikerült adatkezelések közül)*
- ✓ *és még számtalan más esetben...*

Szakmai életünkben

- ✓ *belépünk a szolgálati helyünkre,*
- ✓ *mozgunk a munkahelyünkön felszerelt kamerarendszer kameráinak látószögében*
- ✓ *jelentést írunk,*
- ✓ *éves lövészeten veszünk részt,*
- ✓ *éves szabadságot szervezünk,*
- ✓ *illetményünk bérszámfejtésénél,*
- ✓ *a szolgálati gépjármű igénybevételénél,*
- ✓ *nemzetbiztonsági ellenőrzés során,*
- ✓ *nemzetbiztonsági ellenőrzés végzői vagyunk*
- ✓ *új munkakörbe helyeznek minket,*
- ✓ *külföldi vagy belföldi szolgálati útra megyünk (útlevél szám, foglalás, útiterv),*
- ✓ *használjuk a szolgálati helyünk számítógépét és a számunkra kiadott e-mail címet,*
- ✓ *humán ügyek intézése során,*
- ✓ *élelmezési anyag rendelése során (ételallergia, ételintolerancia),*
- ✓ *(éves) egészségügyi ellenőrzés,*
- ✓ *vendéglátóipari szolgáltatás igénybevétele a szolgálati helyen (kantin – pénzügyi adatok),*
- ✓ *béren kívüli juttatások igénybevétele (tanévkezdési támogatás, nevelési segély),*
- ✓ *temetéssel és születéssel kapcsolatos támogatások stb.*
- ✓ *és még számtalan más esetben…*

A gondolat is erőteljesen negatív érzést kelthet bennünk, miszerint a XXI. század harmadik évtizedében mind a privát, mind a szakmai életünk valójában nem más, mint egy végeláthatatlan adattömeg, amely feletti rendelkezési jogunknak már a részleges elvesztése (eltűnése) is akár önazonosságunk elvesztését (eltűnését) eredményezheti.

Példák adataink feletti rendelkezés elvesztésére

- ✓ *feltörik a közösségi médiás profilunkat és a nevünkben hamis posztokat jelentetnek meg vagy olyan posztokat lájkolnak, amilyeneket mi nem lájkolnánk*
- ✓ *zsarolóvírus miatt kikerülnek a pszichológusnál tett látogatásainkról készült jegyezetek, benne olyan adatokkal mint például szüleinkkel vagy testvérünkkel rossz kapcsolatunk, kicsapongó életmódunk, függőségünk, az általunk utált/megvetett személyek neve, főnökünkre tett megjegyzéseink stb.*
- ✓ *gyermekkori botlásunk napvilágra kerül*
- ✓ *tévedésből halottá nyilvánítható nak bennünket, melynek következtében évekig bizonygathatjuk különböző helyeken azt, hogy még élünk.*
- ✓ *tudtunk nélkül hitelt vesznek fel a nevünkre a személyes adatainkat felhasználva*
- ✓ *szolgálati helyünkön adatvédelmi incidens során kiszivárognak a személyes adataink és terepmunka helyett örökre egy, a figyelő tekintetektől távol eső irodába száműznek minket.*

Ezekben a történetekben a közös az, hogy áldozatként sérül az információs önrendelkezési jogunk, a történések pedig akár jelentős kárt, anyagi és erkölcsi veszteséget is okozhat nekünk.

Amikor mi kezeljük mások adatait

Azonban nemcsak a mi adatainkat kezelik mások, hanem mi is kezel(het)jük mások adatait, és nemcsak nekünk okozhatnak kárt inkompetens adatkezelők, hanem a mi cselekedetünk (mulasztásunk) is eredményezhet másoknak nemcsak időleges problémát, hanem súlyos erkölcsi vagy anyagi veszteséget is. És ahhoz, hogy adatkezelők legyünk nem szükséges az, hogy tudatában legyünk ennek a minőségünknek.

Kutatásunk során a megkérdezett személyek nagy része nem rendelkezett ismeretekkel arról, hogy ő mikor válik/válhat adatkezelővé, ahogy arról sem, hogy ő már jelenleg is – a GDPR alapján – adatkezelőnek minősül.

Amikor mi kezelünk adatokat magánemberként (és nem vonatkozik ránk a GDPR)

- ✓ *saját ingatlanunkat figyeljük úgy, hogy nem látunk át se más ingatlanára, se közterületre*
- ✓ *videófelvételt készítünk nagybátyánk harmadik esküvőjén nagynénénk második férjéről*
- ✓ *fedélzeti kamerát szerelünk az autónkba, mert tartunk attól, hogy legközelebb előttünk büntetőfékez egy agresszív sofőr*
- ✓ *feltöltünk egy fényképet az osztálytalálkozónkról a közösségi médiába*

Amikor mi kezelünk adatokat magánemberként (és a GDPR vonatkozik a tevékenységünkre)

- ✓ *videófelvételt készítünk nagybátyánk harmadik esküvőjén nagynénénk második férjéről és kirakjuk a Facebookra / Instagramra / TikTokra*
- ✓ *ingerült hangnemben levelezünk a gyermekünk osztályfőnökével a gyerekekről, majd ezt közzé is tesszük az osztály levelezőcsoportjában*
- ✓ *fedélzeti kamerát szerelünk az autónkba, mert tartunk attól, hogy legközelebb előttünk büntetőfékez egy agresszív sofőr, majd a felvételt kitesszük a youtube-ra, okuljon belőle mindenki.*

Amikor mi kezelünk adatokat szakmai életünkben (és a GDPR vonatkozik a tevékenységünkre)

- ✓ *szabadidőnkben/unalmunkban a céges laptopunkról végig böngésszük egy olyan személy közösségi médiás jelenlétét (Facebook, LinkedIn stb.), akivel munkakörünk miatt kerültünk kapcsolatba*
- ✓ *levelet írunk az üzleti partnerünk képviselőjének*
- ✓ *jelentést írunk a kollégánkról, meg arról, hogy mit kellett volna csinálnia akkor, amikor nem azt csinálta, amit valójában kellett volna neki.*

Ilyen és hasonló tevékenységekkel már be is lavíroztuk magunkat abba a világba, ahol a játékszabályok keretét az adatvédelmi jog határozza meg, legyen az akár a GDPR, akár az Infotv. Legyünk bármilyen óvatosak is, nem tudjuk elkerülni, hogy előbb vagy

utóbb ne vesszünk el a jogszabályok ingoványában úgy, hogy esélyünk se legyen onnan ép bőrrel kikecmeregni. Az adatvédelem földjén a csapdák száma végtelen és ragadozókból is van bőséges kínálat, legyen az pokoli szomszéd, ideges beosztott vagy még idegesebb főnök.

Az adatvédelmi jog vezértelte össznépi adatkezelős társasjáték földrajzi határokra tekintet nélkül sok-sok szereplőt terel össze egyetlen nagy ernyő alá. Olyanokat, akik több-kevesebb szakértelemmel saját érték- és érdekrendszerük mentén tevékenykednek, ám ugyanazzal a felelősséggel, és ugyan lehet, hogy a saját hibáink tekintetében elnézők vagyunk, azonban ha a mi adatainkat kezelik felelőtlenül mások, egy pillanatig sem jut eszünkbe mentesíteni őket a felelősség alól. Elfogadunk olyan kifogásokat, miszerint

- ✓ „nekem ezt soha nem tanították”,
- ✓ „mi közöm van hozzá”,
- ✓ „nem értem és nem is akarom megérteni”,
- ✓ „ezt a baromságot én nem csinálom”,
- ✓ „mit jogvédősködsz itt”, és egyébként is
- ✓ „ezt mindig így szoktuk csinálni”?

Kizárt. És ez nem véletlen.

Félresikerült adatkezelés következménye lehet

- ✓ *kiderülhetnek rólunk olyanok, amiket nagyon nem szeretnénk napvilágra hozni (munkakör, betegség, eltitkolt kapcsolatok, függőség, rovott múlt, pártállás, világnézet stb.),*
- ✓ *megsérülhetnek vagy akár visszaállíthatatlanul tönkre mehetnek a szakmai és az emberi kapcsolataink (bizalomvesztés, frusztráció, csalódás, harag, féltékenység, irigység, megvetés stb.)*
- ✓ *alacsonyabb beosztásba helyezhetnek a munkahelyünkön vagy ki is rúghatnak minket (nemcsak a presztízsünk van oda, hanem a megélhetésünk is),*
- ✓ *megcsapolhatják vagy akár teljesen le is üríthetik a bankszámlánkat (végképp oda a megélhetésünk), plusz hitelt vehetnek fel a nevünkben és elfelejtik visszafizetni*
- ✓ *becsületünkbe gázolhatnak, jó hírnevünket sárba tiporhatják (és nemcsak a mienket, hanem a közeli hozzátartozóinkét, szeretteinkét is),*
- ✓ *lehetetlenné tehetik a közösségi életünket*
- ✓ *ellophatják akár a személyazonosságunkat is (nevünkben adnak-vesznek a neten stb.), illetve olyan bűncselekmények gyanújába keverhetnek bennünket, amit nem követtünk el.*

A példákat folytathatnánk, a variációk száma a végtelen felé közelít.

Azonban nemcsak nekünk okozhatnak a felelőtlen adatkezelők rossz perceket, heteket vagy akár éveket is, ugyanerre mi is képesek lehetünk, ha mások adatait kezelve nem állunk a helyzet magaslatán. Feneketlen az a kút, amelybe belelökhetjük embertársainkat/munkahelyünket a szabályok be nem tartásával még akkor is, ha a rossz szándék írmagja sem található bennünk. Éppen ezért mindent meg kell tennünk annak érdekében, hogy legalább alapvető ismereteink legyenek a területen és

felismerjük, mikor érkezik el az a pillanat, amikor szakember (adatvédelmi tisztviselő) segítségét kell kérnünk. Azonban ahhoz, hogy tudjuk, közelít a baj, legalább az alapvető szabályokat ismernünk kell, különben hogyan ismernénk fel a veszélyt?

MI AZ AZ ADATKEZELÉS?

Ha nem szeretnénk kellemetlen meglepetéseket sem önmagunknak, sem pedig másoknak, legelőször is az adatkezelés fogalmával kell tisztában lennünk. Mert mi is az az adatkezelés?

Az adatkezelés

Mint már szó esett róla, az Európa Unió az adatvédelemmel kapcsolatban a nemzeti határokon átívelve egységesíti a tagállamokat és biztosítja a védelmet a területén élőknek származásuktól, vagyoni helyzetüktől függetlenül.

Az Európa Unió és a tagállamok által meghatározott keretek között adatkezelőként önállóan határozzuk meg az adatkezeléssel kapcsolatos tevékenységünk célját és eszközeit, az érintettek (akiknek az adatait kezelik) pedig abban bíznak, hogy mindeközben a jogszabályoknak megfelelően tesszük a dolgunkat. Ez mi jelent? Nemcsak az adatokra kell vigyáznunk, hanem figyelemmel kell lenniük az érintettek érdekeire, valamint a jogaikra és szabadságaikra is. Ráadásul, mint adatkezelést végző természetes személy máshol, más adatkezelésekben érintettként fogunk megjelenni, azaz míg az egyik helyen mi kezelünk adatokat és okozhatunk másoknak fejfájást, addig máshol a mi adatainkat kezelik mások. Mindezek alapján joggal várható el tőlünk, hogy miközben adatkezelőként járunk el, bele tudjuk magunkat helyezni az érintett cipőjébe is.

És el is érkeztünk az érdekek, jogok és szabadságok védelméhez. Így, többes számban, jogok és szabadságok.

Az, hogy kinek mi az érdeke még csak-csak tudjuk, de vajon mik azok a jogok és szabadságok? Ezeket az egyes tagállamok alkotmányai taglalják, uniós szinten pedig az Alapjogi Charta rendelkezik róluk. A hagyományos alapjogok (szólás- és sajtószabadság, véleménynyilvánítási szabadság, lelkiismereti szabadság meg a többi) mellett megtaláljuk alapjogként az információs önrendelkezés jogát is, amely biztosítja az egyének számára az adataikhoz való jogukat.

A GDPR – elismerve az adatvédelem komplex viszonyait – az érintettek jogainak és szabadságainak védelme érdekében bevezette az adatvédelmi tisztviselő (DPO)[122] intézményét. A DPO küldetése, hogy az adatkezelők munkáját segítve minél kevesebb gépzaj szűrődjön ki a gépházból. A „méreten aluli" adatkezelők nem kötelesek DPO-t alkalmazni, bizonyos esetekben azonban nélkülözhetetlen egy olyan szakember tudása, aki ismeri nemcsak az uniós rendeletet, hanem a hazai ágazati jogszabályokat, a jogértelmezési tendenciákat és a hatósági gyakorlatot is. A jogalkotó egyes esetekben kötelezi az adatkezelőket DPO kinevezésére, például a közhatalmi szerveket vagy egyéb, közfeladatot ellátó szerveket (kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat).

[122] „data protection officer"

Az adatvédelmi tisztviselő azonban nemcsak azért van, hogy az adatkezelést végzők munkáját segítse, hanem azért is, hogy az érintettek akár közvetlenül is fordulhassanak hozzá érdekeik, jogaik, valamint szabadságaik érvényesítése érdekében. Hiszen kitől mástól számíthatnának korrekt, érthető és mindenre kiterjedő tájékoztatásra, mint attól, aki a legjobban ismeri mind az adatkezelő tevékenységét, mind a vonatkozó jogszabályi környezetet? Éppen ezért az adatkezelésekről szóló adatkezelési tájékoztatók elengedhetetlen része az adatvédelmi tisztviselő elérhetősége, amennyiben rendelkezik ilyennel az adott adatkezelő.

Azonban semmit sem ér a papírra vetett szó, ha nincs mögötte olyan szankciórendszer, amely kikényszeríti ezen jogok és szabadságok tiszteletben tartását. Az adatvédelem hazai zászlóshajója a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH, továbbiakban: Hatóság)[123], amely állásfoglalásokkal, de akár bírság kiszabásával és egyéb szankciókkal (például adatkezelés megtiltásával, törlés elrendelésével) is igyekszik visszaterelni az adatkezelőket az általa jogszerűnek ítélt útra.

Az érintettek is felléphetnek az adatkezelők ellen, ha úgy vélik, sérelem érte őket. Panaszukkal és sérelmeikkel a Hatósághoz, illetve bírósághoz is fordulhatnak és akár kártérítést (sérelmi díjat) is követelhetnek a nekik kárt okozó adatkezelőtől.

Az adatkezelés fogalma

Az adatkezelés[124] a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a

- ✓ gyűjtés,
- ✓ rögzítés,
- ✓ rendszerezés,
- ✓ tagolás,
- ✓ tárolás,
- ✓ átalakítás vagy megváltoztatás,
- ✓ lekérdezés,
- ✓ betekintés,
- ✓ felhasználás,
- ✓ közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján,
- ✓ összehangolás vagy összekapcsolás,
- ✓ korlátozás,
- ✓ törlés, illetve megsemmisítés.

[123] https://naih.hu/
[124] GDPR 4. cikk 2. pont

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A rögzítést nem végző berendezések elhelyezése és a közvetített kép közvetlen megfigyelése hasonlít a megfigyelést végző személy (például a rendőr, a biztonsági őr, a munkahelyi vezető stb.) helyszíni jelenlétéhez, bár bizonyos fokig el is tér attól. Ma már a technika segítségével (például ráközelítéssel) ugyanis jóval szélesebb körű megfigyelésre is lehetőség van, mint a személyes jelenlétkor, így a közvetített képek megfigyelése ezekben az esetekben részletesebb ellenőrzést tesz lehetővé. Továbbá az élőképek közvetítése, illetve megfigyelése is általában valamilyen céllal történik, így egy egységes adatkezelési folyamat részelemének tekinthető, melynek következménye, hogy az adatkezelő az élőkép megtekintése alapján valamilyen döntést hoz. Ezért a személyes jelenlétet helyettesítő technikai megfigyelés, azaz a képek megismerése az általános adatvédelmi rendelet rendelkezései szerint csak abban az esetben nem minősül adatkezelésnek, ha a megfigyelés során az alkalmazott technika nem kínál lehetőséget arra, hogy a megfigyelést végző személy többletinformáció birtokába jusson az érintett természetes személlyel kapcsolatban.”[125]

„(…) azáltal, hogy a rendszer csak élőképet közvetít, az érintettek magánszférájába való beavatkozás jelentősen kisebb foka valósul meg, mint ha sor kerülne a személyes adataik rögzítésére.”[126]

[125] NAIH/2020/643/6, Budapest, 2020. július 17., https://www.naih.hu/files/NAIH-2020-643-hatarozat.pdf, utolsó letöltés: 2022. 07. 14.
[126] A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2022. évi tevékenységéről B/2589, 39.o.

A GDPR hatálya alá tartozó adatkezelések

A GDPR rendelkezéseit kell alkalmaznunk

- ✓ a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni (*tárgyi hatály*).

> ***Az izlandi adatvédelmi hatóság gyakorlatából***
>
> *Az izlandi adatvédelmi hatóság úgy döntött, hogy egy olyan e-mail állítólagos küldése, amelynek létezését a panasz során nem bizonyítják, nem tartozik a GDPR 2. cikke (1) bekezdésének tárgyi hatálya alá (azaz nem tekinthető személyes adatok kezelésének).*[127]

- ✓ a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem (*területi hatály*).
- ✓ az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére, ha az adatkezelési tevékenységek
  - a) áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy
  - b) az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve hogy az Unió területén belül tanúsított viselkedésükről van szó (*területi hatály*).
- ✓ a személyes adatoknak nem az Unióban, hanem olyan helyen tevékenységi hellyel rendelkező adatkezelő által végzett kezelésére, ahol a nemzetközi közjog értelmében valamely tagállam joga alkalmazandó.

Speciális szabályok vonatkoznak a bíróságok által végzett adatkezelési tevékenységekre. Az ő esetükben a GDPR szabályai alkalmazandók, azonban az igazságszolgáltatási tevékenységük keretében végzett adatkezeléseik esetén a felügyeleti hatóság (hazánkban: NAIH) nem gyakorolhat felügyeleti jogkört[128], tekintettel a bírói függetlenség követelményeire. Azonban, ha az adott adatkezelés nem a bíróság igazságszolgáltatási jogkörével kapcsolatos, a felügyeleti hatóság ugyanúgy eljárhat, mint bármely másik, a GDPR hatálya alá tartozó adatkezelő esetében.

Az Infotv. kiterjeszti a GDPR alkalmazandóságát olyan adatkezelésekre is, amelyek eredetileg nem tartoznak a GDPR hatálya alá,[129] azaz nem védekezhetünk azzal, hogy

[127] Ætluð vinnsla persónuupplýsinga hjá Símanum hf. og afgreiðsla á aðgangsbeiðni, Mál nr. 2020010598, https://www.personuvernd.is/urlausnir/aetlud-vinnsla-personuupplysinga-hja-simanum-hf.-og-afgreidsla-a-adgangsbeidni, utolsó letöltés: 2022. 07. 09.
[128] Hazánkban az érintettek panaszaikkal az Országos Bírósági Hivatalhoz fordulhatnak
[129] Lásd Infotv. 2.§ (4) bek.

csak papírhegyekben elveszve kezelünk adatot. Attól, mert a személyes adatokat részben vagy egészben sem kezeljük automatizált módon, illetve a nem automatizált módon kezelt adataink nem képezik valamely nyilvántartási rendszer részét, és nem is akarjuk ezeket nyilvántartási rendszer részévé tenni, még az adatkezelési tevékenységükben a GDPR szabályaira tekintettel kell lennünk.

A tagállamok

- ✓ a GDPR által megengedett esetekben konkrétabb rendelkezéseket vezethetnek be (pl. a munkajog területén),
- ✓ további feltételeket vagy külön korlátozásokat alkalmazhatnak (pl. biometrikus adatok kezelése),
- ✓ választási lehetőséggel élhetnek (pl. gyermekek számára nyújtott információs társadalommal kapcsolatos szolgáltatások esetén az életkor esetében),
- ✓ bizonyos adatkezelési célok esetében korlátozásokkal élhetnek pl. az érintetti jogok érvényesítésével kapcsolatban[130]
- ✓ meghatározott esetekben kivételeket állapíthatnak meg és szabályozhatnak (pl. véleménynyilvánítás szabadságához és a tájékozódáshoz való jog érvényesülése érdekében)

A személyes adatok vallási közösség általi kezelése a GDPR hatálya alá esik, ezen szervezeteken számonkéri a személyes adatok védelméhez fűződő jogok érvényesülését, ugyanis *„nem tekinthető az említett közösségek szervezeti autonómiájába való beavatkozásnak a minden személyt terhelő azon kötelezettség, hogy tiszteletben tartsa a személyes adatok védelmével kapcsolatos uniós jogi szabályokat”*.[131]

Nem a GDPR hatálya alá tartozó adatkezelések (kivételek)

A GDPR hatálya nem terjed ki

- az elhunyt személyek adatainak kezelésére (ezt részlegesen Magyarországon az Infotv. szabályozza[132])
- az anonim információkra, *„nevezetesen olyan információkra, amelyek nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható”*[133]
- az olyan személyes adatkezelésre, amely jogi személyekre, illetve amely különösen olyan vállalkozásokra vonatkozik, amelyeket jogi személyként hoztak létre, beleértve a jogi személy nevét és formáját, valamint a jogi személy elérhetőségére vonatkozó adatokat.[134]

[130] GDPR 23. cikk
[131] Jehovan todistajat ítélet, C-25/17, 74. https://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=HU&mode=lst&dir=&occ=first&part=1&cid=8796980, utolsó letöltés: 2022. 08. 30.
[132] Infotv. 25.§
[133] GDPR (26) preambulumbekezdés
[134] GDPR (14) preambulumbekezdés

A 29. cikk szerinti adatvédelmi munkacsoport gyakorlatából

„A jogi személyekre vonatkozó információt természetes személyekre „vonatkozónak" is lehet tekinteni saját jellemzői alapján, az e dokumentumban meghatározott feltételeknek megfelelően. Ilyen eset lehet, amikor a jogi személy neve természetes személy nevéből származik. Másik példa lehet a vállalati e-mail, amelyet rendes körülmények között egy adott alkalmazott használ, vagy egy olyan kicsi vállalkozásra (jogi értelemben inkább „tárgyra", mint jogi személyre) vonatkozó információ, amely jellemezheti tulajdonosának viselkedését. Mindezen esetekben, ahol a „tartalom", a „cél" vagy az „eredmény" feltétele lehetővé teszi, hogy a jogi személyre vagy vállalkozásra vonatkozó információt természetes személyre „vonatkozónak" tekinthessük, az információt személyes adatnak kell tekinteni, és az adatvédelmi szabályokat alkalmazni kell."[135]

Az Európa Bizottság gyakorlatából

„(...) az egyszemélyes gazdasági társaságokkal kapcsolatos információk személyes adatnak minősülhetnek, ha egy természetes személy azonosítását teszik lehetővé. A jogszabály minden olyan személyes adatra is alkalmazandó, amely természetes személyek szakmai tevékenységéhez kapcsolódik, például ha ezek a személyek egy vállalkozás vagy szervezet alkalmazottai, például az „utónév.családnév@vallalkozas.eu" típusú e-mail-címek vagy az alkalmazottak üzleti telefonszáma esetében."[136]

A magyar adatvédelmi hatóság (NAIH) gyakorlatából:

„Ha elfogadjuk, hogy egy tulajdonos esetén a jogi személyre vonatkozó, hitelkockázatot befolyásoló esemény ténye a természetes személyre vonatkozó információ is egyben, akkor a személyes adat minőség egy kétszemélyes korlátolt felelősségű társaság esetén is tagadhatatlanul fennállna. Ennek megfelelően nem lehetne a jogbiztonság, előreláthatóság és kiszámíthatóság követelményeinek megfelelően meghatározni, hogy pontosan mi is az a mennyiségi határ, amelytől kezdve a jogi személyre vonatkozó adat és a tulajdonosok közti kapcsolat túl távoli ahhoz, hogy az egyben személyes adatnak is minősüljön.

[135] A 29. CIKK ALAPJÁN LÉTREHOZOTT ADATVÉDELMI MUNKACSOPORT: 4/2007 vélemény a személyes adat fogalmáról, 01248/07/HU WP 136, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf, utolsó letöltés 2022. 08. 19.

[136] Az adatvédelmi szabályok vállalkozásokkal kapcsolatos adatokra is vonatkoznak? https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_hu, utolsó letöltés: 2022. 08. 19.

(…) a rendelet hatálya nem terjed ki az olyan személyes adatkezelésre, amely jogi személyekre, illetve amely különösen olyan vállalkozásokra vonatkozik, amelyeket jogi személyként hoztak létre."[137]

A GDPR nem alkalmazandó a személyes adatok kezelésére, ha azt

a) az uniós jog hatályán kívül eső tevékenységek során végzik

A német bírósági gyakorlatból

A GDPR 2. cikk (2) bekezdésének a) pontja szerint a rendelet nem alkalmazandó a személyes adatoknak az uniós jog hatálya alá nem tartozó tevékenység keretében történő kezelésére. Ezért a bíróság úgy ítélte meg, hogy a GDPR adójogi területen hozott rendelkezései csak a harmonizált adókra alkalmazandók, a természetes személyek jövedelemadóztatásának területén azonban nem, mivel e tekintetben az Európai Unió területén nincs megfelelő harmonizáció. A bíróság kifejtette továbbá, hogy a nemzeti jogalkotó nem terjesztette ki a GDPR 2. cikkében foglalt norma tárgyi alkalmazási körét a nem harmonizált adók területére, ezért a Bíróság a GDPR 15. cikke alapján megtagadta a kért hozzáférést.[138]

A francia legfelsőbb közigazgatási bíróság (Conseil d'Etat „CE") gyakorlatából

A CE úgy döntött, hogy a pszichiátriai kezelés alatt álló személyek személyes adatainak a hozzájárulásuk nélkül, a terrorista radikalizálódás megelőzése céljából történő kezelése a nemzetbiztonsággal és a honvédelemmel kapcsolatos adatkezelések közé tartozik, és ezért a GDPR 2. cikk (2) bekezdésének a) pontja értelmében nem tartozik az uniós jog hatálya alá.[139]

b) a tagállamok az EUSZ V. címe 2. fejezetének hatálya alá tartozó tevékenységek[140] során végzik (közös kül- és biztonságpolitika)

c) természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzik („háztartási adatkezelés")

A háztartási adatkezelések körének meghatározása esetében a leggyakrabban az EUB František Ryneš ítélete kerül szóba, mely szerint „*egy olyan*

[137] NAIH-740-8/2022, https://naih.hu/hatarozatok-vegzesek/file/538-az-egyszemelyes-ugyvedi-irodara-vonatkozo-nyilvanos-informaciok, utolsó letöltés: 2022. 08. 19.

[138] Kein Anspruch des Steuerpflichtigen auf Einsicht in die Einkommensteuerakte – Sachlicher Anwendungsbereich der DSGVO – Bindung des BMF an Gesetz und Recht, http://www.dbovg.niedersachsen.de/jportal/?quelle=jlink&docid=STRE202075040&psml=bsndprod.psml&max=true, utolsó letöltés 2022. 07. 09.

[139] Conseil d'État, 10ème – 9ème chambres réunies, 27/03/2020, 431350, https://www.legifrance.gouv.fr/ceta/id/CETATEXT000041785967/, utolsó letöltés: 2022. 07. 09.

[140] Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata és az Európai Unió Alapjogi Chartája, Brrüsszel, 2015. január 30., https://data.consilium.europa.eu/doc/document/ST-6655-2008-REV-8/hu/pdf

kamerarendszer működtetése, amely személyekről készített videófelvételt adatrögzítő eszközön – például merevlemezen – tárol végtelenített formában, és amelyet egy természetes személy azért szerelt fel a családi házára, hogy megvédje a háztulajdonosok tulajdonát, testi épségét és életét, a kamerarendszerrel végzett megfigyelés pedig közterületre is kiterjed, nem minősül olyan adatkezelésnek, amelyet e rendelkezés értelmében kizárólag személyes, illetve otthoni tevékenységek gyakorlása céljából végeznek." [141]

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A Hatósághoz nagy számban érkeztek olyan panaszok is, amelyben a panaszosok a szomszédjuk ingatlanán elhelyezett kamerákat panaszolták, miszerint az az ő ingatlanukon történteket is rögzíti (NAIH/2018/3550/V.). A Hatóság az ilyen jellegű beadványok megválaszolása során azt hangsúlyozta, hogy amennyiben az üzemelő kamera úgy van beállítva, hogy csak azon az ingatlanon történteket rögzíti, amelyen a kamerát elhelyezték, úgy az adatkezelésre nem vonatkoznak a GDPR rendelkezései, amint azonban a más ingatlanán vagy közterületen történteket is rögzíti, nem alkalmazandó a kivételszabály és az adatkezelő köteles megfelelni a GDPR által támasztott követelményeknek."[142]

A GDPR is nyújt kapaszkodót ahhoz, hogy eldöntsük, mi számít háztartási adatkezelésnek és mi nem, eszerint „*ez a rendelet nem alkalmazandó a személyes adatoknak a természetes személy által kizárólag személyes vagy otthoni tevékenység keretében végzett kezelésére, amely így semmilyen szakmai vagy üzleti tevékenységgel nem hozható összefüggésbe. Személyes vagy otthoni tevékenységnek minősül például a levelezés, a címtárolás, valamint az említett személyes és otthoni tevékenységek keretében végzett, közösségi hálózatokon történő kapcsolattartás és online tevékenységek. E rendeletet kell alkalmazni azonban azokra az adatkezelőkre és adatfeldolgozókra, akik a személyes adatok ilyen személyes vagy otthoni tevékenység keretében végzett kezeléséhez az eszközöket biztosítják."*[143]

Az osztrák bírósági gyakorlatból

A bíróság álláspontja szerint

- ✓ *a GDPR 2. cikk (2) bekezdésének c) pontja szerinti háztartási kivétel a nem nyilvános Facebook-oldalakra vonatkozik, amikor is a címzettek köre valószínűleg korlátozott. A GDPR (18) preambulumbekezdése kifejezetten említi a közösségi hálózatok*

[141] C-212/13., ECLI:EU:C:2014:2428, https://curia.europa.eu/juris/document/document.jsf;jsessionid=3B98750B11B932A5C1456CBC7893397A?text=&docid=160561&pageIndex=0&doclang=hu&mode=lst&dir=&occ=first&part=1&cid=3518876, utolsó letöltés 2022. 08. 19

[142] A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2018. évi tevékenységéről, B/4542, Budapest, 2019, 24.o. https://naih.hu/files/Beszamolo-2018-MR.PDF, utolsó letöltés 2022. 07. 09.

[143] GDPR (18) preambulumbekezdés

használatát és az online tevékenységeket az ilyen tevékenységekkel összefüggésben, a szabályozás célja pedig az egyénekre háruló szükségtelen terhek elkerülése.

- ✓ *az állam szabályozási jogkörének ott kell megszűnnie, ahol az adatok kezelése magánjellegű kontextusban, tehát az általános személyiségi jog gyakorlása során történik. A „kizárólag megfogalmazás alapján a vegyes, azaz a magán- és a szakmai felhasználás is a GDPR hatálya alá tartozik.*
- ✓ *a közösségi hálózatok használata csak akkor esik a háztartási kivétel alá, ha az a felhasználók egy bizonyos csoportjára korlátozódik. Ez a kivétel nem alkalmazható abban az esetben, amint az adatokat nyilvánosan hozzáférhetővé teszik az interneten (mint például magánjellegű családfa online közzététele).*
- ✓ *a háztartási kivétel nem vonatkozik a nyilvános Facebook-oldalakra.*[144]

d) az illetékes hatóságok bűncselekmények megelőzése, nyomozása, felderítése, vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzik, ideértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését [lásd (EU) 2016/680 irányelv, illetve Infotv.].

A tagállamok az (EU) 2016/680 irányelv szerint az illetékes hatóságokat megbízhatják olyan egyéb feladatokkal is, amelyeknek ellátása nem feltétlenül a bűncselekmények megelőzése, nyomozása, felderítése vagy a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása, illetve nem a közbiztonságot fenyegető veszélyekkel szembeni védelem és e veszélyek megelőzése céljából történik, ebben az esetben a személyes adatoknak az említett egyéb célokból történő, egyébiránt az uniós jog hatálya alá tartozó kezelése a GDPR hatálya alá tartozik.[145]

A spanyol adatvédelmi hatóság (AEPD) gyakorlatából

A Covid-19 járványra tekintettel a Belügyminisztérium Nemzetbiztonsági Igazgatósága iránymutatást adott ki a rendőri erők számára a hírek és a közösségi hálózatok megfigyelésére annak érdekében, hogy kiszűrjék az álhíreket és a félretájékoztatást, valamint megakadályozzák egyes szereplők társadalmi feszültségkeltését. Az iránymutatás célja a félretájékoztatás hatásainak megelőzése, illetve minimalizálása olyan hálózatok és weboldalak figyelemmel kísérésével, ahol hamis üzeneteket és a társadalmi stressz fokozására irányuló információkat terjesztenek.

[144] 6Ob56/21k, https://www.ris.bka.gv.at/Dokumente/Justiz/JJT_20210623_OGH0002_0060OB00056_21K0000_000/JJT_20210623_OGH0002_0060OB00056_21K0000_000.pdf, utolsó letöltés 2022. 07. 25.
[145] GDPR (19) preambulumbekezdés

Az iránymutatás szerint a rendőri erők csak ezen célokkal és elvekkel összhangban avatkozhatnak be, illetve személyes adatok kezelésére csak akkor kerül sor,

- ✓ *ha bűncselekményre utaló jelek állnak fenn, összhangban a LED rendelkezéseivel*
- ✓ *ha a tevékenységek nemzetbiztonsági vonatkozásúak, összhangban az államtitkokra és a minősített ügyekre vonatkozó nemzeti jogszabályokkal.*

Az AEPD vizsgálatot indított annak ellenőrzésére, hogy az iránymutatásban foglaltak megfelelnek-e a személyes adatok kezelésére vonatkozó jogszabályi előírásoknak. A Nemzetbiztonsági Igazgatóság az AEPD-nek adott válaszában kijelentette, hogy nem gyűjtenek személyes adatokat, hanem csak a közösségi hálózatokból származó hírek vagy nyilvános információk napi megfigyelését végzik, ahol az összegyűjtött információk olyan nyilvános jellegű adatokra vonatkoznak, amelyeket a szerzők a közösségi hálózatokon és a nyilvános médián keresztül osztanak meg, és amelyek elsősorban a kommunikáció tartalmából és a terjesztés médiumából állnak. A híreket a Guardia Civil szakosodott tisztjei böngészik és anonim profilokat hoznak létre a közösségi hálózatok, például a Twitter, a Facebook, az Instagram, a Badoo és más weboldalak megfigyelésére, ezt követően pedig olyan témákban készítenek jelentéseket, mint a kiberbűnözés, a kiberterrorizmus, a hacktivizmus, a kibertámadások és a félretájékoztatások. Amennyiben bűncselekményre utaló jelek merülnek fel, bizonyítékokat gyűjtenek.

Az AEDP arra a következtetésre jutott, hogy nem történt sem a GDPR 2. cikkének, sem a LED rendelkezéseinek megsértése, mivel a személyes adatok kezelése nem történt és nem volt bizonyíték arra, hogy jogellenes adatkezelésre került volna sor (ártatlanság vélelmének elve).[146]

e) uniós intézmények, szervek, hivatalok és ügynökségek végzik [lásd (EU) 2018/1725 rendelet[147]]

Az európai adatvédelmi biztos (EDPS) gyakorlatából

2022. január 3-án az EDPS arra utasította az Europolt, hogy törölje azokat az egyénekre vonatkozó adatokat, akiknek nincs megállapított

[146] AEPD Procedimiento Nº: E/03783/2020, https://www.aepd.es/es/documento/e-03783-2020.pdf, utolsó letöltés 2022. 07. 09.

[147] Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről, https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32018R1725&from=HU

kapcsolata bűncselekményekkel.[148] *Az intézkedés előzménye, hogy az Europol a szükségesnél hosszabb ideig őrizte meg ezeket az adatokat, ellentétben az adatok minimalizálására és tárolásának korlátozására vonatkozó, az Europol-rendeletben foglalt elvekkel.* [149]

f) tagállamok nemzetbiztonsági céllal végzik.

Emberi Jogok Európai Bíróság gyakorlatából

„Konkrétabban a titkos megfigyeléssel kapcsolatos ügyekre vonatkozóan a Bíróság viszonylag rugalmasan viszonyul a sértetti státusz elismerésének kérdéséhez. Ami azt a feltételt illeti, hogy a beavatkozásnak „a törvénnyel összhangban„ kell lennie, a Bíróság úgy véli, hogy a jognak, mind a hozzáférhető, mind az előrelátható jognak viszonylag részletesnek kell lennie. A Bíróság különös hangsúlyt fektet a megfigyelést és a nyilvántartások vezetését kísérő biztosítékokra. Ami a demokratikus társadalomban a szükségesség feltételét illeti, a Bíróság mérlegeli az alperes államnak a nemzetbiztonsági védelméhez fűződő érdekét a kérelmező magánéletének tiszteletben tartásához való jogának megsértése súlyosságával szemben, a szigorú szükségességet a gyakorlatban úgy határozzák meg, hogy a visszaélések elleni megfelelő és hatékony garanciákat és legalább végső soron az igazságügyi hatóságok, vagy legalábbis független ellenőrző szervek általi felügyeletet követel meg (Klass és társai kontra Németország).

Egy „informátor ügyében, aki jogellenes titkos megfigyeléseket fedett fel (Bucur és Toma kontra Románia), a Bíróság úgy ítélte meg, hogy a nyilvánosságra hozott információk közvetlenül érintik a civil társadalmat, mivel bárki lehallgathatja a telefonját. Továbbá, mivel ez az információ magas rangú tisztviselők által elkövetett visszaélésekhez kapcsolódik, és az állam demokratikus alapjait érinti, ezek nagyon fontos kérdések voltak, amelyek politikai vitát váltottak ki, és amelyekről a nyilvánosságnak jogos érdeke fűződik ahhoz, hogy értesüljön. Ezért meg kellett vizsgálni, hogy az információ titkosságának megőrzéséhez fűződő érdek felülkerekedik-e azon közérdeken, hogy megtudják, hogy jogellenes telefonlehallgatás történt.”[150]

[148] EDPS orders Europol to erase data concerning individuals with no established link to a criminal activity, Press Release, https://edps.europa.eu/press-publications/press-news/press-releases/2022/edps-orders-europol-erase-data-concerning_en

[149] Az Európai Parlament és a Tanács (EU) 2016/794 rendelete (2016. május 11.) a Bűnüldözési Együttműködés Európai Uniós Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0794&from=HU

[150] European Court of Human Rights, Research Division: National security And European case-law, 2013.
https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf

Nem mindig könnyű egyértelmű határokat húzni a különböző rendszerek között, például

- ✓ a bűnözés elleni rendőri fellépés,
- ✓ a rend biztosítását célzó rendőri fellépés,
- ✓ a rendőrség és más hatóságok belső biztonság, közbiztonság és nemzetbiztonság érdekében tett intézkedése, valamint
- ✓ e fellépések és az Unió terrorizmussal, az uniós missziók feladataival és a nemzetközi biztonsággal kapcsolatos fellépése között.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

(háztartási adatkezelés és a GDPR hatálya alá tartozó adatkezelés elhatárolása)
A Kérelmező sérelmezte, hogy a Kérelmezett titokban készített, majd egy Facebook csoportban közzétett egy felvételt egy beszélgetésről, amelyen a Kérelmező személyes és különleges adatainak minősülő információk hangoztak el. A Kérelmezett a felvételt három másik szülőnek is e-mailen továbbította.
A felvétellel végzett adatkezelés két különböző adatkezelési műveletből állt. Az első művelet a felvétel rögzítése, míg a második művelet a felvétel közlése volt, ez utóbbi pedig két különböző formában is megvalósult, amikor a Kérelmezett először a csoportban osztotta meg a felvételt, majd pedig e-mailen küldte el három személy számára.

A felvétel rögzítésével kapcsolatban a Hatóság megállapította, hogy az mindaddig, amíg tisztán magáncélt szolgál, azaz, ahogyan arra a Kérelmezett is hivatkozott, a beszélgetésen elhangzottak felidézését segíti a Kérelmezett számára, addig a felvétel elkészítése az úgynevezett „háztartási adatkezelés" kategóriájába tartozik, és a GDPR nem alkalmazandó rá.

Abban a pillanatban azonban, ahogy a Kérelmezett a közte és a Képviselő, valamint az óvodavezető között létrejött beszélgetést tartalmazó felvételt további személyek számára hozzáférhetővé tette – ezáltal megismerhetővé téve a Kérelmező személyes és különleges személyes adatait –, a rögzítést jellemző magánjelleg, vagyis a kizárólagosan saját érdek megszűnt. Ebből fakadóan a Hatóság álláspontja szerint a felvétel megosztása túlmutat a GDPR alkalmazása alóli kivételt jelentő háztartási adatkezelés fogalmán és a GDPR hatálya alá tartozik.[151]

[151] NAIH-1743/2021. sz. határozat

HOGYAN KERÜLHETÜNK BELE EGY ADATKEZELÉSBE?

Érintettként nincs mindig lehetőségünk eldönteni, részesei kívánunk-e lenni egy adott adatkezelésnek vagy sem.

Hogy kerülhetünk bele egy adatkezelésbe?

- ✓ *jogszabály írja elő függetlenül attól, hogy azt akarjuk vagy sem*
  - *az újszülöttek bekerülnek a népességnyilvántartásba*
  - *ha fizetést kapunk, az azzal kapcsolatos adatszolgáltatást a kifizetőnek teljesítenie kell az adóhatóság felé.*
- ✓ *közfeladat ellátása vagy közhatalmi tevékenység során az adatkezelő erre hivatkozva kezeli az adatainkat*
  - *iskolában az osztályfőnök nyilvántartja szülőként a kapcsolattartási adatainkat*
  - *a hulladékelszállító cég kezeli az ingatlanok számára kiadott kukákkal kapcsolatos adatokat, az áramszolgáltató pedig az áramfelhasználásunkat számlázza ki nekünk.*
- ✓ *szerződő félként kerülünk be az adatkezelésbe*
  - *bútort rendelünk, a vállalkozó pedig nyilvántartja az adatainkat, milyen szekrényt akarunk és milyen névre kérjük a számlát*
  - *hűtőgépet veszünk és a kereskedő cég házhoz szállítja azt az általunk megadott címre*
  - *esküvőnkről hivatásos fotós felvételeket készít.*
- ✓ *valakinek a jogos érdeke alapján kerülünk bele az adatkezelésbe*
  - *a Munka törvénykönyvének felhatalmazása alapján a munkáltatónk ellenőrzi, hogyan használjuk a céges e-mail fiókot, vagy szolgálati telefonunkat*
  - *szabadságunk alatt az elöljáró az arra illetékes személlyel kinyittatja a szekrényünket, mert benne felejtettük az uzsonnánkat és megbüdösödött*
  - *szolgálati helyünkön elektronikus beléptető rendszer működik, amelyet minden munkanapunkon kénytelenek vagyunk használni*
  - *a bevásárlóközpont kamerarendszert üzemeltet, ami minket is felvesz, amíg barátainkkal elfogyasztjuk a pizzánkat.*
- ✓ *hozzájárulunk az adataink kezeléséhez*
  - *feliratkozunk hírlevél szolgáltatásra*
  - *hozzájárulunk, hogy egy adott honlapra kitegyék a fényképünket*
  - *szeretnénk egy tengerparti nyaralást, ezért hozzájárulunk, hogy részt vegyünk egy fogyasztásösztönző nyereményjátékban*
  - *hozzájárulunk a sütikhez egy honlapon.*
- ✓ *az is előfordulhat, hogy az életünk múlik azon, hogy gyorsan orvosi segítséget kapjunk, ám nem vagyunk olyan állapotban, hogy hozzájáruljunk az adataink kezeléséhez. Ilyen helyzetben a sürgős segítségnyújtás érdekében kezelhetőek az adataink, hiszen aki segíteni akar nekünk, annak ki kell hívnia a mentőket és tájékoztatnia kell őket mindenről, amit csak tud a balesetünkről és az állapotunkról.*

Milyen lehetőségeink vannak, ha már bekerültünk egy adatkezelésbe?

- ✓ amikor jogszabály kötelezése alapján kezelik az adatainkat, nincs választásunk, akár akarjuk, akár nem, bekerülünk az adatkezelésbe és ott is maradunk mindaddig, amíg az adatkezelés feltételei fennállnak
    - veszünk egy kutyát, ebben az esetben bekerülünk az erre felhatalmazott hatóság által üzemeltetett ebnyilvántartásba
    - útlevelet igénylünk
    - ingatlant vásárlunk
- ✓ közfeladatként ellátott szolgáltatást veszünk igénybe és emiatt kell a jogszabályban meghatározott, illetve a szolgáltatás igénybevételéhez egyébként szükséges adatokat szolgáltatnunk (az ilyen esetekben tiltakozhatunk az adataink kezelése ellen)
    - az iskola nyilvántartja a gyermekünk és szülőként a mi adatainkat
    - a vízművek nyilvántartja a fogyasztásunkat
    - a kórház udvarán felvesz minket egy kamera miközben elesünk
- ✓ szerződést kötünk és ezen szerződés megkötése és teljesítése érdekében kezelik az adatainkat, vagy a szerződés előkészítése érdekében ajánlatot teszünk (ez esetben az adatszolgáltatásunk elmulasztása a szerződés előkészítését, megkötését vagy teljesítését meghiúsíthatja)
    - rendelünk pizzát, de nem adjuk meg a házhoz szállításhoz a címünket
    - járatunk egy horgászmagazint, de elköltöztünk és elfelejtettük megmondani az új címünket
- ✓ hozzájárulunk az adataink kezeléséhez (mert az jó nekünk, például valamilyen előnyt remélünk). Ez esetben ezt a hozzájárulást bármikor ingyenesen visszavonhatjuk, azaz saját döntésünk alapján kiléphetünk az adatkezelésből.
    - feliratkozunk hírlevélre
    - hozzájárulunk, hogy szerepeljünk a szervezetünk imázsfilmjében
- ✓ egyszer csak bent találjuk magunkat egy jogos érdekre hivatkozó adatkezelésben. Ez esetben tiltakozhatunk az adataink kezelése ellen, az adatkezelőnek pedig figyelembe kell vennie ezt a tiltakozást. Amennyiben helyt ad a tiltakozásunknak, meg kell szüntetnie a tiltakozásunkkal érintett adatkezelést, ha pedig elutasítja, meg kell tudni indokolnia ezt a döntését.
    - a plázában vásárlás közben felvesz minket a kamera
    - megszondáztatnak a munkahelyünkön.

Jogszabályok

GDPR

- ✓ Adatkezelés fogalmának meghatározása [GDPR 4. cikk 2. pont]
- ✓ Tárgyi hatály [GDPR 2. cikk, (14), (15), (16), (17), (18), (19), (20), (21) preambulumbekezdések]
- ✓ Területi hatály [GDPR 3. cikk, (22), (23), (24), (25) preambulumbekezdések]
- ✓ Infotv. 2.§ (2) bekezdés

AZ ADATVÉDELEM ALAPELVEI

Az adatvédelem szabályai – különös tekintettel a technikai fejlődésre – időről időre módosulnak, ám az alapelvek több évtizede nem változtak gyökeresen bizonyítva, kiállják az idő próbáját. Elmondhatjuk, hogy a több, mint harminc éve meghatározott és lényeges elemeikben ma is változatlan és irányadó alapelvek szükségesek, valamint a gyakorlatban jól alkalmazhatók a technikai, gazdasági és társadalmi változásokra tekintettel is és a GDPR 5. cikkének (1) és (2) bekezdése sem kötelezte az adatkezelőket szemléletváltásra.

Az alapelvek nem önálló szigetek – tartalmuk összeér, és nagyon gyakran előfordul, hogy szorosan összefüggenek egymással. Ha például már nem kellenek az adatok, de még mindig nem semmisítettük meg azokat, akkor megsértettük a célhoz kötöttség és a korlátozott tárolhatóság elvét is, ha pedig az adattakarékosság elvébe ütközünk, akkor valójában a célhoz kötöttséget sem tiszteltük olyan mértékben, mint ahogy elvárható lett volna tőlünk.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A Hatóság tehát a kezelt adatok körének vizsgálata során összefoglalva arra a megállapításra jutott, hogy az Egyetem az adatkör meghatározásakor megsértette a GDPR 5. cikk (1) bekezdés a) és b) pontjait, illetve nagymértékben megsértette a GDPR 5. cikk (1) bekezdés c) pontját.

Több igazolás/okmány esetén nem egyértelmű, hogy azok kezelése mely körülmény alátámasztásához szükséges, illetve több bekért igazolás/okmány esetén megállapítható volt, hogy azok kezelése nem szolgál egyértelmű és jogszerű célt, vagy az adott cél teljesítéséhez nem szükséges.

Nagymértékben jogsértő a teljes okmányok (teljes albérleti szerződés, teljes bontó ítélet, teljes születési anyakönyvi kivonat, teljes halotti anyakönyvi kivonat, teljes lakcímkártya, teljes személyazonosító igazolvány) másolatának bekérése, anélkül, hogy az Egyetem mérlegelte volna, hogy az okmány milyen adatkört tartalmaz, és szükséges-e valamennyi adat kezelése vagy elegendő helyette az okmány kivonatának benyújtása.

A Hatóság továbbá úgy ítélte meg, hogy az Egyetem nem mérlegelte kellő gondossággal, hogy mely okmányok, illetve igazolások benyújtása szükséges mindenképp, azaz nem törekedett az adatminimalizálásra, hanem az jelent meg a gyakorlatában, hogy minden igazolni kért körülmény biztosan alá legyen támasztva, akkor is, ha esetleg adott körülmény igazolása így szükségtelenül plusz adatkör kezelésével járt együtt."[152]

Amennyiben személyes adatokkal foglalkozunk, a GDPR alapelveit egyfajta kályhának is tekinthetjük, ahova a legkülönfélébb jogértelmezési problémáinkra

[152] NAIH/2020/54/4. https://www.naih.hu/hatarozatok-vegzesek?download=325:1-rendszeres-szocialis-osztondijakkal-kapcsolatos-adatkezeles-a-budapesti-muszaki-es-gazdasagtudomanyi-egyetemen-modositasokkal-egyseges-szerkezetben, utolsó letöltés 2022. 08. 21.

választ keresve mindig vissza-visszatérhetünk. És nem utolsó sorban jó, ha tudjuk, a felügyeleti hatóságok „csupán" alapelv sértés esetén is kiszabhatnak bírságot, különösen, ha nemcsak egyet, hanem egyszerre többet is sikerül megsértenünk.

A finn adatvédelmi hatóság (Tietosuojavaltuutetun toimisto) gyakorlatából

Az adatvédelmi hatóság megállapította, hogy egy biztosítótársaság megsértette többek között a tisztességes eljárás, az adattakarékosság, valamint az integritás és bizalmas jelleg elvét, amikor a biztosító felelősségének megállapítása érdekében az érintett teljes orvosi kartonját bekérte az egészségügyi szolgáltatótól.

Egy biztosítótársaság arra kérte az élet- vagy egészségbiztosítást igénylő érintetteket, hogy írjanak alá egy olyan általános nyilatkozatot, amely felhatalmazza a biztosítótársaságot arra, hogy egészségügyi információkat szerezzen be közvetlenül az érintettek egészségügyi szolgáltatóitól. A biztosítónak ezekre az adatokra a kérelem benyújtásának szakaszában a kockázat meghatározásához volt szüksége, valamint a későbbiekben a felelősségének meghatározásához akkor, amikor az érintettek kártérítést igényeltek. Egyes esetekben a biztosító ezt az általános felhatalmazást arra használta fel, hogy egy meghatározott időszakra vonatkozóan az érintett teljes egészségügyi dokumentációját bekérje.

Az adatvédelmi hatóság megállapította, hogy

- ✓ *a biztosító nem hivatkozhatott arra, hogy az adatok szerződés teljesítéséhez szükségességek, mivel az egészségügyi adatok a személyes adatok különleges kategóriáihoz tartoztak, azok kezelése esetében pedig a GDPR nem tartalmaz „szerződéses szükségességet", mint hivatkozható kivételt [9. cikk (2) bekezdés].*
- ✓ *a biztosító nem hivatkozhatott az általános érvényű meghatalmazásra sem, mivel a GDPR 15. cikke szerinti hozzáférési jog célja – többek között – az adatkezelés jogszerűségének és az adatok pontosságának ellenőrzése. A biztosító azonban ezen hozzáférési jogra hivatkozva megszerzett személyes adatokat a saját kockázatának és felelősségének meghatározása céljából kezelte, ez pedig ellentétes a célhoz kötöttség elvével. Ezen túlmenően a meghatalmazás formanyomtatványának megfogalmazása nem tette egyértelművé és érthetővé az érintettek számára, hogy a biztosítónak meghatalmazást adnak az érintetti hozzáférési joguk gyakorlására.*
- ✓ *a biztosító az érintettek kifejezett hozzájárulására támaszkodhat [9. cikk (2) bekezdés a) pont], de csak abban az esetben, ha az megfelel az érvényességi kritériumoknak. Az érvényes hozzájárulás többek között megköveteli, hogy az érintettek részletes tájékoztatót kapjanak arról, hogy pontosan milyen információkat gyűjtenek róluk, és azokat az adatkezelő milyen konkrét célokra használja fel. A biztosító formanyomtatványa azonban az adatok és az egészségügyi szolgáltatók meghatározatlan körére vonatkozott, így az eljáráskori formájában nem volt elég konkrét ahhoz, hogy érvényes és kifejezett hozzájárulásnak minősülhessen.*
- ✓ *az érintettek számos különböző okból állhatnak kapcsolatban az egészségügyi szolgáltatókkal, és nem minden információ releváns a biztosítótársaságok kockázatának és felelősségének meghatározása*

szempontjából. Ezért az érintett teljes egészségügyi dokumentációjának az egészségügyi szolgáltatóktól való bekérése sértette a tisztességes eljárás, az adattakarékosság és az integritás és bizalmas jelleg elvét, valamint a beépített és alapértelmezett adatvédelmet [GDPR 25. cikk (2) bekezdés].

Az adatvédelmi hatóság javasolta, hogy

- ✓ *ha egy biztosítótársaság egy személy egészségügyi adatait kikéri az egészségügyi szolgálatoktól, a kérést csak a biztosítótársaság felelősségének értékeléséhez szükséges konkrét esetre, betegségre vagy tünetre vonatkozó információkra kell korlátoznia, továbbá*
- ✓ *a biztosítótársaságnak fel kell mérnie, hogy milyen időszakra vonatkozóan szükséges az információkérés.*[153]

[153] Insurance companies have gathered excessive amounts of health information, https://tietosuoja.fi/-/tietosuojavaltuutettu-vakuutusyhtiot-keranneet-terveystietoja-tarpeettoman-laajasti?languageId=en_US, utolsó letöltés 2022.08.20

Jogszerűség, tisztességes eljárás és átláthatóság

„Jogszerűség, tisztességes eljárás és átláthatóság” elve alapján az adatkezelést jogszerűen és tisztességesen, valamint az érintettek számára átlátható módon kell végeznünk.

Ahhoz, hogy a személyes adatok feldolgozása jogszerűnek minősüljön, összhangban kell állnia a jogszabályokkal, jogszerű célt kell szolgálnia, valamint a cél eléréséhez szükségesnek és arányosnak kell lennie egy demokratikus társadalomban.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Jogsértő eszközzel eleve nem lehet jogszerű adatkezelést végezni, de jogszerű eszközökkel a többi feltételtől – cél, jogalap stb. – függően lehet jogszerű vagy jogszerűtlen az adatkezelés.”[154]

Az EDPB iránymutatása alapján[155] a jogszerűség fő beépített és alapértelmezett elemei a következők lehetnek:

- ✓ az adatkezelésünkre a megfelelő jogalapot alkalmazzunk (relevancia) és különböztessük meg az egyes adatkezelési tevékenységek esetében alkalmazott jogalapokat (differenciálás).
- ✓ az általunk választott jogalap egyértelműen az adatkezelésünk meghatározott céljához kapcsolódjon.
- ✓ ahhoz, hogy jogszerű legyen, az adatkezelésünknek szükségesnek és feltétel nélkülinek kell lennie.
- ✓ az érintettek számára biztosítsunk lehető legnagyobb mértékű autonómiát a személyes adataik feletti ellenőrzésük tekintetében (a hivatkozott jogalap keretein belül).
- ✓ az érintettek hozzájárulásának önkéntesnek, konkrétnak, megfelelő tájékoztatáson alapulónak és egyértelműnek kell lennie és fordítsunk külön figyelmet arra, hogy a 18 éven aluli személyek képesek-e előzetes tájékoztatáson alapuló hozzájárulást adni.
- ✓ amennyiben hozzájárulás az adatkezelésünk jogalapja, a hozzájárulás visszavonását is lehetővé kell tennünk. A visszavonásnak ugyanolyan egyszerűnek kell lennie, mint a hozzájárulás megadásának, különben a hozzájárulási mechanizmusunk nem felel meg a GDPR-nak.
- ✓ amennyiben az adatkezelésünk jogalapja jogos érdek, mérlegeljük a különböző érdekeket, külön figyelmet fordítva a kiegyensúlyozatlan erőviszonyokra, különösen a 18 év alatti személyek és más kiszolgáltatott csoportok (például munkavállalók) esetében. Az érintettekre gyakorolt kedvezőtlen hatás mérséklésére léptessünk életbe intézkedéseket és garanciákat.

[154] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: 2022. 07. 17.
[155] 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről 2.0 változat, Elfogadás időpontja: 2020. október 20., https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_hu.pdf, utolsó letöltés 2022. 08. 01.

- ✓ az általunk hivatkozott jogalapot az adatkezelésünk előtt kell megállapítanunk és amennyiben az adott jogalap alkalmazandósága megszűnik, vessünk véget az adatkezelésünknek is.
- ✓ amennyiben az adatkezelésünk jogalapja érvényesen megváltozik, igazítsuk ki a folyamatban lévő adatkezelésünket az új jogalapnak megfelelően.
- ✓ közös adatkezelés tervezése esetén – partnereinkkel – egyértelmű és átlátható módon osszuk meg az érintettel szembeni felelősségünket, és az adatkezelésünket e felelősségmegosztásnak megfelelően tervezzük meg.

A GDPR alapján a jogszerűséghez a következők valamelyike szükséges („jogalapok”):

- ✓ az érintett hozzájárulása,
- ✓ olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges,
- ✓ adatkezelőre vonatkozó jogszabályi kötelezettség,
- ✓ az érintett vagy más személy létfontosságú érdekei védelmének szükségessége,
- ✓ közérdekből elvégzendő feladat végrehajtásának szükségessége,
- ✓ az adatkezelő vagy valamely harmadik fél jogos érdekének szükségessége, amennyiben az érintett érdekei és jogai nem élveznek elsőbbséget.

Mit jelent a tisztesség?

A tisztességes adatkezelés azt jelenti, hogy az adatokat nem szerezhetjük meg tisztességtelen eszközökkel, megtévesztéssel vagy az érintett tudta nélkül, illetve a megszerzett adatokat nem kezelhetjük az eredeti adatkezelési céltól eltérően.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Az adatkezelés tisztességes volta az adatkezelést meghatározó elv, az érintett magánszférájának, emberi méltóságának tiszteletben tartását jelentő követelmény. A tisztességes adatkezelés elve értelmében az érintett nem válhat kiszolgáltatottá az adatkezelővel vagy más személlyel szemben.”[156]

Az EDPB iránymutatása alapján[157] a tisztességes eljárás fő beépített és alapértelmezett elemei a következők lehetnek:

- ✓ biztosítsunk az érintettek számára a lehető legnagyobb mértékű autonómiát ahhoz, hogy meghatározzák, hogyan használjuk fel személyes adataikat, továbbá hogy ellenőrizhessék az adatok felhasználását, valamint az adatkezelés hatókörét és feltételeit
- ✓ tegyük lehetővé az érintettek számára, hogy az általunk kezelt személyes adatokkal kapcsolatban kommunikálhassanak velünk, és gyakorolhassák a jogaikat velünk szemben (interakció)

[156] NAIH-1743/2021. sz. határozat (39)
[157] 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről 2.0 változat, Elfogadás időpontja: 2020. október 20., https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_hu.pdf, utolsó letöltés 2022. 08. 01.

- ✓ az adatkezelésünknek meg kell felelnie az érintettek észszerű elvárásainak
- ✓ nem alkalmazhatunk tisztességtelen módon hátrányos megkülönböztetést az érintettekkel szemben, valamint nem használhatjuk ki az érintettek helyzetét, nehézségeit vagy sebezhetőségeit
- ✓ nem „tarthatjuk fogva" tisztességtelen módon a felhasználóinkat. Amennyiben a személyes adatok kezelésével járó szolgáltatásunk „védett", a felhasználó (azaz az érintett) a szolgáltatásunk foglyául eshet, és nem tisztességes, ha gátoljuk az érintetteket az adathordozhatósághoz való joguk gyakorlásában
- ✓ fontos, hogy köztünk és az érintett között kiegyenlített erőviszonyok legyenek. Kerüljük a kiegyensúlyozatlan, az adatkezelő számára előnyös erőviszonyokat, ha pedig ezt valami miatt nem tudjuk megtenni, akkor hozzunk megfelelő ellenintézkedéseket
- ✓ ne hárítsuk át adatkezelésünk kockázatait az érintettekre
- ✓ az adatkezelésünkkel kapcsolatos információkat és lehetőségeket tárgyilagosan és semlegesen mutassuk be, kerülve a megtévesztő vagy manipulatív nyelvezetet vagy megfogalmazást, illetve ábrázolást („dark pattern" alkalmazásának tilalma)
- ✓ tartsuk tiszteletben az érintettek alapvető jogait, valamint szabadságait és ennek érdekében megfelelő intézkedéseket és garanciákat léptessünk életbe, továbbá e jogokat nem korlátozhatjuk, hacsak azt valamilyen törvényi rendelkezés kifejezetten nem indokolja
- ✓ lássuk az adatkezelésünk egyének jogaira és méltóságára gyakorolt szélesebb körű hatásait is (etikusság)
- ✓ adjunk őszinte tájékoztatást a személyes adatok kezelésének módjáról, valamint annak megfelelően járjunk el, amit elmondunk, és ne vezessük félre az érintetteket
- ✓ legyen olyan képzett személyzetünk, amely képes felfedni azokat a torzulásokat, amelyeket a gépek okozhatnak az érintettek ahhoz való jogával kapcsolatban, hogy ne terjedjen ki rájuk az egyedi ügyekben történő automatizált döntéshozatalunk
- ✓ értékeljük rendszeresen, hogy az algoritmusok a céljuknak megfelelően működnek-e, a feltárt torzulások mérséklése érdekében módosítsuk az algoritmusokat, valamint biztosítsuk az adatkezelésünk tisztességességét. Az érintetteket tájékoztassuk a személyes adataik olyan algoritmusok alapján történő kezeléséről, amelyek rájuk vonatkozó elemzéseket vagy előrejelzéseket végeznek például a munkahelyi teljesítményükkel, gazdasági helyzetükkel, egészségi állapotukkal, személyes preferenciáikkal, megbízhatóságukkal vagy viselkedésükkel, tartózkodási helyükkel vagy mozgásukkal kapcsolatban.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Az adatkezelés tisztességes volta a jogszerűséget is magában foglaló követelmény, az érintett információs önrendelkezési jogának, és ezen keresztül magánszférájának, emberi méltóságának tiszteletben tartását jelenti: az érintett nem válhat kiszolgáltatottá az adatkezelővel, sem más személlyel szemben. Az

adatalany mindvégig alanya kell, hogy maradjon a személyes adatok kezelésével járó folyamatnak, és nem válhat annak puszta tárgyává."[158]

Adatkezelőként megteszünk minden szükséges lépést a tisztesség érdekében?

- ✓ Az érintett akkor is számíthat az adatkezelésünk következményére, ha nem olvassa el az adatkezelési tájékoztatónkat?
- ✓ Válthat ki ellenérzést az adatkezelésünk az érintettben? Milyen mértékben hatolunk be az érintett privát szférájába, mennyire vagyunk tolakodóak?
- ✓ Okozhatunk diszkriminációt az adatkezelésünkkel? Mit teszünk annak érdekében, hogy ezt a kockázatot csökkentsük?
- ✓ Amennyiben az adatkezelésünk hozzájáruláson alapul, az érintett ténylegesen szabad akaratából adja azt meg számunkra? Hogyan dokumentáljuk a hozzájárulását, és hogyan vonhatja azt vissza? Lehetővé tesszük azt, hogy ez a folyamat ugyanolyan könnyű legyen, mint ahogy megadta azt? És garantáljuk, hogy mindezt az érintett ingyenesen tehesse meg?
- ✓ Hogyan, mi módon tájékoztatjuk az érintettet a tiltakozás, illetve az elfeledtetés jogáról?
- ✓ Az adatkezelésünkben érintett személy milyen könnyen gyakorolhatja az érintetti jogait? (hozzáférés, helyesbítés, adathordozhatóság stb.)

Holland adatvédelmi hatóság (AP[159]) gyakorlatából

Az AP 2,75 millió euróra bírságolta az Adó- és Vámhivatalt a GDPR rendelkezéseinek megsértése miatt. A hatóság „jogellenesnek, diszkriminatívnak és ezért helytelennek" minősítette azt a gyakorlatot, hogy az adóhatóság a gyermekgondozási segélyt kérelmezőkkel kapcsolatban kettős állampolgárságukkal kapcsolatos információkat kezelt. Az adóhivatal a szervezett módon elkövetett csalás elleni küzdelem céljából kezelte a gyermekgondozási segélyt kérelmezők állampolgársági adatait is, noha ezekre az adatokra nem volt szüksége e célból, valamint a kérelmezők állampolgárságát (holland/nem holland) egy olyan rendszerben használta indikátorként, amely bizonyos kérelmeket automatikusan kockázatosnak minősített.

Az adóhatóságnak már 2014 januárjában törölnie kellett volna a holland állampolgárok kettős állampolgárságára vonatkozó adatokat, mivel a holland állampolgárok kettős állampolgársága nem játszhat szerepet a gyermekgondozási segély iránti kérelmek elbírálásában (az adóhatóság rendszereiben 2018 májusában még mindig mintegy 1,4 millió személy volt kettős állampolgárként nyilvántartva).[160]

[158] NAIH/2019/51/11., https://naih.hu/files/NAIH-2019-51-hatarozat.pdf, utolsó letöltés: 2022. 08. 21.
[159] Autoriteit Persoonsgegevens
[160] Tax Administration fined for discriminatory and unlawful data processing, Press release, 8 December 2021, https://autoriteitpersoonsgegevens.nl/en/news/tax-administration-fined-discriminatory-and-unlawful-data-processing

Mit jelent az átláthatóság?

A GDPR alapján a *„természetes személyek számára átláthatónak kell lennie, hogy a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, azokba, hogy tekintenek bele vagy milyen egyéb módon kezelik, valamint azzal összefüggésben, hogy a személyes adatokat milyen mértékben kezelik vagy fogják kezelni. Az átláthatóság elve megköveteli, hogy a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen, valamint, hogy azt világosan és egyszerű nyelvezettel fogalmazzák meg. Ez az elv vonatkozik különösen az érintetteknek az adatkezelő kilétéről és az adatkezelés céljáról való tájékoztatására, valamint az azt célzó további tájékoztatásra, hogy biztosított legyen az érintett személyes adatainak tisztességes és átlátható kezelése, továbbá arra a tájékoztatásra, hogy az érintetteknek jogukban áll megerősítést és tájékoztatást kapni a róluk kezelt adatokról. A természetes személyt a személyes adatok kezelésével összefüggő kockázatokról, szabályokról, garanciákról és jogokról tájékoztatni kell, valamint arról, hogy hogyan gyakorolhatja az adatkezelés kapcsán megillető jogokat.”*[161]

Az átláthatóság tehát azt jelenti, hogy

- ✓ az adatkezelést megelőzően tájékoztatnunk kell az adatkezelésünkben érintetteteket többek között az adatkezelés céljáról, valamint az adatkezelő, azaz a mi kilétünkről és címünkről.
- ✓ az adatkezelés során be kell tartanunk a vonatkozó jogszabályokat, valamint tájékoztatnunk kell az érintetteket arról, hogy mi, hogyan és miért történik.
- ✓ az adatkezelési műveletekre vonatkozó tájékoztatásunknak világosnak és közérthetőnek kell lennie annak érdekében, hogy az érintettek könnyen megérthessék a szabályokat, a kockázatokat, a garanciákat és az érintetti jogaikat.
- ✓ az érintetteknek az adatkezelés helyén hozzá kell tudni férniük az adataikhoz.

Az EDPB iránymutatása alapján[162] az átláthatóság elvének fő beépített és alapértelmezett elemei a következőket foglalhatják magukban:

- ✓ az általunk rendelkezésre bocsátott információknak világosan és közérthetően megfogalmazottnak, tömörnek és érthetőnek kell lenniük (egyértelműség) és a tájékoztatásunknak egyértelmű jelentéssel kell bírnia a célközönségünk számára.
- ✓ tegyük az információt könnyen hozzáférhetővé az érintettek számára.
- ✓ az információkat a megfelelő időpontban és formában adjuk meg (kontextualitás), legyenek azok relevánsak, és vonatkozzanak konkrét érintettre.
- ✓ az általunk rendelkezésre bocsátott információt minden érintett számára tegyük hozzáférhetővé, ideértve a géppel olvasható nyelvek használatát is (az olvashatóság és az érthetőség elősegítése és automatizálása érdekében).

[161] GDPR (39) preambulumbekezdés

[162] 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről 2.0 változat, Elfogadás időpontja: 2020. október 20., https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_hu.pdf, utolsó letöltés 2022. 08. 01.

- ✓ az adatkezeléseinkben érintetteknek megfelelő ismeretekkel kell rendelkezniük arról, hogy mit várhatnak el személyes adataik kezelése tekintetében, különösen akkor, ha az érintettek gyermekek vagy más kiszolgáltatott csoportok.
- ✓ az információkat különböző csatornákon és médiumokon keresztül (nem csupán szöveges változatban) adjuk meg annak érdekében, hogy a tájékoztatásunk minél nagyobb valószínűséggel ténylegesen is eljussanak az érintetthez.
- ✓ a teljesség és érthetőség egyidejű biztosítása érdekében nyújtsunk többrétegű tájékoztatást (figyelembe véve az érintettek észszerű elvárásait).

A holland hatóság (AP) gyakorlatából

A holland külügyminisztérium a vízumkérelmek feldolgozása során személyes adatokat kezelt, melyek között szerepelt az ujjlenyomat, a név, a cím, a lakóhely, a születési ország, a látogatás célja, az állampolgárság és fénykép. Az adatvédelmi hatóság vizsgálatot folytatott az Új Vízuminformációs Rendszerrel kapcsolatban, amelyet a minisztérium a vízumfeldolgozási műveletekhez használt és megállapította, hogy az új rendszer nem rendelkezik megfelelő biztonsági szinttel, ami azzal a kockázattal jár, hogy illetéktelen személyek betekinthetnek a fájlokba és módosíthatják azokat. Ez növeli annak kockázatát is, hogy más hibák észrevétlenül maradnak. Probléma volt még a biztonsági terv hiánya, a fizikai biztonsági biztosítékok elégtelen volta, a rendszerhez való hozzáféréssel kapcsolatos hivatalos regisztrációs és törlési eljárások hiánya, valamint a biztonsági incidensek bejelentésére szolgáló eljárás hiányosságai.

Az adatvédelmi hatóság azt is megállapította, hogy a vízumkérelmezőket nem tájékoztatták megfelelően arról, hogy adataikat hogyan osztották meg harmadik felekkel.

A Külügyminisztérium évek óta tisztában volt ezekkel a hiányosságokkal, ezért az adatvédelmi hatóság a múltbeli jogsértések miatt 565 ezer eurós bírságot szabott ki. Emellett a biztonság megsértése miatt kéthetente 50 ezer eurós, az átláthatóság hiánya miatt pedig hetente 10 ezer eurós bírságot szabott ki.[163]

Adatkezelőként megteszünk minden lépést az átláthatóság érdekében?

- ✓ Hogyan tájékoztatjuk az érintetteket az adataik kezeléséről?
- ✓ Hogyan biztosítjuk, hogy a tájékoztatásunk ne csak „legyen”, de az el is jusson az érintetthez?
- ✓ Az érintett számára rendelkezésre bocsátottuk-e az összes szükséges információt úgy, hogy az könnyen érthető legyen?
- ✓ Az általunk használt nyelvezet a célközönségünkhöz igazodik? Eltérően kommunikálunk munkavállalóinkkal, a gyerekekkel, az ügyvédi kamarai tagokkal stb.?

[163] Besluit tot het opleggen van een boete en een last onder dwangsom, Buitenlandse Zaken, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_bz_24_februari_2022_openbare_versie_definitief.pdf, utolsó letöltés: 2022. 07. 10.

- ✓ Amennyiben elhalasztjuk a tájékoztatás megadását, ezt a GDPR elvárásainak megfelelően meg tudjuk indokolni?

A belga adatvédelmi hatóság (APD/GBA) gyakorlatából

A panaszos azt állította, hogy a távközlési szolgáltató (Telenet) weboldalán nagyon nehéz megtalálni, hogy hogyan gyakorolhatja a közvetlen üzletszerzéses adatkezelésből való kilépéshez való jogát, és a további információk iránti kérelme sem vezetett eredményre.

Az adatvédelmi hatóság vizsgálata a következőket állapította meg:
A honlapon az információstruktúrában nehéz eligazodni, mert túl sok az információ és ismétlődik. A panaszosnak 14-szer kellett kattintania, hogy elérje a teljes adatvédelmi szabályzatot, az abban szereplő információk azonban nem voltak elég világosak ahhoz, hogy a panaszos élni tudjon a tiltakozáshoz való jogával.

A honlap átláthatósága nem elégséges, és a Telenetnek világosabb információs struktúrát kellene alkalmaznia. A tiltakozáshoz való jognak könnyen hozzáférhetőnek kell lennie, az erre vonatkozó információnak egyértelműnek kell lennie, és nem szabad összekeverni más információkkal, valamint a weboldal nyilvános részén keresztül is elérhetőnek kell lennie, nemcsak a felhasználói oldalon.

A „többrétegű„ tájékoztatás esetén az első réteg felhasználható a GDPR 13–14. cikkében foglalt tájékoztatási kötelezettség teljesítésére, ha kellően világos, de nem túl részletes az átlagos internetfelhasználó számára. Ugyanez vonatkozik a „kinyitható„ rétegekre is, ezeknek világosnak és hozzáférhetőnek kell lenniük.

A Telenet esetében az első réteg túl részletes volt, valamint túl sok volt a kereszthivatkozás. Ahelyett, hogy közvetlen linket adott volna ahhoz az operatív oldalhoz, ahol a tiltakozási jog gyakorolható, az olvasó egy leíró magyarázatot kapott a tiltakozási jog gyakorlásának módjáról. Ez a leírás nem elegendő ahhoz, hogy megkönnyítse az egyén számára a tiltakozási jog konkrét gyakorlását. [164]

Célhoz kötöttség

„Az Alkotmánybíróság megállapítja, hogy személyes adatok meghatározott cél nélküli, tetszőleges jövőbeni felhasználásra való gyűjtése és feldolgozása alkotmányellenes.
Az Alkotmánybíróság megállapítja, hogy a korlátozás nélkül használható, általános és egységes személyazonosító jel (személyi szám) alkotmányellenes.”
[15/1991. (IV. 13.) AB határozat]

[164] Recht van bezwaar tegen direct marketing en tegen verwerkingen op basis van het gerechtvaardigd belang bij telecomoperator Telenet BV, Dossiernummer : AH-2018-0124, https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-19-2021.pdf, utolsó letöltés 2022. 07. 10.

A célhoz kötöttség elve más alapvető elvek előfeltételeként megköveteli, hogy az adatokat meghatározott, egyértelmű és jogszerű célokra gyűjtsük és ne kezeljük azokat oly módon, amely e célokkal összeegyeztethetetlen. Ezeket a célokat már a személyes adatok gyűjtésének időpontjában meg kell meghatároznunk; a személyes adatok meghatározatlan vagy korlátlan célból kezelése nem jogszerű, mivel nem teszi lehetővé az érintett számára az adatkezelés körének (terjedelmének) pontos behatárolását.

A magyar Alkotmánybíróság gyakorlatából

„Az információs önrendelkezési jog gyakorlásának feltétele és egyben legfontosabb garanciája a célhoz kötöttség. Ez azt jelenti, hogy személyes adatot feldolgozni csak pontosan meghatározott és jogszerű célra szabad. Az adatfeldolgozásnak minden szakaszában meg kell felelnie a bejelentett és közhitelűen rögzített célnak. Az adatfeldolgozás célját úgy kell az érintettel közölni, hogy az megítélhesse az adatfeldolgozás hatását jogaira, és megalapozottan dönthessen az adat kiadásáról; továbbá, hogy a céltól eltérő felhasználás esetén élhessen jogaival. Ugyanezért az adatfeldolgozás céljának megváltozásáról is értesíteni kell az érintettet. Az érintett beleegyezése nélkül az új célú feldolgozása csak akkor jogszerű, ha azt meghatározott adatra és feldolgozóra nézve a törvény kifejezetten megengedi. A célhoz kötöttségből következik, hogy a meghatározott cél nélküli, „készletre", előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és -tárolás alkotmányellenes."[165]

Az adatkezelés céljainak egyértelműnek, világosnak és jogszerűnek kell lennie és nem maradhatnak rejtve és nem okozhatnak aránytalan beavatkozást az érintettek érdekeibe, valamint jogaiba és szabadságaiba.

Az, hogy mi minősül jogszerű célnak, az mindig a körülményektől függ, azonban a jogellenes (azaz jogszabályba ütköző) célt szolgáló adatkezelés nem tekinthető jogszerűnek.

A fentiek alapján tehát az adatkezelési célt mindig az adatkezelés megkezdése előtt kell meghatároznunk és nem gyűjthetünk adatot csak azért, hogy „egyszer majd biztos jó lesz valamire", azaz tilos adatot raktároznunk. És ha már megmondtuk, hogy az adott adatokat milyen célból kezeljük, menet közben nem találhatunk ki újabb és újabb célokat, ha már „úgyis a rendelkezésre állnak az adatok".

Példa a célhoz kötöttségre

- ✓ *az, hogy egy kereskedelmi cég a vevői adatait a velük kötött szerződések alapján nyilvántartja még nem hatalmazza fel arra, hogy hírleveleket vagy direkt marketing leveleket küldözgessen nekik.*

Vannak olyan esetek, amikor a GDPR engedékeny és megengedi a további adatkezelést, azonban annak meghatározásához, hogy ez a további adatkezelés összeegyeztethetőnek minősül-e, (többek között) mérlegelnünk kell:

[165] 15/1991. (IV. 13.) AB határozat. A határozat esetében az „adatfeldolgozás" alatt a jelenlegi adatvédelmi jogban adatkezelést kell érteni.

- ✓ minden, az eredeti célok és a tervezett további adatkezelési célok között fennálló összefüggést
- ✓ az adatgyűjtésünk körülményeit, ideértve különösen az érintetteknek a további adatfelhasználásra vonatkozó, a velünk, mint adatkezelővel fennálló kapcsolatán alapuló észszerű elvárásait
- ✓ a személyes adatok jellegét, különös tekintettel arra, hogy az adott adat különleges vagy bűnügyi adat-e
- ✓ a tervezett további adatkezelés következményeit az érintettekre nézve, valamint
- ✓ a megfelelő garanciák meglétét mind az eredeti, mind a tervezett további személyes adatok kezelésére vonatkozó műveletek során (ideértve a titkosítást és az álnevesítést is).

A belga adatvédelmi hatóság (APD/GBA) gyakorlatából

Az APD/GBA úgy ítélte meg, hogy az érintett egészségügyi vonatkozású személyes adatainak megvitatása egy olyan munkaértekezleten, amelyen az érintett nem volt jelen, illetve ezen adatoknak az értekezlet jegyzőkönyvébe való felvétele összeegyeztethetetlen az eredeti adatkezelés céljával (munkaerőgazdálkodás), és az adatkezelőnek nem volt más jogalapja, amelyre hivatkozni lehetett volna.

Egy olyan megbeszélésen, amelyen az érintett nem volt jelen, az érintett vezetője (adatkezelő) bejelentette az érintett távozását, valamint felolvasott egy, a vállalati orvos által kiállított dokumentumot, amely szerint az érintett alkalmatlan a munkavégzésre. Ezt a nyilatkozatot felvették az értekezlet jegyzőkönyvébe is.

Amikor az érintett ezt megtudta, panaszt nyújtott be az adatkezelő ellen a belga adatvédelmi hatóságnál, amiért az egészségügyi vonatkozású személyes adatai jogellenesen lettek továbbítva harmadik félnek. Hozzátette, hogy a jegyzőkönyvet ezután az adatkezelő szerverére mentették, amely szabadon hozzáférhető volt az összes alkalmazott számára, beleértve más részlegek munkatársait is.

A hatóság megállapította, hogy

- ✓ *az érintett nem a munkaképtelenségére vonatkozó információ kezelésnek jogszerűségét vitatta, hanem azt, hogy a vezető ezt követően az egészségi állapotáról tájékoztatta a kollégáit és más munkatársait is.*
- ✓ *nem tudta ellenőrizni, hogy a jegyzőkönyveket ténylegesen elérhetővé tették-e az adatkezelő szerverén, ha azonban ez megtörtént volna, akkor ez további adatkezelési tevékenységnek minősülne, és a jogsértésre vonatkozó megállapítások is alkalmazandók lennének rá.*
- ✓ *az eredeti adatkezelés célja a munkaerőgazdálkodás volt és az érintett észszerűen nem számíthatott arra, hogy az adatokat a munkaerőgazdálkodásra felhatalmazott személyeken kívül széles körben nyilvánosságra hozzák, különösen az adatok különleges (egészségügyi) adat jellegére. Ezért az adatvédelmi hatóság úgy ítélte meg, hogy a további adatkezelés összeegyeztethetetlen volt az eredeti adatkezelés céljával.*

Mivel a további adatkezelés összeegyeztethetetlen volt az eredeti adatkezelés céljával, az csak akkor lehet jogszerű, ha a 9. cikk (2) bekezdése és a 6. cikk (1)

bekezdése szerint saját jogalapja van, ez azonban ebben az esetben nem állt fenn, ebből kifolyólag az adatkezelő nem rendelkezett megfelelő jogalappal az érintett egészségügyi adatainak kezelésére, és ezáltal megsértette a célhoz kötöttség alapelvét [6. cikk (4) bekezdés, illetve a 9. cikk (2) bekezdés].[166]

Az EDPB iránymutatása alapján[167] a célhoz kötöttség fő beépített és alapértelmezett elemei a következők lehetnek:

- ✓ a jogszerű céljainkat határozzuk meg még az adatkezelésünk megtervezése előtt.
- ✓ a célokat úgy határozzuk meg, hogy azok egyértelművé tegyék, miért kezeljük az adott személyes adatokat.
- ✓ az adatkezelésünk céljának megfelelve tervezzük meg az adatkezelésünk és annak hatókörét.
- ✓ a célunk határozza meg, hogy mely személyes adatok szükségesek az adatkezelésünkhöz.
- ✓ minden új célunknak összeegyeztethetőnek kell lennie azzal az eredeti célunkkal, amely alapján az adatokat gyűjtöttük és az adatkezelésünk kialakítását adott esetben ezen új célunknak megfelelően módosítsuk.
- ✓ nem kapcsolhatjuk össze az adatkészleteket és nem végezhetünk további adatkezelést új, összeegyeztethetetlen célok érdekében.
- ✓ a további felhasználás korlátozása érdekében – a hash-t és titkosítást is ideértve – alkalmazzunk megfelelő technikai és szervezési intézkedéseket (például szabályzatokat, szerződéses kikötéseket) a személyes adatok további felhasználásának korlátozására.
- ✓ vizsgáljuk felül rendszeresen, hogy az adott adatkezelésünk szükséges-e azon céljainkhoz, amelyekből az adatokat gyűjtöttük, és vizsgáljuk meg az adatkezelésünk kialakítását a célhoz kötöttség szempontjából.

A belga adatvédelmi hatóság (APD/GBA) gyakorlatából

A hatóság álláspontja alapján az adatkezelő jogalapként hivatkozhat a jogos érdekre, ha korábbi ügyfeleinek közvetlen marketing üzenetet küld, amennyiben a kapcsolat „nem olyan régen„ ért véget, és az érintett nem tiltakozott az adatkezelés ellen.

Az érintett az adatkezelő korábbi ügyfele volt és közvetlen üzletszerzéssel kapcsolatos üzeneteket kapott tőle („direkt marketing"). Az érintett tiltakozott személyes adatainak további kezelése ellen, ugyanakkor hozzáférést kért az adatkezelő kezelt valamennyi személyes adatához és a hivatkozott jogalaphoz.
Az adatkezelő határidőben válaszolt és megerősítette, hogy az érintett a továbbiakban nem fog ilyen üzeneteket kapni. Az érintett ezt követően panaszt

[166] Numéro de dossier : DOS-2020-01492, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-115-2022.pdf, utolsó letöltés 2022. 08. 10.
[167] 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről 2.0 változat, Elfogadás időpontja: 2020. október 20., https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_hu.pdf, utolsó letöltés 2022. 08. 01.

nyújtott be az adatvédelmi hatósághoz, amelyben azt állította, hogy az adatkezelő nem hivatkozhat jogos érdekre az e-mail címe kezelésekor, mivel ő korábbi, nem pedig jelenlegi ügyfél.

Az adatvédelmi hatóság úgy ítélte meg, hogy az adatkezelő hivatkozhat jogos érdekre a közvetlen üzletszerzés esetében, beleértve bizonyos feltételek fennállta esetén a korábbi ügyfeleket is. Amennyiben az adatkezelő és az érintett között nem állt fenn kapcsolat, vagy ha az „régen volt", a jogos érdekre nem lehet hivatkozni, mivel a közvetlen marketing nem része az érintett észszerű elvárásainak. Ebben az esetben azonban az adatkezelő és az érintett közötti kapcsolat nem olyan régen szűnt meg (körülbelül két évvel korábban), ezért az érintett észszerűen elvárhatta, hogy az adatait továbbra is közvetlen üzletszerzésre használják fel, az adatkezelő pedig jogalapként jogos érdekre hivatkozhatott.

Az adatkezelő is megerősítette, hogy a közvetlen üzletszerzés céljából történő adatkezelésre csak a szolgáltatás felmondását követő két évig kerül sor, ez alapján az adatvédelmi hatóság úgy ítélte meg, hogy az adatkezelő nem sértette meg a GDPR-t.[168]

Adatkezelőként megteszünk minden lépést a célhoz kötöttség érdekében?

- ✓ Megfelelően azonosítottuk az adott adatkezelésünk összes célját?
- ✓ Minden új adatkezelési célunk összeegyeztethető az eredeti adatkezelési célunkkal?
- ✓ Fennáll annak az esélye/veszélye, hogy az adott adatkezelés keretében kezelt személyes adatokat más célokra újra felhasználjuk? Ha igen, hogyan tesszük ezt jogszerűvé? (például üzleti partnereink kapcsolattartási adatait marketing célokra szeretnénk felhasználni)
- ✓ Hogyan garantáljuk azt, hogy egy adott adatkezelésünk keretében kezelt személyes adatokat csak ezen adatkezelés megkezdése előtt meghatározott céljainkra használjuk fel?
- ✓ Amennyiben a személyes adatokat tudományos kutatási, statisztikai vagy történelmi célokra kívánjuk újra felhasználni, netalán megosztani másokkal, milyen biztosítékokat alkalmazunk az érintettek jogainak és szabadságainak védelme érdekében?

A norvég adatvédelmi hatóság gyakorlatából

A norvég adatvédelmi hatóság 37 400 euró bírságot szabott ki a Norvég Közúti Igazgatóságra, mivel a személyes adatokat az eredetileg meghatározott célokkal össze nem egyeztethető célokra kezelte, valamint a videofelvételeket hét nap elteltével nem törölte.

A Közúti Igazgatóság a személyes adatokat igen kiterjedten kezelte, a szerződéses felek, alkalmazottak, alvállalkozók, illetve az alvállalkozók alkalmazottainak megfigyelésére használt fix közúti kamerák segítségével. A hatóság megállapította,

[168] Dossiernummer : DOS-2021-07812, https://www.gegevensbeschermingsautoriteit.be/publications/zonder-gevolg-nr.-117-2022.pdf, utolsó letöltés 2022. 08. 13.

hogy a felvételek ily módon történő felhasználása (a szerződésszegések dokumentálására több hónappal az események bekövetkezése után) összeegyeztethetetlen az adatkezelés eredeti céljával, amely azonnali biztonsági intézkedések lehetővé tétele volt. Ezeket a videofelvételeket nem szabad felhasználni a szerződések teljesítésének nyomon követésére, az adatok újrafelhasználása pedig jelentős hátrányt jelentett a szerződő felek és alkalmazottai számára, és ellentétes azzal, ahogyan a szerződő felek elvárhatják a személyes adatok felhasználását.[169]

A belga adatvédelmi hatóság (APD/GBA) gyakorlatából

Egy fitneszklub tagjával (a panaszossal) felvette a kapcsolatot ugyanannak a fitneszklubnak egy másik tagja (a harmadik fél) és tájékoztatta, hogy egy hiba miatt a panaszos tagsági díját ő fizette ki, és hogy ezen fizetési ügy kapcsán a fitneszklub megosztotta vele a panaszosra vonatkozó személyes adatokat (nevét, telefonszámát, e-mail címét, születési dátumát, valamint a panaszos legutolsó fitneszklubban tett látogatásainak időpontját).

A panaszos úgy vélte, hogy a fitneszklub megsértette a célhoz kötöttség elvét, mivel ezeket a személyes adatokat eredetileg a panaszos és a fitneszklub közötti szerződés teljesítése céljából gyűjtötték, éppen ezért a fitneszklubnak nem lett volna szabad megosztania ezeket az adatokat a klub egy másik tagjával egy fizetési probléma miatt. A panaszos ezért panaszt nyújtott be a belga adatvédelmi hatósághoz a fitneszklub ellen.

A hatóság véleménye szerint a panaszos nevének, születési adatainak stb. megosztása egy fizetési probléma megoldása érdekében nem volt összeegyeztethető és szükséges a fitneszklub és a panaszos közötti szerződés teljesítésének céljával.

A hatóság szerint nem volt szükséges, hogy a fitneszklub felfedje a panaszos személyazonosságát és egyéb adatait a harmadik fél előtt, aki véletlenül a panaszos tagdíját kifizette, ezen kívül a panaszos nem számíthatott arra, hogy személyes adatait, beleértve a fitneszklubokban tett legutóbbi látogatásaira vonatkozó információkat is, egy fizetési probléma megoldása érdekében megosztják egy harmadik féllel.
Mivel a panaszos személyes adatainak jogellenes megosztása csak egyszeri esemény volt, amelyet valószínűleg emberi hiba okozott, és mivel a fitneszklub időközben megfelelő intézkedéseket hozott a GDPR további megsértésének elkerülése érdekében, a hatóság nem szabott ki pénzbírságot.[170]

[169] Norwegian DPA: Decision to fine The Norwegian Public Roads Administration, https://edpb.europa.eu/news/national-news/2020/norwegian-dpa-decision-fine-norwegian-public-roads-administration_en, 2022. 07. 10.
[170] Betreft : doorgifte persoonsgegevens van lid sportclub aan een derde, Dossiernummer : DOS-2020-00292, https://gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-125-2021.pdf, utolsó letöltés: 2022. 07. 11.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Ha az Ügyfél a kötelezően rögzített hangfelvételekkel további adatkezelési műveleteket kíván végezni, azokat elemezni kívánja automata módon új és nem teljesen ismert, kockázatos technológiákkal, akkor meg kell felelnie az általános adatvédelmi rendelet 6. cikk (4) bekezdésének is, mivel az adatgyűjtés céljától eltérő célból kíván személyes adatokat kezelni. Ilyen esetben az, hogy az érintettek számíthatnak-e észszerűen az adatkezelésre és az új adatkezelés az eredeti céllal – jelen esetben a jogszabályi kötelezettség teljesítése miatti beszélgetésrögzítéssel – összhangban van-e, azt az adatkezelő köteles megvizsgálni még az adatkezelés megkezdése előtt, a megfelelő garanciák meglétét pedig folyamatosan köteles biztosítani. Az érintettek érdemi tudomása és választási joga nélkül, egy teljesen más okból rendelkezésre álló hangfelvétel elemzése nem lehet adatvédelmi szempontból jogszerű, ha arról az érintettek érdemben tudomást nem szerezhettek, és a garanciális érintetti jogok hiányoznak, amelyet az Ügyfél tudomása ellenére utóbb sem vett figyelembe, ennek tudatában is folytatta az adatkezelést. Ez igazolja a jogsértés szándékos jellegét.”[171]

Adattakarékosság

Az „**adattakarékosság” elve** alapján az adatkezelésünket valamely jogszerű cél teljesítéséhez szükségesre kell korlátoznunk és a személyes adatok kezelésére csak akkor keríthetünk sort, ha az adatkezelés célját más eszközökkel észszerűen nem tudjuk teljesíteni.

Példa az adattakarékosságra

- ✓ *biztonsági regisztrációhoz kötjük, hogy a látogatók beléphessenek az adott intézmény területére. A regisztráció során kérünk személyes adatokat (például név, telefonszám) azért, hogy amennyiben a látogatás időtartama alatt például tűz ütne ki/bombariadó stb. történne, ezeket átadhassuk a mentés vezetőjének. Azért is elkérhetjük az adatokat, hogy a védett objektum látogatását például honvédelmi/nemzetbiztonsági érdekből kontrollálni tudjuk. Azonban olyan adatokat, amelyek a területen tartózkodással kapcsolatban nem relevánsak (pl. gyermekek száma, családi állapot), nem gyűjthetünk.*

Fontos kritérium az is, hogy az adatkezelésünk nem avatkozhat be aránytalanul az érintettek érdekeibe, jogaiba és szabadságaiba. Az EDPS iránymutatása[172] nyolc lépéses szükségességi-arányossági vizsgálatot ajánl annak érdekében, hogy megfeleljünk az adatkezelésünkkel szemben támasztott követelményeknek.

A szükségesség vizsgálata:

a) írjuk le az adatkezelésünket (tényszerűen)

[171] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: 2022. 07. 17.
[172] https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf, utolsó letöltés: 2022. 08. 21.

b) azonosítsuk az adatkezelésünk által korlátozott alapvető érintetti jogokat és szabadságokat. Korlátozzuk a magánélethez és a személyes adatok védelméhez való jogot, esetleg más jogokat is? Az adatkezelésünknek minden esetben tiszteletben kell tartania ezen jogok lényegét.
c) határozzuk meg az adatkezelésünk célkitűzéseit. Ezek közé tartozhat az Európa Unió által elismert általános érdekű cél vagy mások jogai és szabadságai védelmének szükségessége.
d) válasszuk ki azt a lehetőséget, amely (valóban) hatékony és a legkevésbé beavatkozó a szóban forgó jogok szempontjából.

Az arányosság vizsgálata:

a) értékeljük a célunk fontosságát és azt, hogy az adatkezelésünk megfelel-e ennek a célnak.
b) értékeljük a beavatkozásunk hatókörét, kiterjedtségét és intenzitását.
   - ✓ hány személyt érint az adatkezelésünk? (hatókör)
   - ✓ milyen típusú adatokat kezelnénk és mennyi ideig? (kiterjedtség)
   - ✓ az eljárásunk lehetővé teszi-e pontos következtetések levonását az egyének magánéletére vonatkozóan? (intenzitás)
c) végezzük el az adatkezelésünk „méltányos egyensúly„ értékelését.
d) amennyiben az adatkezelésünk nem arányos, határozzunk meg a biztosítékokat és vezessük be azokat, például
   - ✓ csökkentsük a személyes adatok kezelésének hatókörét vagy terjedelmét,
   - ✓ vezessünk be törlési vagy érvényességi határidőt,
   - ✓ írjunk elő különleges felügyeleti/irányítási intézkedéseket stb.

Az EDPB iránymutatása alapján[173] az adattakarékosság fő beépített és alapértelmezett elemei a következők lehetnek:

- ✓ amennyiben az adott célunk elérésének szempontjából lehetséges, kerüljük teljes mértékben a személyes adatok kezelését;
- ✓ korlátozzuk az összegyűjtött személyes adatok mennyiségét a célunk szempontjából a legszükségesebbre;
- ✓ alakítsuk ki oly módon az adatkezelésünket, hogy csak minimális számú személynek kelljen hozzáférnie a személyes adatokhoz feladataik ellátása érdekében, a hozzáférést pedig ennek megfelelően korlátozzuk (érvényesítsük a „need to know" elvét, a kevesebből a több felé haladva);
- ✓ legyenek a személyes adatok relevánsak az adott adatkezelésünk szempontjából és tudjuk bizonyítani is ezt a relevanciát;
- ✓ minden személyesadat-kategória legyen szükséges az előre meghatározott céljaink eléréséhez, és a személyes adatokat csak akkor kezeljük, ha a céljainkat más módon nem érhetjük el;
- ✓ lehetőség szerint használjunk összesített adatokat,
- ✓ álnevesítsünk, amint már nincs szükségünk az érintetteket közvetlenül azonosító személyes adatokra, és tároljunk külön az azonosítási kulcsokat. Ez a gyakorlatban azt jelenti, hogy például az érintett nevét úgy cseréljük ki (lásd

[173] 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről 2.0 változat, Elfogadás időpontja: 2020. október 20., https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_hu.pdf, utolsó letöltés 2022. 08. 01.

például „jelige" használata egy novella író versenyen), hogy a nevet és az álnevet csak azok láthatják együttesen, akik erre jogosultak.

- ✓ amennyiben a személyes adatok a célunk szempontjából már nem szükségesek, azokat anonimizáljuk vagy töröljük;
  ne hozzunk létre a szükségesnél több másolatot.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Az Egyetem közjegyző vagy jegyző előtt tett nyilatkozatot kér a szülőktől, amely nyilatkozati forma plusz adatkezelést generál a közjegyző vagy jegyző előtt. Amennyiben a szülők a nyilatkozatokat a közjegyző előtt teszik meg annak érdekében, hogy a közjegyző az általuk előadott tényt közjegyzői okiratba foglalja, akkor a szülők nyilatkozata így közokiratnak minősül. A jegyző előtt tett nyilatkozat azonban nem egyenértékű, hiszen, ha a szülők a jegyző előtt nyilatkoznak arról, hogy adott személy nem él a háztartásban, az írásba foglalt nyilatkozat nem minősül közokiratnak. Az Egyetem a Hatóság erre irányuló kérdésére sem tudott választ adni arra, hogy miért követelik meg e nyilatkozati formát – ezzel új adatkezelést generálva a közjegyző vagy jegyző előtt –, és miért nem elegendő, ha az érintett személy két tanú előtt tesz nyilatkozatot, amely nyilatkozat teljes bizonyító erejű magánokirat, amely ellenkező bizonyításig tanúsítja az okiratban szereplő körülményeket.
A Hatóság megítélése szerint a GDPR 5. cikk (1) bekezdés c) pontja szerinti adattakarékosság elvébe ütközik, ha az Egyetem – ezzel többletadatkezelést generálva – közjegyző vagy jegyző előtti nyilatkozattételt kíván, mivel a Hatóság álláspontja szerint a két tanú által aláírt nyilatkozat is képes lenne biztosítani az Egyetem által elérni kívánt célt."[174]

Mit teszünk az adattakarékosság érdekében?

- ✓ Az adatok, amiket gyűjtünk, megfelelnek az adatkezelési célunknak?
- ✓ Vannak olyan adatok, amelyeket ugyan gyűjtünk az adott adatkezelésünk keretében, ám azok eltávolítása esetén is ugyanúgy meg tudjuk valósítani az adatkezelési célunkat? (Ha igen, ezek feleslegesek az adott adatkezelésünk szempontjából!)
- ✓ Amennyiben úgy gyűjtünk adatot, hogy az érintettek számára választási lehetőséget adunk a gyűjtött adatok köre tekintetében, akkor a kötelező és a választható adatszolgáltatások között határozott, azaz az érintettek számára világosan érzékelhető különbséget tesztünk?
- ✓ Amennyiben az adatkezelési célunk megvalósulása után az adatokat meg kívánjuk tartani statisztikai, kutatási vagy történelmi célokra, akkor hogyan kezeljük az újraazonosítás kockázatát?

[174] NAIH/2020/54/4. https://www.naih.hu/hatarozatok-vegzesek?download=325:1-rendszeres-szocialis-osztondijakkal-kapcsolatos-adatkezeles-a-budapesti-muszaki-es-gazdasagtudomanyi-egyetemen-modositasokkal-egyseges-szerkezetben, utolsó letöltés 2022. 08. 21.

Az osztrák bírósági gyakorlatból

A Szövetségi Közigazgatási Bíróság megállapította, hogy egy takarítócég nem sértette meg az adattakarékosság elvét azzal, hogy értesítette a vele együttműködő ingatlankezelő társaságot arról, hogy az egyik takarítóját elbocsátották.

Az érintett a takarítócégnél (az adatkezelőnél) dolgozott takarítóként körülbelül három-négy évig. 2019 októberében az érintettet a takarítócég elbocsátotta és a munkaszerződés megszűnését követően értesítette az ingatlankezelőt, hogy az érintettet már nem foglalkoztatják, és új takarító személyzet veszi át a szerepét. A takarítócég nem említette, hogy melyik fél szüntette meg a munkaviszonyt. Körülbelül másfél évvel később az érintett tudomást szerzett a korábbi munkáltatója és az ingatlankezelő cég közötti levélváltásról.

A bíróság megállapította, hogy a takarítócég nem sértette meg az adattakarékosság elvét. Annak ellenére, hogy a szerződés nem írta elő azt a kötelezettséget, hogy a takarító személyzet változásáról tájékoztatni kell az ingatlankezelőt, a bíróság megállapította, hogy a takarítócég olyan jogos érdekre törekedett, amelyet az érintett érdekei nem írnak felül. A bíróság véleményét meghatározó elemek:

- ✓ *az épületek takarításával kapcsolatos személyes elem*
- ✓ *a takarítócég kisvállalkozói dimenziója (személyes szolgáltatást nyújt ügyfeleinek)*
- ✓ *az érintett a komplexum egyik épületében lakott, ahol korábban dolgozott*
- ✓ *a munkaszerződés megszüntetésére vonatkozó információ alapvetően nem érzékeny adat (elfogulatlan, pejoratív jelentés nélküli).*

Az adattakarékosság elve nem sérül, ha nem lehetséges az adatkezelés további adatok eltávolítása anélkül úgy, hogy a cél elérését ne nehezítené – azaz az elv akkor sérül, ha az adatokat el lehet távolítani az adott adatkezelésből anélkül, hogy a cél elérését megnehezítenénk.[175]

A román adatvédelmi hatóság gyakorlatából

A román adatvédelmi hatóság 5 ezer eurós bírságot szabott ki egy vállalatra (S.C. Tip Top Food Industry S.R.L.) az adattakarékosság elvének megsértése miatt. A hatóság úgy ítélte meg, hogy a munkahelyi kamerarendszerrel kapcsolatos adatkezelés túlzott mértékű, és az alkalmazottakat olyan helyiségekben is rögzítik, mint az öltöző vagy az étkező. Ezen túlmenően a munkavállalók által az ilyen adatkezeléshez adott hozzájárulás nem tekinthető szabadon megadottnak.

A hatóság megállapította, hogy a munkavállalók olyan helyiségekben történő rögzítése, mint az öltöző vagy az étkező, nem szükséges a kitűzött cél eléréséhez (a vállalat eszközeinek védelme és a lopások megelőzése), és ugyanezt az eredményt más, a munkavállalók magánéletébe kevésbé beavatkozó intézkedésekkel is el lehetett volna érni.

[175] Bundesverwaltungsgericht Republik Österreich, W 2742246355-1/20E, https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20211222_W274_2246355_1_00/BVWGT_20211222_W274_2246355_1_00.pdf, utolsó letöltés: 2022. 07. 12.

Ezen túlmenően az adatvédelmi hatóság megállapította, hogy a hozzájárulás nem tekinthető érvényes jogalapnak a munkáltató és a munkavállaló közötti kiegyensúlyozatlan kapcsolat miatt. [176]

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A Kötelezett nyilatkozata szerint a közszolgálati tisztviselők feladata az, hogy figyelemmel kísérjék a kültéri kamerák által rögzített felvételeket, és amennyiben a kamerák jogszabálysértést észlelnek, ezt jelezzék a diszpécsernek, aki intézkedik a közterület-felügyelők helyszínre irányítása érdekében.

A Hatóság álláspontja szerint azonban a közszolgálati tisztviselők ezen feladatainak ellenőrzésére a belső kamera jelen formájában nem alkalmas, mivel a felvételek alapján csupán az állapítható meg, hogy az adott közszolgálati tisztviselő a monitort nézi-e, azt azonban nem mutatja meg, hogy valójában mit néz a monitoron, és milyen tevékenységet végez a számítógépén. A Hatóság álláspontja szerint az ellenőrzés ebben az esetben megvalósulhat például gyakoribb, személyes ellenőrzéssel a vezető részéről, vagy úgynevezett csoportvezető kinevezésével, akinek feladatkörébe tartozna a munkatársak feladatellátásának ellenőrzése.

Az adatbiztonsági követelmények betartása kapcsán a Hatóság álláspontja szerint a térfelügyeleti rendszer védelme szintén megvalósítható hatékonyabban más módszerekkel, kamerák nélkül is. Így például megfelelő számítástechnikai védelmi fejlesztésekkel, melyek megakadályozzák azt, hogy a munkaállomásokról adatokat mentsenek le, mint például az adatvesztés megakadályozását szolgáló eszközökkel, újgenerációs tűzfalakkal és egyesített fenyegetéskezelő rendszerekkel, illetve különféle biztonsági alkalmazásokkal és intézkedésekkel, mint az internet korlátozásával, tiltásával, a külső adathordozók (például pendrive) csatlakoztatásának letiltásával, illetve a kép-, illetve hangrögzítésre alkalmas eszköz bevitelének hatékony kiszűrésével.

Annak megakadályozására, hogy a közszolgálati tisztviselők a térfelügyeleti helyiségbe bevigyék kép-, illetve hangrögzítésre alkalmas eszközeiket, a Hatóság álláspontja szerint a Kötelezettnek szintén a rendelkezésére áll más módszer, mint például gyakoribb, személyes ellenőrzés a vezető részéről, vagy erre az esetre is kinevezhető csoportvezető, akinek feladatkörébe tartozna a munkatársak ellenőrzése annak érdekében is, hogy megakadályozzák a felvételkészítést.

A Hatóságnak megküldött videofelvétel alapján továbbá a közszolgálati tisztviselőket a kamera akként figyeli meg, hogy a felvétel alapján nem is feltétlenül állapítható meg minden esetben, hogy az adott közszolgálati tisztviselő használja-e a kép-, illetve hangrögzítésre alkalmas eszközét, vagy azzal készít-e felvételt a munkaeszközéről, illetve annak monitoráról, amiből következően az adott kamera ilyen célra egyébként sem feltétlenül alkalmas.

[176] Sancțiune pentru încălcarea RGPD, https://www.dataprotection.ro/?page=Comunicat_Presa_15_/_04_/_2021&lang=ro, utolsó letöltés: 2022. 07. 12.

Mindebből következően a Hatóság tehát, bár az adatkezelés célját legitim adatkezelési célként elismeri ugyan, azonban az adatkezelés e cél megvalósításához való szükségességét, arányosságát, illetve költséghatékonyságát a Kötelezett nem támasztotta alá. A Kötelezett nem igazolta továbbá, hogy más – az érintettek magánszférához való jogát kevésbé sértő – módszerek ne lettek volna alkalmasak az általa megjelölt cél elérésére. Ebből következően a Hatóság megállapítja, hogy a Kötelezett megsértette az általános adatvédelmi rendelet 5. cikk (1) bekezdés c) pontja szerinti adattakarékosság elvét. (…).”[177]

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„mivel nem csak a védendő vagyontárgyakra irányul az említett kamera, hanem szélesebb spektrumú látókört foglal magába az általa közvetített kép, így lehetővé téve a helyiség teljes megfigyelését is, a Hatóság álláspontja szerint az adattakarékosság elvét – az általános adatvédelmi rendelet 5. cikk (1) bekezdés c) pontját – is sérti Kérelmezett ezen adatkezelése.”[178]

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„(…) a lakások és helyiségek bérletére, valamint az elidegenítésükre vonatkozó egyes szabályokról szóló 1993. évi LXXVIII. törvény (…) alapján az önkormányzat rendeletében a szociális helyzeten alapuló bérbeadások esetében a bérbeadás feltételeként csak vagyoni és jövedelmi körülményekhez igazodó feltételt határozhat meg. Fentiekre figyelemmel a Hatóság álláspontja szerint a lakásbérleti szerződés megkötéséhez nem elengedhetetlenül szükséges a bérlő hatósági erkölcsi bizonyítványa tartalmának ismerete, ezért ez az adatkezelés az adattakarékosság elvébe (…) ütközik.”[179]

Adatok pontossága

Az **„adatok pontosságának” elvé**t minden adatkezelési művelet során érvényesítnünk kell és a pontatlan adatokat haladéktalanul törölnünk vagy helyesbítenünk kell. A pontosság érdekében szükségünk lehet az adatok rendszeres ellenőrzésére és aktualizálására is.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„(…) a személyes adat nem annak pontosságától, hanem konkrét személyhez rendeléstől lesz személyes adat. Például egy pontatlanul rögzített és adott beazonosítható érintetthez kötötten tárolt nem valós életkor tárolása ugyanúgy

[177] NAIH/2019/2466/12. Budapest, 2019. augusztus 2., https://naih.hu/files/NAIH_2019_2466_hatarozat.pdf, utolsó letöltés: 2022. 07. 14.
[178] NAIH/2020/2729/15. Budapest, 2020. október 14., https://www.naih.hu/hatarozatok-vegzesek?download=239:munkahelyi-kameras-megfigyeles-celhoz-kototttseggel-adattakarekossaggal-es-az-erintettek-tajekoztatasaval-kapcsolatos-hianyossagai, utolsó letöltés: 2022. 07. 14.
[179] NAIH/2020/5985/2. állásfoglalás

személyesadatkezelés lesz az adott adatkezelő részéről, mintha az adat pontos lenne. (…)
Az, hogy egy adat utólag tévesnek, pontatlannak bizonyul, még nem teszi kétségessé annak személyes adat jellegét, hiszen bármely – nemcsak valós – adat meghatározott természetes személyhez kötve személyes adatot eredményez."[180]

Adatkezelőként gondoskodnunk kell arról, hogy az általunk kezelt adatok pontosak és szükség esetén naprakészek legyenek, valamint minden észszerű intézkedést meg kell tennünk annak érdekében, hogy az adatkezelésünk céljai szempontjából pontatlan személyes adatokat töröljük vagy helyesbítsük.

A spanyol bírósági gyakorlatból

A Canary Islands Cars autókölcsönző cég tévesen használta fel A ügyfél adatait, hogy autóbérleti szerződést kössön B ügyféllel, aki a gépjárművet használva közlekedési szabálysértést követett el. Ezt követően A ügyfél adatait tévesen továbbították a Közlekedési Főigazgatóságnak (DGT). Amikor a DGT felvette a kapcsolatot A ügyféllel akkor derült ki, hogy a bírság kiszabása céljából átadott szerződés nem egyezett azzal, amelyet ő eredetileg aláírt.

A spanyol adatvédelmi hatóság (AEPD) megállapította, hogy az adatkezelőnek lettek volna lehetőségei a „tévedés" elkerülésére, például a jogosítvány számok egyeztetése, ez azonban nem történt meg, ezért az adatpontosság elvének megsértése miatt 25 ezer eurós bírságot szabott ki. Az adatkezelő fellebbezett a döntés ellen, a bíróság pedig megállapította, hogy a név és a vezetéknév puszta egybeesése nem indokolja, hogy a gépkocsikölcsönzési szerződés egy másik személy adataival kössük meg különösen akkor, ha az a személy, akinek a gépkocsit átadjuk előttünk áll, valamint több személy közreműködése is be van építve a szerződés előkészítése, az adatgyűjtés és a jármű átadásának jegyzőkönyvezése, a szerződés másolatának átadása, illetve a fizetés folyamatába. Ezen eljárások mindegyikében ellenőrizni kell a szerződő fél személyazonosságát, és ebben az esetben nem állapítható meg kellő körültekintés az adatkezelő részéről. A bíróság helybenhagyta a hatóság döntését és a bírság összegét.[181]

Az EDPB iránymutatása alapján[182] az adatpontosság fő beépített és alapértelmezett elemei a következők lehetnek:

- ✓ a személyes adatok forrásai legyenek megbízhatóak (az adatok pontossága szempontjából);
- ✓ minden személyes adatelemnek a meghatározott céljainkhoz szükséges pontosságú legyen;

[180] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés 2022. 07. 17.
[181] AN – 578/2021,
[182] 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről 2.0 változat, Elfogadás időpontja: 2020. október 20., https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_hu.pdf, utolsó letöltés 2022. 08. 01.

- ✓ csökkentsük a hamis pozitívok és negatívok számát (például automatizált döntéshozatalban és mesterséges intelligencia esetén a torzítások mérséklése érdekében);
- ✓ ellenőrizzük a személyes adatok helyességét az adatkezelés előtt és annak különböző szakaszaiban (attól függően, hogy milyen gyakran változhatnak);
- ✓ haladéktalanul töröljük vagy helyesbítsük a pontatlan adatokat. Ez különösen akkor fontos, ha az érintettek az adatok gyűjtésekor még gyermekek voltak és a későbbekben el akarják távolíttatni a szóban forgó személyes adataikat;
- ✓ mérsékeljük az adatkezelési láncunkban felhalmozódott hibák hatását;
- ✓ a pontosság ellenőrzése és szükség esetén a helyesbítés érdekében az érintettek számára nyújtsunk tájékoztatást a személyes adataikról, és biztosítsunk számukra tényleges hozzáférést;
- ✓ biztosítsuk, hogy a személyes adatok az adatkezelésünk minden szakaszában pontosak, illetve a kritikus lépéseknél végezzük el újra a pontosság ellenőrzését;
- ✓ tegyük naprakésszé a személyes adatokat, amennyiben ez a célunk szempontjából szükséges;
- ✓ ne adjunk meg olyan feltétlen teljesítendő kritériumokat az adatgyűjtésnél, amelyek már eleve pontatlanná teszik az adatszolgáltatást (például ne kényszerítsük az érintettet arra hogy kitalálja, hogyan írhatja be az űrlapunkba a munkáltatójának nevét számok nélkül, ha annak a hivatalos nevében számok is szerepelnek);
- ✓ alkalmazzunk technikai és szervezési intézkedéseket a pontatlanság csökkentése érdekében, például tömör, előre meghatározott választási lehetőségek megadásával üres szövegmezők helyett (különben saját kárunkon tudjuk meg, ugyanazt a szót/kifejezést hányféleképpen képesek leírni az adatot szolgáltatók).

Példa a pontosságra

- ✓ *az adatkezelésünk céljára tekintettel mennyit ér egy olyan nyilvántartás, ami az öt évvel ezelőtti neveket és védőeszköz méreteket tartalmazza, amikor most van szükségünk a védőeszközök pótlására? Nem tudjuk megindokolni, miért van szükségünk ebben az adatbázisban a már leszerelt állomány adataira (naprakészség), illetve ha valaki a nyilvántartás frissítése óta lefogyott vagy meghízott, akkor az ő méretével kapcsolatos adatokat is helyesbítenünk kell.*
- ✓ *a rendkívüli esetben értesítendő személyek nyilvántartása esetében a személyi állomány figyelmét rendszeresen fel kell hívnunk, ha változás történik ezen személyek körében (például válás, külön költözés, összeveszés stb. miatt), feltétlen szóljanak és mi haladéktalanul korrigáljuk az adatokat, ellenkező esetben a nyilvántartásunk nem tudja betölteni a célját.*
- ✓ *mennyire használható az az adatbázis, ahol ugyanaz az adatkategória (pl. kutya/macska fajtája, gépjármű típusa stb.) sokféleképpen leírva szerepelhet (pl. német juhász, n. juhász, német juh., farkaskutya, németh juhász stb.)*

Mit teszünk az adatpontosság érdekében?

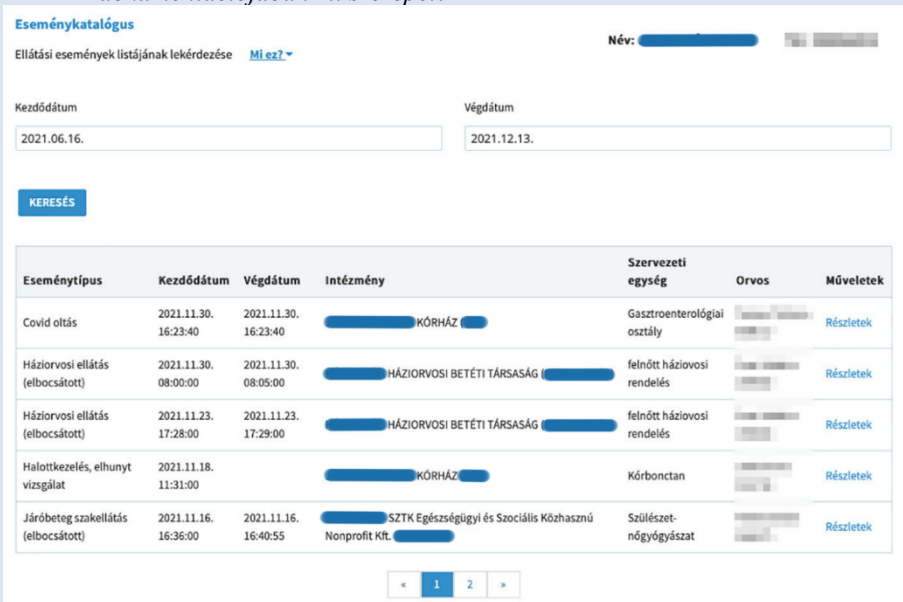
- ✓ Hogyan biztosítjuk, hogy a szervezetünk által az érintettektől, illetve harmadik féltől begyűjtött adatok pontosak legyenek?

- ✓ Milyen következményekkel járhat az az érintettek számára, ha pontatlan személyes adatokat kezelünk velük kapcsolatban?
- ✓ Hogyan tesszük lehetővé az adatkezelési folyamatainkban az adatok frissítést, illetve a szükséges mértékű pontosítást, valamint módosítást?
- ✓ Hogyan ellenőrizzük az adataink konzisztenciáját?

A hibás személyes adat is személyes adat – attól mert hibás, még mindig az érintett személyes adata marad, egy-egy téves információ pedig komoly következményekkel járhat az érintettre nézve.

Példák a pontatlanság következményeire

- ✓ *téves adat szerepel az érintett hitelképességére vonatkozó adatokat tartalmazó nyilvántartásban és ezért az érintett hiába kér hitelt, nem kap*
- ✓ *a személyzeti osztályon elírják az alkalmazott lakcímét, ennek következtében a szolgálati/munkaviszonya nem túl békés megszűnése után „címzett ismeretlen" megjegyzéssel jönnek vissza a neki küldött levelek*
- ✓ *téves munkaidő-nyilvántartás bejegyzések miatt a munkavállaló nem azt a bért kapja, amit kapnia kellene*
- ✓ *az EESZT[183] téves adatot tartalmaz[184], mely nemcsak azt a kérdést teszi fel, hogy hogyan jelenhet meg háziorvosi ellátáson meg covid-oltáson egy elhunyt személy (azaz a rendszer miért nem szűri ki az ilyen eseteket) hanem az is, vajon ki az, aki ténylegesen elhunyt, és az ő EESZT dokumentációjában mi szerepel?*



Vannak olyan adatkezelések (például a műtéti jegyzőkönyvek, szolgálati naplók), amelyek esetében a tárolt adatok frissítését (utólagos korrigálását) jogszabály/utasítás

[183] https://www.eeszt.gov.hu/hu/nyito-oldal
[184] https://telex.hu/zacc/2021/12/13/arra-keltem-hogy-meghaltam-es-felboncoltak

tiltja, mivel az adatok tárolásának elsődleges célja az események, mint múltbeli „pillanatfelvételek" dokumentálása. Az ilyen típusú adatkezelések esetében is szükségünk lehet az utólagos helyesbítésre, ám az csak például megjegyzés, kiegészítés formájában vagy egyéb módon – az eredeti adat megtartásával és a korrigálásra utalással – történhet.

Korlátozott tárolhatóság

A „**korlátozott tárolhatóság" elv**nek megfelelve biztosítanunk kell, hogy az adatok tárolása olyan formában történjen, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig tegye lehetővé. Amennyiben a személyes adatokat ennél hosszabb ideig kívánjuk tárolni, azt minden további nélkül megtehetjük, de teljesítenünk kell a GDPR közérdekű archiválásra, tudományos és történelmi kutatásra, valamint a statisztikai célú felhasználásra vonatkozó előírásait.

Ez az alapelv az, ami alapján nincs mentségünk, időnként selejteznünk kell és ennek során mindent ki kell dobnunk amire már nincs szükségünk. A sok-sok munkaórát elemésztő tevékenység egyik haszna, hogy nem kell még egy helyiséget irattár céljára kialakítanunk és az újrahasznosított papír is sok mindenre jó, természetesen miután már nem tartalmaz egyetlen egy személyes adatot sem.

A dán bírósági gyakorlatból

A bíróság úgy döntött, az IDdesign A/S (jelenleg ILVA A/S) vállalat megsértette a korlátozott tárolhatóság elvét azzal, hogy mintegy 350 ezer ügyfél adatait hosszabb ideig őrizte meg, mint amennyi az adatgyűjtés céljaihoz szükséges volt. A régi informatikai rendszerében tárolt személyes adatok között szerepelt az ügyfelek neve, címe, telefonszáma, e-mail címe és rendelési előzményei.
A cég mintegy 100 ezer dán korona bírságot kapott.[185]

A személyes adatok tárolására vonatkozó időbeli korlátozás természetesen csak olyan adatokra vonatkozik, amelyeket az érintettek azonosítást lehetővé tevő formában tárolunk, így például az anonimizált adatokra nem (ellenben az álnevesítettekre igen).

Az ír adatvédelmi hatóság (DPC) gyakorlatából

A DPC 70 ezer eurós bírságot szabott ki a University College Dublinra (UCD), amiért az nem hajtott végre megfelelő biztonsági intézkedéseket, a szükségesnél hosszabb ideig tárolta a személyes adatokat, illetve nem értesítette indokolatlan késedelem nélkül a DPC-t az adatvédelmi incidensről.

Több adatvédelmi incidens során illetéktelen harmadik személyek hozzáfértek az UCD e-mail fiókjaihoz, illetve az UCD e-mail fiókjainak belépési adatait az interneten közzétették.

A DPC megállapította, hogy az UCD

[185] Retten i Aarhus – J.nr. SS 3662/2020, https://domstol.dk/aarhus/aktuelt/2021/2/selskab-idoemt-en-boede-paa-100000-kr/m utolsó letöltés: 2022. 07. 18.

- ✓ *az e-mail szolgáltatásában nem kezelte a személyes adatokat oly módon, hogy megfelelő technikai és szervezési intézkedésekkel biztosította volna a személyes adatok megfelelő biztonságát.*
- ✓ *bizonyos személyes adatokat egy e-mail fiókban olyan formában tárolt, amely az érintettek azonosítását a személyes adatok kezelésének céljához képest a szükségesnél hosszabb ideig tette lehetővé, valamint*
- ✓ *az egyik adatvédelmi incidenst 13 nappal azután jelentette be, hogy tudomást szerzett róla.*[186]

Az EDPB iránymutatása alapján[187] a korlátozott tárolhatóság fő beépített és alapértelmezett elemei a következők lehetnek:

- ✓ a törlésre és/vagy anonimizálásra vonatkozóan rendelkezzünk egyértelmű belső eljárásokkal és funkciókkal, illetve győződjünk meg arról, hogy nem lehet újraazonosítani az anonimizált adatokat, illetve helyreállítani a törölt adatokat;
- ✓ amennyiben lehetséges, automatizáljuk a személyes adatok törlését;
- ✓ határozzuk meg, hogy milyen adatokat meddig szükséges tárolnunk és indokoljuk is meg a döntésünket, tekintettel az adatkezelési céljainkra;
- ✓ készítsünk adatmegőrzési szabályzatot és ellenőrizzük, a szervezetünk alkalmazza-e az abban foglaltakat;
- ✓ határozzuk meg, hogy a biztonsági másolatokhoz és a naplókhoz milyen személyes adatokat meddig szükséges tárolnunk;
- ✓ legyünk tisztában azzal, szervezetünkben hogyan áramlanak a személyes adatok és azzal, azokról hol, ki és milyen formában tárol másolatot, továbbá törekedjünk arra, hogy a lehető legnagyobb mértékben korlátozzuk a személyes adatok „ideiglenes" tárolását („raktározását").

Mit teszünk a korlátozott tárolhatóság érdekében?

- ✓ Van az adatok megőrzésének idejére vonatkozó iránymutatásunk (például irattári terv stb.)?
- ✓ Az adatkezelésünkben az adatok tárolási időtartamát meghatározza uniós vagy tagállami jogszabály?
- ✓ Tisztában vagyunk azzal, hogy az egyes adatkezeléseink esetén mennyi ideig kell megőriznünk az adatokat?
- ✓ Milyen szempontok alapján határozzuk meg az egyes adatokra vonatkozó megőrzési időszakot?
- ✓ Amennyiben nem tudjuk még törölni az adatokat, tudjuk korlátozni az azokhoz való hozzáférést?
- ✓ Eszközeink lehetővé teszik az automatikus törlést a megőrzési időszak végén?

[186] DPC – Inquiry into University College Dublin (IN-19-7-4), https://www.dataprotection.ie/sites/default/files/uploads/2021-02/17.12.2020_Decision_IN-19-7-4_UniversityCollegeDublin.pdf, utolsó letöltés 2022. 07. 18.

[187] 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről 2.0 változat, Elfogadás időpontja: 2020. október 20., https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_hu.pdf, utolsó letöltés 2022. 08. 01.

- ✓ Hogyan valósítjuk meg a törlést (megsemmisítést)? Van rá rendszeresített eljárásrendünk?

Integritás és bizalmas jelleg

Az „**integritás és bizalmas jelleg" elv** alapján a személyes adatok kezelését oly módon kell végeznünk, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítsuk a személyes adatok megfelelő biztonságát, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

Az intézkedések megtételekor figyelembe kell vennünk

- ✓ a tudomány és technológia állását és a megvalósítás költségeit,
- ✓ az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint
- ✓ a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatot – azaz

mindent meg kell tennünk annak érdekében, hogy az adatokhoz ne férjen hozzá olyan, aki nem jogosult hozzáférni és ne módosíthassa-törölhesse olyan, aki ezt jogszerűen nem teheti meg.

A svéd adatvédelmi hatóság (Integritetsskyddsmyndigheten – IMY) gyakorlatából

Az IMY mintegy 150 ezer eurós bírságot szabott ki az Uppsalai Egyetemi Kórházra azért, mert titkosítatlan e-mailben küldte el külföldre a betegeknek és kórházaknak az egészségügyi adatokat.[188]

Az EDPB iránymutatása alapján[189] az integritás és bizalmas jelleg fő beépített és alapértelmezett elemei a következők lehetnek:

- ✓ rendelkezzünk információbiztonsági szabályzattal és az eljárások irányításának operatív eszközével;
- ✓ értékeljük – az egyének jogaira gyakorolt hatás figyelembevételével – a személyes adatok biztonságára jelentett kockázatokat és kezeljük az azonosított kockázatokat. A kockázatértékelés céljára átfogó, szisztematikus és realisztikus kockázati modellt dolgozzunk ki és alkalmazzuk is azt;
- ✓ a biztonsági követelményeket már a rendszer tervezésekor (azaz a lehető legkorábban) vegyük figyelembe, valamint dolgozzunk ki releváns teszteket, és ezeket folyamatosan integráljuk és végezzük;
- ✓ rendszeresen vizsgáljuk felül a szoftvereinket, hardvereinket, rendszereinket és szolgáltatásainkat, valamint teszteljük ezeket az adatkezelést támogató rendszereink sebezhetőségének feltárása érdekében;
- ✓ oldjuk meg, hogy a személyes adatokhoz csak azok a feljogosított alkalmazottjaink férjenek hozzá, akiknek erre adatkezelési feladataik

[188] DI-2021-559. https://www.imy.se/globalassets/dokument/beslut/2022/beslut-sjukhusstyrelsen-region-uppsala.pdf, utolsó letöltés: 2022. 07. 30.
[189] 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről 2.0 változat, Elfogadás időpontja: 2020. október 20., https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_hu.pdf, utolsó letöltés 2022. 08. 01.

ellátásához szükségük van, és csak olyan és amilyen mértékben erre szükség van;

- ✓ az adatkezeléseinket oly módon alakítsuk ki, hogy feladataink ellátása érdekében csak minimális számú személynek kelljen hozzáférnie a személyes adatokhoz, a hozzáférést pedig ennek megfelelően korlátozzuk.
  - az egyes adatkezelési műveletekkel összefüggésben a hozzáférést adatállományként azokra az attribútumokra korlátozzuk, amelyek a művelet elvégzéséhez szükségesek. Ezenfelül a hozzáférést azokra az adatokra korlátozzuk, amelyek az adott alkalmazottunk feladatkörébe tartozó érintettekre vonatkoznak.
  - az adatkezeléseket oly módon alakítsuk ki, hogy egyetlen személynek se kelljen hozzáférnie egy érintettről gyűjtött valamennyi adathoz, legkevésbé pedig az érintettek egy konkrét kategóriájának valamennyi személyes adatához.
  - úgy oldjuk meg az adatok továbbítását, hogy azt védjük a jogosulatlan és véletlen hozzáféréssel és változtatásokkal szemben;
- ✓ az adattárolásunk legyen biztonságos a jogosulatlan hozzáféréssel és változtatásokkal szemben. Léptessünk életbe eljárásokat a központosított vagy decentralizált adattárolás kockázatának értékelésére és annak felmérésére, hogy ez a személyes adatok mely kategóriáira vonatkozik. Bizonyos adatok esetében további biztonsági intézkedésekre lehet szükségünk, illetve szükséges lehet azok más adatoktól való elkülönítése is.
- ✓ a biztonsági másolatokat és a naplókat az információbiztonsághoz szükséges mértékben őrizzük meg, használjunk rutinszerű biztonsági ellenőrzésként ellenőrzési nyomvonalakat, és kövessük nyomon az eseményeket. Ezeket a biztonsági másolatokat és naplókat védenünk kell a jogosulatlan vagy véletlen hozzáféréssel és változtatásokkal szemben, valamint rendszeresen vizsgáljuk felül ezeket, és az incidenseket is kezeljük haladéktalanul;
- ✓ betartjuk az információs rendszerek katasztrófa utáni helyreállításával és az üzletmenet-folytonossággal kapcsolatos követelményeit annak érdekében, hogy a személyes adatok súlyosabb incidensek után ismét elérhetőek legyenek számunkra;
- ✓ a személyes adatok valamennyi kategóriáját – a biztonsági incidensek kockázata szempontjából – védjük megfelelő intézkedésekkel. Amennyiben lehetséges, a különleges kockázatot jelentő adatokat a többi személyes adattól elkülönítve tároljuk;
- ✓ alkalmazunk az adatvédelmi incidensek felderítésére, kezelésére, bejelentésére és az azokból való tanulásra vonatkozó gyakorlatokat, eljárásokat és erőforrásokat;
- ✓ a szabálysértések és incidensek kezelésére alkalmazzunk folyamatokat annak érdekében, hogy az adatkezelési rendszerünk megbízhatóbb legyen. Idetartoznak az értesítési eljárások is, például a felügyeleti hatóságnak küldött értesítés és az érintetteknek szükség szerinti tájékoztatásának intézése.

A finn adatvédelmi hatóság (Tietosuojavaltuutetun toimisto) gyakorlatából

A finn adatvédelmi hatóság 608 ezer eurós bírságot szabott ki egy pszichoterápiával foglalkozó cégre, mert az nem jelentett időben két olyan adatvédelmi incidenst, amelyek miatt a betegadatok nyilvánosságra kerültek, valamint nem gondoskodott

a személyes adatok biztonságáról. A támadó a céget és a pácienseket is megzsarolta az adatvédelmi incidenseket követően.
A Vastaamo Oy's pszichoterápiával foglalkozó cégnél 2018 novemberében és 2019 márciusában két alkalommal is adatvédelmi incidens történt, mely során a támadó a betegnyilvántartásokat feltörte. Az incidenseket csak 2020. szeptember végén jelentették a finn adatvédelmi hatóságnak, nem sokkal azután, hogy a támadó megzsarolta a céget. A támadó a következő hónapokban legalább 15 ezer beteget is megzsarolt azzal, hogy egészségügyi adataikat közzéteszi és mintegy 300 adat valóban ki is szivárgott az interneten a Tor-hálózaton.

A finn adatvédelmi hatóság megállapította, hogy a cég
- ✓ *nem jelentette kellő időben az adatvédelmi incidenseket a finn adatvédelmi hatóságnak és az érintetteket sem tájékoztatta azokról,*
- ✓ *nem hajtott végre megfelelő biztonsági intézkedéseket a személyes adatok sértetlenségének és bizalmas jellegének biztosítása érdekében, valamint*
- ✓ *nem felelt meg az elszámoltathatóság elvének, mivel nem tudta bizonyítani a GDPR alapelveinek való megfelelést.*

A cégre kiszabott közigazgatási bírság összesen 608 ezer euró volt, ami a cég 2020. évi forgalmának mintegy 4,2%-át jelenti.[190]

Mit teszünk az adatbiztonság érdekében?
- ✓ Vannak-e eljárásaink az általunk kezelt személyes adatokat, illetve az informatikai rendszereinket esetlegesen érintő információbiztonsági kockázatok azonosítására, elemzésére és értékelésére?
- ✓ Vizsgálataink kiterjednek-e nemcsak a szervezetünket, hanem az érintettek érdekeit, jogait és szabadságait érintő kockázatokra is?
- ✓ A kockázatok felmérése során figyelembe veszük-e az adatkezelésünk célját, jellegét, hatályát és kontextusát is?
- ✓ Nemcsak feltárjuk, de kezeljük is a rendszereinkkel és a személyes adatok kezelésével kapcsolatos kockázatokat?
- ✓ Vannak-e olyan erőforrásaink, illetve megfelelő tudással rendelkező munkavállalóink (megbízottjaink), akik képesek végrehajtani a kockázatmenedzseléssel kapcsolatos feladatokat?

Természetesen egy-egy rosszul kivitelezett adatkezelés/adatfeldolgozás esetén nemcsak egy elvet sérthetünk meg, hanem egyszerre akár többet is.

Elszámoltathatóság elve

Az „elszámoltathatóság" elve a GDPR „szuperelve", mely alapján bármikor bizonyítani kell tudnunk az adatvédelmi rendelkezések betartását az érintettek, valamint a nyilvánosság és a felügyeleti hatóságok felé.

[190] Tietosuojavaltuutetun toimisto (Finland) – 1150/161/2021, https://finlex.fi/fi/viranomaiset/tsv/2021/20211183, utolsó letöltés 2022. 07. 18.

A magyar adatkezelési hatóság (NAIH) gyakorlatából

„A GDPR nem tartalmaz megkötést a hozzájárulás megvalósulási formájára vonatkozóan, csak az érvényességéhez szükséges követelményeket – önkéntes, konkrét, megfelelő tájékoztatáson alapuló, egyértelmű akaratkinyilvánítás, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez – határozza meg.

Amennyiben tehát az adatkezelés jogalapja (…) hozzájárulás, úgy az adatkezelőnek tudnia kell bizonyítani, hogy érvényes hozzájárulást szerzett az érintettől, az érintett az adatkezeléshez hozzájárulását adta. A Hatóság megállapította, hogy a Kötelezett nem tudta bizonyítani, hogy az érintettek a GDPR-nak megfelelő hozzájárulásukat adták a személyes adataik kezeléséhez, ezért a Hatóság azt is megállapította, hogy a Kötelezett a GDPR 5. cikk (2) bekezdés szerinti elszámoltathatóság elvét is megsértette.”[191]

A szó elszáll, az írás megmarad, ezért aztán adatkezelőként nem tehetünk mást, mint szabályzatokat/utasításokat alkotunk, tartunk és tartatunk be annak érdekében, hogy bizonyítsuk a megfelelést, valamint gondoskodunk az érintettek tájékoztatásáról, illetve kérdéseikre, kérelmeikre időben és tárgyszerűen válaszolunk.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Valamely dokumentum előállítása önmagában nem az adatkezelői kötelezettségek teljesítése, az csak eszköze, rögzítése kell, hogy legyen az érdemi mérlegelés és döntés előkészítésének, döntésnek, és szükséges időközökben azok felülvizsgálatának. (…). Mind a preambulumban foglaltak, mind az általános adatvédelmi rendelet cikkei eredmény elérését írják elő az adatkezelő kötelezettségeinek meghatározásakor, nem csak egy meghatározott minimális adminisztráció elvégzését az adatkezelő részéről.”[192]

Az EDPB iránymutatása alapján[193] a GDPR alapelveinek való megfelelés bizonyításaként bemutathatjuk, hogy az érintettek jogainak védelme érdekében hozott intézkedéseink milyen hatással bírnak, és azok miért bizonyulnak megfelelőnek és hatékonynak. Az EDPB azt is kifejti, hogy a személyes adatok felelősségteljes kezeléséhez rendelkeznünk kell az adatvédelem megvalósításához szükséges ismeretekkel, és képesnek is kell lennünk az intézkedéseink kompetens megvalósításra. Ehhez pedig az szükséges, hogy tisztában legyünk az általános adatvédelmi rendelet szerinti adatvédelmi kötelezettségeinkkel és teljesíteni is tudjuk azokat.

---

[191] NAIH/2020/1866/5. NAIH/2019/2314.
[192] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: 2022. 07. 17.
[193] 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről 2.0 változat, Elfogadás időpontja: 2020. október 20., https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_hu.pdf, utolsó letöltés 2022. 08. 01.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Az I.r. kérelmezett nem vetette össze a saját adatkezelése által megvalósítható érdekét a Kérelmező jogaival és érdekeivel, az azok közti súlyozást nem végezte el, továbbá saját érdekének a Kérelmező jogaival és érdekeivel szembeni elsőbbségét nem igazolta. Különösen nem igazolta az I.r. kérelmezett azt, hogy konkrétan a Kérelmező vonatkozásában ténylegesen mely adatok kezelése szükséges, továbbá azt, hogy ez az adatkezelés a Kérelmezőnek a személyes adatai védelméhez fűződő érdekével és alapvető jogaival, szabadságaival szemben arányban áll.

Az elszámoltathatóság elve alapján az adatkezelőknek az adatkezelés teljes folyamata során úgy kell megvalósítaniuk az adatkezelési műveleteket, hogy képesek legyenek az adatvédelmi szabályoknak való megfelelés bizonyítására. Az elszámoltathatóság elve, tehát nem csak általában, folyamat szinten értelmezhető, az valamennyi konkrét adatkezelési tevékenység, egy konkrét érintett személyes adatai kezelésének vonatkozásában is érvényesül.

Az adatkezelő felelős az általa végzett adatkezelés jogszerűségéért. Az általános adatvédelmi rendelet 6. cikk (1) bekezdés f) pontja szerinti jogalap természetéből fakadóan azon adatkezelőnek, aki ezen jogalapra hivatkozik, pontosan meg kell tudni jelölnie, hogy egy konkrét személyes adat kezelését az adatkezelő mely jogos érdeke alapozza meg, és ezen érdekre tekintettel miért szükséges az adatkezelés, egyben igazolnia, bizonyítania is tudnia kell, hogy az elsőbbséget élvez az érintett jogos érdekével, személyes adatok védelméhez fűződő jogával szemben. A jogos érdek jogalap fennállását érdekmérlegeléssel kell igazolni az általános adatvédelmi rendelt (47) preambulumbekezdése alapján is.

Az általános adatvédelmi rendelet 5. cikk (2) bekezdése alapján az I.r. kérelmezettnek tudnia kell igazolnia azt, hogy az általános adatvédelmi rendeletben írtaknak megfelel az adatkezelése, tehát a jelen esetben azt, hogy elvégezte az érdekmérlegelést. Tekintettel arra, hogy az I.r. kérelmezett nem igazolta – a Hatóság felhívására sem – azt, hogy elvégezte az általános adatvédelmi rendeletben előírt érdekmérlegelést, ezért a Hatóság megállapítja, hogy az I.r. kérelmezett megsértette az általános adatvédelmi rendelet 5. cikk (2) bekezdését.”[194]

[194] NAIH/2020/4365, NAIH/2019/1516, NAIH/2018/6769/H, https://www.naih.hu/files/NAIH-2020-4365-hatarozat.pdf, utolsó letöltés 2022. 07. 25.

AZ ÁTLÁTHATÓSÁGRÓL RÉSZLETESEBBEN

Az átláthatóság elve alapján mindent meg kell tennünk annak érdekében, hogy tájékoztassuk az érintetteket az adataik felhasználásának módjáról. Az átláthatóság vonatkozhat

- ✓ az adatkezelés megkezdése előtti tájékoztatásra,
- ✓ magára a tájékoztatásra, amelynek az adatkezelés során könnyen hozzáférhetőnek kell lennie, illetve
- ✓ az érintetteknek saját adataikhoz való hozzáférésre irányuló kérésüket követően az általunk adott tájékoztatásra.

Az adatkezelési műveleteket könnyen érthető módon kell elmagyaráznunk annak érdekében, hogy az érintettek megértsék, mi történik az adataikkal. Ez ténylegesen azt jelenti, hogy

- ✓ a személyes adatok gyűjtése pillanatában az érintetteknek tisztában kell lenniük a személyes adataik kezelésének konkrét céljával, ez pedig csak akkor valósul meg, ha világos és közérthető nyelvezetet használunk a tájékoztatás folyamán. A zavaros, átláthatatlan, több dokumentumban szétszórt, jogszabályi idézetekkel telezsúfolt adatkezelési tájékoztatónak kikiáltott „bármi" nem felel meg ezen kritériumnak.
- ✓ az érintettek számára egyértelműnek kell lennie, hogy személyes adataik kezelése milyen kockázatokkal jár számukra és milyen szabályok, biztosítékok, valamint jogok vonatkoznak az adott adatkezelésre.

Az átláthatóság elve azonban nem merül ki ennyiben, ugyanis hármas kötelezettséget ró ránk az érintetti jogokkal kapcsolatban. Az elvnek megfelelve adatkezelőként

- ✓ tájékoztatást kell adnunk az érintetteknek a jogaikról,
- ✓ biztosítanunk kell azt, hogy ez a tájékoztatás megfeleljen az átláthatóság elvének (könnyen érthető legyen stb.), valamint
- ✓ meg kell könnyítenünk az érintettek számára az adatvédelemre vonatkozó jogszabályokban foglalt jogaik gyakorlását.

A GDPR-nak az a célja, hogy ténylegesen olyan helyzetbe hozza az érintetteket, hogy képesek legyenek jogaik érvényesítésére és az adatkezelők felelősségre vonására a személyes adataik kezelésével kapcsolatban – az adatvédelmi hatóságok pedig ezen elv tiszteletben nem tartásáért szabják ki a legtöbb büntetést.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Mind az általános adatvédelmi rendelet, illetve munkavállalók esetében mind az Mt. előírja azt, hogy az érintetteket tájékoztatni kell az adatkezeléssel kapcsolatos körülményekről. (...) A tájékoztatás formáját a jogszabályok nem határozzák meg, azonban a Hatóság javasolja az írásbeli formát azon okból, hogy – az elszámoltathatóság elvéből is következően – az adatkezelőnek kell bizonyítania, igazolnia az előzetes tájékoztatás megtörténtét. (...)

A Hatóság álláspontja szerint tehát a munkáltatónak mint adatkezelőnek az elektronikus megfigyelőrendszer alkalmazására vonatkozó, munkavállalók részére nyújtott tájékoztatójában minden egyes kamera vonatkozásában pontosan meg kell

jelölnie, hogy az adott kamerát milyen célból helyezte el az adott területen és milyen területre, berendezésre irányul a kamera látószöge. A munkáltató az általános adatvédelmi rendelet 6. cikk (1) bekezdés f) pontja szerinti jogos érdek jogalapja alapján ezzel tudja igazolni a munkavállalók számára azt, hogy miért tekinthető szükségesnek az adott terület megfigyelése. Nem fogadható el az a gyakorlat, amikor a munkáltató általánosságban tájékoztatja a munkavállalókat arról, hogy elektronikus megfigyelőrendszert alkalmaz a munkahely területén. (…)

Ugyanakkor ezen bővebb tájékoztatás a Hatóság álláspontja szerint már nem szükséges a munkavállalókon kívüli harmadik személyek felé, tekintettel arra, hogy az ő magánszférájukat az elektronikus megfigyelőrendszer kevésbé érinti, illetve amennyiben ezen személyek is tudomással bírnának arról, hogy az adott kamera milyen területet, vagyontárgyat figyel meg, a rendszer elvesztené vagyonvédelmi funkcióját. Ebből kifolyólag a munkavállalókon kívüli személyek felé az általános, az egyes kamerákról szóló részletes leírás nélküli tájékoztatási kötelezettség terheli az adatkezelőt.".[195]

Kutatásunk során megállapítottuk, hogy az érintettek alapvetően és döntő többségben nem olvassák el az adatkezelési tájékoztatókat. Ez több okra is visszavezethető:

- az érintett előképzettsége kevés ahhoz, hogy értelmezni tudja a tájékoztatót,
- az érintett álláspontja az, hogy a szolgáltató nem kezeli a személyes adatait,
- sosem hallott még a GDPR-ról.

Abban az esetben, ha el is olvassa, annak értelmezése során az alábbi problémák merülnek fel:

- ✓ az érintett nem tudja értelmezni az adat, az információ, az adatkezelő és az adatkezelés fogalmát,
- ✓ az adatkezelési tájékoztató túl hosszú,
- ✓ az adatkezelési tájékoztatóban számos olyan fogalom van a fentiek mellett, amely értelmezhetetlenné teszi azt,
- ✓ a tájékoztatóban túl sok jogi kifejezés van,
- ✓ az érintettek kutatásunk szerint maximálisan egy oldalas adatkezelési tájékoztatót olvasnak el, és erre maximálisan 3-5 percet szánnak.

A kutatásunk alapján elmondható, hogy az érthetőség, a minél egyszerűbb megfogalmazás (szóhasználat) és a többrétegű tájékoztatás az, amely segítségével az érintettek közelebb kerülhetnek ahhoz, hogy adatvédelemtudatos érintettként éljék meg a velük kapcsolatos adatkezeléseket.

[195] NAIH-3748-1/2021. https://www.naih.hu/hatarozatok-vegzesek?download=380:kamerak-uzemeltetese-idosek-otthonaban, utolsó letöltés 2022. 08. 20.

AZ ELSZÁMOLTATHATÓSÁGRÓL RÉSZLETESEBBEN

Adatkezelőként akkor felelünk meg a GDPR szuperelvének, azaz az elszámoltathatóság elvének, ha az adatkezelési tevékenységünk során nemcsak megtervezzük, de aktívan végre is hajtjuk az adatvédelem előmozdítására és a folyamatos megfelelőség biztosítására irányuló intézkedéseinket.

A GDPR kimondja, hogy

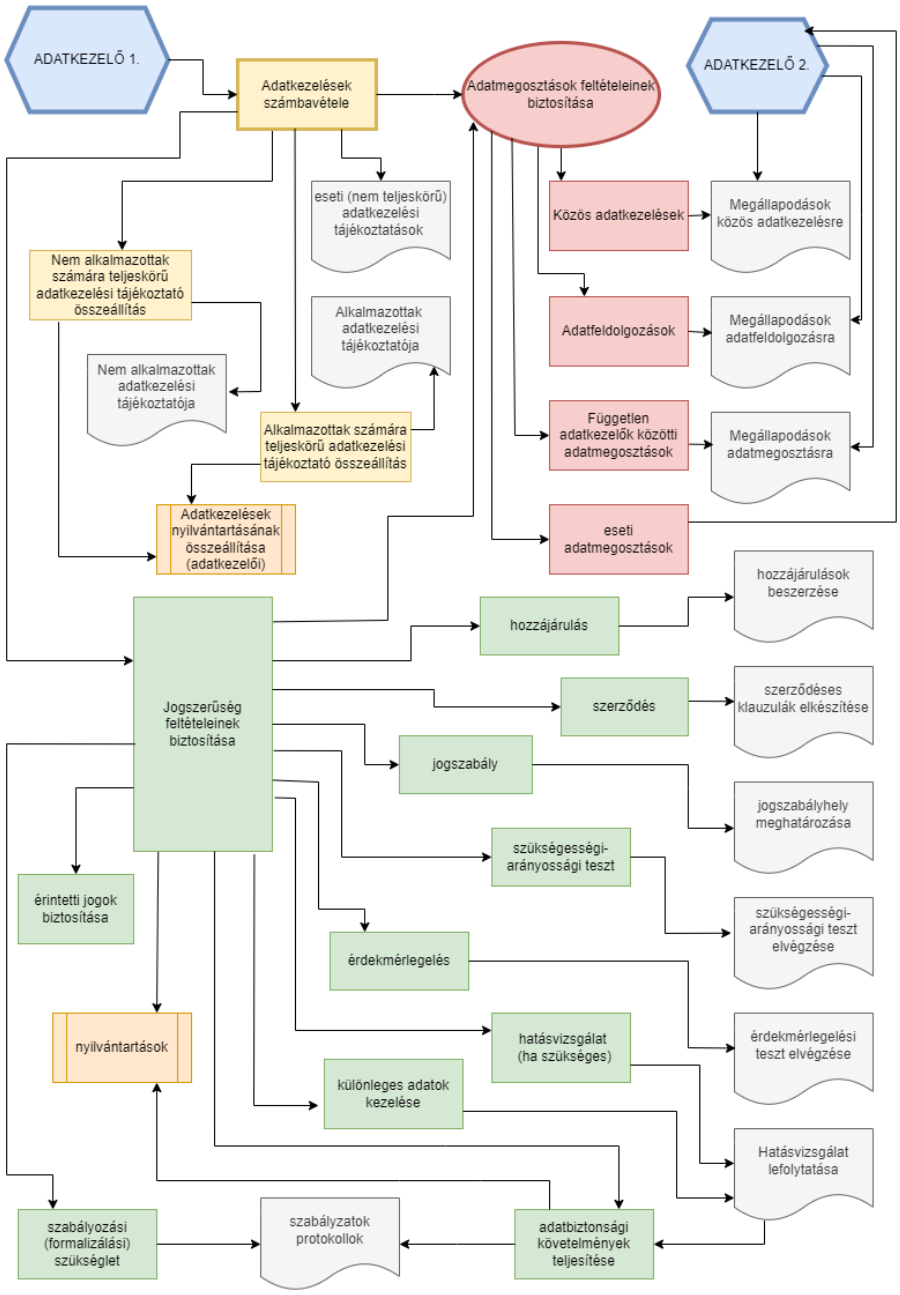
- ✓ *az adatkezelők és adatfeldolgozók az adatkezelési műveleteik során felelősek az adatvédelmi jog rendelkezéseinek és saját kötelezettségeik betartásáért*
- ✓ *az adatkezelőknek bármikor tudniuk kell bizonyítani az adatvédelmi rendelkezések betartását mind az érintettek, mind a nyilvánosság és a felügyeleti hatóságok felé*
- ✓ *az adatfeldolgozóknak is meg kell felelniük az elszámoltathatósághoz kapcsolódó kötelezettségnek.*

Az adatvédelmi szabályoknak megfelelőséget segíti például

- ✓ az adatvédelmi tevékenységek nyilvántartása (ezt adatkezelőként a felügyeleti hatóság kérésére rendelkezésre kell tudnunk bocsátani);
- ✓ adatvédelmi tisztviselőt vonunk be az adatkezeléseinkbe (akár kötelezően, akár önkéntesen);
- ✓ kockázatkezelési eljárást dolgozunk ki és követünk, valamint adatvédelmi hatásvizsgálatot végzünk az adatkezelések olyan típusaira, amelyek valószínűleg magas kockázatot jelentenek a természetes személyek jogaira és szabadságaira nézve;
- ✓ biztosítjuk a beépített és alapértelmezett adatvédelmet;
- ✓ intézkedéseket és eljárásokat alakítunk ki és tartunk be az érintettek jogainak minél zökkenőmentesebb gyakorlására érdekében;
- ✓ csatlakozunk jóváhagyott magatartási kódexhez vagy tanúsítási mechanizmushoz;
- ✓ vezetői intézkedéseket rendszeresítünk (pl. megfelelő szervezeti struktúra kialakítása, jelentési láncolat következetes betartása és betartatása, ellenőrzés, az ellenőrzés megállapításaiból levont következtetések folyamatba építése stb.);
- ✓ adatvédelmi oktatásokat szervezünk;
- ✓ belső szabályzatokat hozunk létre, vezetünk be és tartunk/tartatunk be;
- ✓ megfelelő szerződéskötési és adattovábbítási gyakorlatot alakítunk ki az adatokhoz való hozzáférés, illetve az adatmegosztások során;
- ✓ közös adatkezelőkkel és adatfeldolgozóinkkal törekszünk a formalizált kapcsolatra (a GDPR előírásainak megfelelő megállapodásokat kötünk és tartunk/tartatunk be);
- ✓ adatvédelmi incidensek esetére megfelelő incidenskezelési gyakorlatot rendszeresítünk.

A megfelelőségi elemek kapcsolatait mutatja az alábbi sematikus ábra, mely egy adatkezelő szempontjából írja le a főbb tevékenységek kapcsolódását, illetve ezen adatkezelési tevékenységek követelményeit, különös tekintettel az elszámoltathatóság elvére. A kapcsolat más adatkezelőkkel az adatokhoz való hozzáférés biztosításával,

illetve adatmegosztásokon keresztül történik, akár egymással kapcsolatban lévő szervezetekről (például vállalatcsoport tagjairól, projektben együttműködő entitásokról), akár egymástól független szervezetekről van szó.



Kötelező nyilvántartások

A GDPR előírja néhány kötelező nyilvántartás vezetését, egyebekben pedig az adatkezelőre, azaz ránk bízza, hogy milyen saját nyilvántartásokat vezetünk annak érdekében, hogy képesek legyünk megfelelni az elszámoltathatóság elvének.

***Kötelező nyilvántartások**, például:*

- ✓ *az adatkezelők által vezetendő adatkezelések nyilvántartása*[196]*. Ahogy leltározzuk a székeinket, asztalainkat meg egyéb eszközeinket, úgy leltárba kell vennünk az adatkezeléseinket is. Különben honnan tudnák, hogy szervezetünkben milyen adatkezelések vannak, azokat kik és milyen hatókörben végzik, hogyan áramlanak az adatok a szervezeti egységek, valamint az adatfeldolgozóink és közös adatkezelők között, mely adatokat továbbítjuk, valamint mely mozzanatokra kell különösen nagy figyelmet fordítaniuk?*
- ✓ *az adatfeldolgozóknak nemcsak a saját adatkezeléseiket kell nyilvántartaniuk, hanem ettől elkülönítve egy külön nyilvántartásban az adatkezelők megbízása alapján végzett adatfeldolgozási tevékenységeiket*[197] *is.*
- ✓ *nyilván kell tartaniuk az adatvédelmi incidenseinket*[198] *függetlenül attól, hogy azokat be kell-e jelenteni a felügyeleti hatóság felé, illetve azok milyen kockázatot jelentenek az érintettek érdekeire, jogaira és szabadságaira nézve.*

Adatkezelések nyilvántartása

Az adatkezelőként a felelősségi körünkben végzett adatkezelési tevékenységekről nyilvántartást kell vezetnünk, amelynek a kötelező a tartalma:

- ✓ az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnk a neve és elérhetősége;
- ✓ az adatkezelés céljai;
- ✓ az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
- ✓ olyan címzettek kategóriái, akikkel a személyes adatokat közöljük vagy közölni fogjuk, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
- ✓ adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a GDPR 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;
- ✓ ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők;
- ✓ ha lehetséges, a GDPR 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

[196] GDPR 30. cikk (1) bekezdés
[197] GDPR 30. cikk (2) bekezdés
[198] GDPR 33. cikk (5) bekezdés

A francia adatvédelmi hatóság (CNIL) gyakorlatából

A CNIL egy vizsgálatban megállapította, hogy

- ✓ *a megfigyelő kamerák olyan személyes adatokat rögzítettek, amelyek nem voltak megfelelőek, mivel nem voltak relevánsak és nem korlátozódtak a szükségesre, ezért az adatkezelő megsértette az adattakarékosság elvét [GDPR 5. cikk (1) bekezdés c) pont];*
- ✓ *az érintettek nem kaptak tájékoztatást a személyes adataik gyűjtéséről és az adatok tárolási időtartamáról [GDPR 13. cikkének sérelme];*
- ✓ *a kamerák karbantartásával foglalkozó informatikai szolgáltató adatfeldolgozónak minősíthető, azonban az adatfeldolgozó és az adatkezelő közötti megkötött megállapodás nem tartalmazott olyan intézkedést, amely az adatkezelés biztonságára vonatkozóan elegendő garanciát nyújtott volna;*
- ✓ *a kamerák által rögzített és az adatkezelő kezelőszoftverén keresztül lekérdezett személyes adatok nem voltak titkosítva, és könnyen hozzáférhetőek voltak [GDPR 28. és 32. cikkének sérelme];*
- ✓ *az adatkezelő nem tett eleget az adatkezelési tevékenységek nyilvántartására vonatkozó kötelezettségének [GDPR 30. cikk (1) bekezdés].*[199]

Adatfeldolgozások nyilvántartása

A GDPR alapján adatfeldolgozóként nyilvántartást kell vezetnünk az adatkezelő nevében végzett adatkezelési tevékenységeink minden kategóriájáról, melynek kötelező tartalma:

- ✓ az adatfeldolgozó vagy adatfeldolgozók neve és elérhetőségei, és minden olyan adatkezelő neve és elérhetőségei, amelynek vagy akinek a nevében az adatfeldolgozó eljár, továbbá – ha van ilyen – az adatkezelő vagy az adatfeldolgozó képviselőjének, valamint az adatvédelmi tisztviselőnek a neve és elérhetőségei;
- ✓ az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái;
- ✓ adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a GDPR 49. cikk (1) bekezdésének második albekezdése szerinti továbbítás esetében a megfelelő garanciák leírása;
- ✓ ha lehetséges, a GDPR 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

[199] Décision MED-2019-025 du 5 novembre 2019. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000039466203/, utolsó letöltés 2022. 07. 30.

Az előzőekben említett nyilvántartásokat írásban kell vezetnünk (ideértve az elektronikus formátumot is), valamint megkeresés alapján a felügyeleti hatóság rendelkezésére kell tudnunk bocsátani azokat.

Ezen nyilvántartási kötelezettségek nem vonatkoznak a 250 főnél kevesebb személyt foglalkoztató vállalkozásra vagy szervezetre kivéve akkor,

- ✓ ha az általunk végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár,
- ✓ ha az adatkezelés nem alkalmi jellegű, vagy
- ✓ ha az adatkezelés kiterjed a személyes adatok különleges kategóriáinak vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére.

Példa a nyilvántartási kötelezettségre

- ✓ *egy mikrovállalkozás valószínűleg rendszeresen kezeli a munkavállalóira vonatkozó személyes adatokat, így ez az adatkezelés nem tekinthető „alkalmi„ adatkezelésnek, tehát ezt a tevékenységet szerepeltetni kell az adatkezelések nyilvántartásban. Más, ténylegesen alkalmi adatkezelési tevékenységeket azonban nem kell felvenni az adatkezelési tevékenységek nyilvántartásába, feltéve, hogy azok valószínűleg nem jelentenek kockázatot az érintettek jogaira és szabadságaira nézve, és nem tartalmaznak különleges adatok kategóriájába tartozó vagy büntetőítéletekkel és bűncselekményekkel kapcsolatos személyes adatokat.*

Az elszámoltathatóság elvének megfelelve meg kell oldanunk az erre vonatkozó konkrét jogszabályi előírás hiányában is – többek között –

- ✓ az adattovábbítások (megosztások) regisztrálását, hiszen ennek hiányában hogyan tudunk beszámolni arról, hogy kikkel is osztottuk meg egy adott érintett vagy az érintettek egy csoportjának a személyes adatait;
- ✓ az érintetti kérelmek nyilvántartását (ismétlődő kérelmek regisztrálása, kérelem GDPR-ban foglaltak szerinti teljesítésének igazolása stb. érdekében);
- ✓ a direkt marketing üzenetek ellen tiltakozók nyilvántartását (pl. e-mail címek adatbázisa, amelyekre a továbbiakban tilos levelet küldenünk); az ilyen listát „Robinson listának” hívják.

Jogszabályok:

GDPR

A személyes adatok kezelésére vonatkozó elvek [5. cikk és a (39), (40), (41), (42), (43), (44), (45), (46), (47), (48), (49), (50), (155) preambulumbekezdések]
Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések [12. cikk és (58)-(59) preambulumbekezdések]
Rendelkezésre bocsátandó információk, ha a személyes adatokat az érintettől gyűjtik [13. cikk és (60)-(62) preambulumbekezdések]
Rendelkezésre bocsátandó információk, ha a személyes adatokat nem az érintettől szerezték meg [14. cikk]
Az érintett hozzáférési joga [15. cikk és (63)-(64) preambulumbekezdések]
Az adatkezelési tevékenységek nyilvántartása [30. cikk és (13), (39) és (82) preambulumbekezdések]

ADATTÍPUSOK I.: A SZEMÉLYES ADAT

A személyes adat fogalma

Sokféle adatot bízhatnak ránk, adatkezelőkre – ezek közül van, amit az érintettek önként, van, amit pedig muszájból adnak át, az adott adatkezelésünk körülményeitől függően.

***Sokféle adatot kezelhetünk**, például*

- ✓ *munkavállalók adatait (név, beosztás, munkakör, TAJ szám, adóazonosítójel, bankszámlaszám, házastárs és gyermekek adatai, geolokációs adatok stb.),*
- ✓ *üzleti partnerek adatait (cégnév, képviselő neve, tevékenységi kör, ajánlatok és szerződések tartalma stb.),*
- ✓ *termeléssel, szolgáltatásokkal kapcsolatos adatok (termékspecifikációk, az adott szolgáltatások nyújtásával kapcsolatos adatok, marketing, panaszkezelés stb.)*
- ✓ *gazdálkodással kapcsolatos adatok (beszámolókban, üzleti és projekttervekben található adatok, foglalkoztatással kapcsolatos adatok stb.)*
- ✓ *üzleti titkokat képező adatok (kutatással és fejlesztéssel kapcsolatos adatok, know-how, szabadalmak stb.)*
- ✓ *szolgálati/államtitkot képező adatok stb.*

Ezen adatok titokban maradásához jelentős érdekünk fűződhet és – ideális esetben – mindent meg is teszünk annak érdekében, hogy ezek ne tudódjanak ki, akár személyes adatról, akár más védendő adatról van szó (pl. üzleti/szolgálati titok stb.).

A személyes adatok közül mindenképpen megemlítendőek

- ✓ a természetes személyazonosító adatok, amelyek az adott személy
  - a) családi és utóneve, születési családi és utóneve,
  - b) születési helye,
  - c) születési ideje és
  - d) anyja születési családi és utóneve.[200]
- ✓ az azonosító kódok, amelyek olyan, matematikai módszerrel képzett, különleges adatra nem utaló számjegysorok, amely a személyt az adatkezelés során egyértelműen azonosítja. Ilyen kód például
  - a) az adóazonosító jel (adózással kapcsolatos nyilvántartás azonosító kódja)
  - b) a Társadalombiztosítási Azonosító Jel („TAJ szám”, az egészségügyi, a szociális és a társadalombiztosítási és a magánnyugdíj rendszerrel kapcsolatos nyilvántartások azonosító kódja)

[200] a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról1 szóló 1996. évi XX. törvény 4.§ (4) bekezdés

c) a személyi azonosító (a személyiadat- és lakcímnyilvántartás azonosító kódja).[201]

Az adóazonosító jel képzésének szabályai

1. Az adóazonosító jel tízjegyű szám.

2. Az adóazonosító számot az alábbiak szerint kell képezni:
a) az 1. számjegy konstans 8-as szám, mely az adóalany magánszemély voltára utal,
b) a 2-6. számjegyek a személy születési időpontja és az 1867. január 1. között eltelt napok száma,
c) a 7-9. számjegyek az azonos napon születettek megkülönböztetésére szolgáló véletlenszerűen képzett sorszám,
d) a 10. számjegy az 1-9. számjegyek felhasználásával matematikai módszerekkel képzett ellenőrző szám.

3. Az adóazonosító jel 10. számjegyét úgy kell képezni, hogy a 2. a)-c) pontok szerint képzett 9 számjegy mindegyikét szorozni kell azzal a sorszámmal, ahányadik helyet foglalja el az azonosítón belül. (Első számjegy szorozva eggyel, második számjegy szorozva kettővel és így tovább.)

Az így kapott szorzatok összegét el kell osztani 11-gyel, és az osztás maradéka a 10. számjeggyel lesz egyenlő. A 2. c) pont szerinti születési sorszám nem adható ki, ha a 11-gyel való osztás maradéka egyenlő tízzel.

A Társadalombiztosítási Azonosító Jel képzésének szabályai

A TAJ szám egy kilenc számjegyből álló szám, amelyben az első nyolc számjegy egy folyamatosan kiadott egyszerű sorszám, amely mindig az előző, utoljára kiadott sorszámból egy hozzáadásával keletkezik. A kilencedik számjegy ellenőrző ún. CDV kód, melynek képzési algoritmusa az alábbi:

A TAJ szám első nyolc számjegyéből a páratlan helyen állókat hárommal, a páros helyen állókat héttel szorozzuk, és a szorzatokat összeadjuk. Az összeget tízzel elosztva a maradékot tekintjük a kilencedik, azaz CDV kódnak.

[201] a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról1 szóló 1996. évi XX. törvény 5-6.§

A személyi azonosító képzésének szabályai
I. Az 1997. január 1. előtt születettek esetében

1. A személyi azonosító tizenegy jegyű szám.

2. A személyi azonosítót az alábbiak szerint kell képezni:
a) az 1. számjegy a polgár állampolgárságát, születésének évszázadát és nemét jelöli a következők szerint:

	1900. január 1. után született		*1900. január 1. előtt született*	
állampolgárság	*férfi*	*nő*	*férfi*	*nő*
magyar	*1*	*2*	*3*	*4*
nem magyar	*5*	*6*	*7*	*8*

b) a 2-7. számjegyek a polgár születési évének utolsó két számjegyét, a születés hónapját és napját tartalmazzák;
c) a 8-10. számjegyek az azonos napon születettek születési sorszáma;
d) a 11. számjegy az 1-10. számjegyek felhasználásával, matematikai módszerekkel képzett ellenőrző szám.

3. A személyi azonosító 11. számjegyét úgy kell képezni, hogy a 2. a)-c) pontok szerint képzett tíz számjegy mindegyikét szorozni kell azzal a sorszámmal, ahányadik helyet foglalja el a személyi azonosítón belül. (Első számjegy szorozva eggyel, a 2. számjegy szorozva kettővel és így tovább.) Az így kapott szorzatokat össze kell adni és az összeget tizeneggyel elosztani. Az osztás maradéka a 11. számjeggyel lesz egyenlő. A 2. c) pont szerinti születési sorszám nem osztható ki, ha tizeneggyel való osztás maradéka egyenlő tízzel.

4. Az 1996. december 31-e után képzett személyi azonosító az állampolgárságra utaló adatot nem tartalmaz, azaz a jelzett időpont után képzett személyi azonosító 1. számjegye csak 1, 2, 3 vagy 4 lehet a 2000 előtt született polgárok esetében.

5. A hontalan polgárt – a hontalan, Magyarországon született gyermeke kivételével – a nem magyar állampolgárságnak megfelelő személyi azonosítóval kell ellátni.

II. 1996. december 31-e után születettek esetében

1. A személyi azonosító tizenegy jegyű szám.

2. A személyi azonosítót az alábbiak szerint kell képezni:
a) az 1. számjegy az állampolgár születésének évszázadát és nemét jelöli a következők szerint:

1997. 01.01 – 1999. 12.31 között született		*1999.12. 31. után született*	
férfi	*nő*	*férfi*	*nő*
1	*2*	*3*	*4*

b) a 2-7. számjegyek a polgár születési évének utolsó két számjegyét, a születés hónapját és napját tartalmazzák;
c) a 8-10. számjegyek az azonos napon születettek születési sorszáma;
d) a 11. számjegy az 1-10. számjegyek felhasználásával, matematikai módszerekkel képzett ellenőrző szám.

3. A személyi azonosító 11. számjegyét úgy kell képezni, hogy a 2. a)-c) pontok szerint képzett számjegy mindegyikét meg kell szorozni egy számmal, mégpedig a 10. helyen állót eggyel, a 9. helyen állót kettővel és így tovább. A szorzatokat össze kell adni, és az összeget tizeneggyel elosztani.

A 2. c) pont szerinti születési sorszám nem osztható ki, ha a tizeneggyel való osztás maradéka egyenlő tízzel.[202]

Adatkezelőként az érintettel, illetve más adatkezelővel való, meghatározott célú kapcsolattartása során csak azt az azonosító kódot használhatjuk, amelyre a feladatot meghatározó törvény felhatalmazott minket. Amennyiben nincs ilyen felhatalmazó jogszabály, akkor ezen azonosító kódokat csak az érintett előzetes, a GDPR 4. cikk 11. pontja szerinti hozzájárulása vagy az ügyintézési rendelkezésben tett hozzájárulása alapján használhatjuk fel. Az érintettet a hozzájárulás megadása, megtagadása, illetve visszavonása miatt hátrány nem érheti, a hozzájárulás megadásáért bármilyen előny kilátásba helyezése tilos.[203]

Az adatok természetétől függően különböző jogszabályi környezet lehet irányadó a kezelésükre. A személyes adatokra – alapvetően – az adatkezelésünk céljától függően a GDPR, az Infotv.[204] illetve az Eht.[205] vonatkozik olyan ágazati jogszabályokkal

[202] a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény 1-3. sz. mellékletek
[203] a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény 7.§
[204] az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény („Infotv.")
[205] elektronikus hírközlésről szóló 2003. évi C. törvény („Eht.")

kiegészítve, mint például a Mt.[206], az Nkt.[207], az Eüak.[208] vagy az Szvtv.[209] Ilyen ágazati jogszabályból több mint kétszáz van, amennyiben jogszerűen akarjuk végezni a feladatainkat, a szakterületünkre vonatkozó speciális előírások ismerete elengedhetetlen.

Mi az a személyes adat?

Személyes adat: azonosított vagy azonosítható természetes személyre („**érintett**”) vonatkozó bármely információ; **azonosítható az a természetes személy**, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.[210]

A GDPR alapján tehát

- ✓ személyes adat bármely információ, amely azonosított vagy azonosítható természetes személyre vonatkozik,
- ✓ az állat és a növény nem természetes személy,
- ✓ nem számít bele a természetes személy fogalmába az elhunyt személy sem, az ő adatai kezelésével kapcsolatban az Infotv. tartalmaz rendelkezéseket.

Nem olyan egyszerű annak kiderítése, hogy egy adat személyes adat vagy sem, mivel ugyanaz az adat az egyik esetben lehet személyes adat, míg a másikban nem, ezt pedig mindig az adott helyzet dönti el.

Példa a személyes adatra

- ✓ *személyes adat például a név, a személyes azonosító, a tartózkodási hely és az online azonosító, köztük az IP-cím is, amennyiben az egy személyhez és nem egy nagyvállalathoz vagy laktanyához köthető.*
- ✓ *termelés szempontjából egy gép termelési adatai lehetnek „csak” műszaki adatok, ám lehetnek annak a munkavállalónak a személyes adatai is, aki az adott műszakban azzal a géppel valamilyen terméket állít elő, sőt akár ezen teljesítmény adatok egyben a munkabérének megállapításához szükséges adatok is lehetnek.*
- ✓ *egy gépjármű adatai lehetnek „csak” műszaki adatok, ám lehetnek annak a szerelőnek a személyes adatai is, aki a járművet karbantartja, illetve azé is, aki az adott autót vezeti / üzemelteti / tulajdonosi jogokat gyakorolja felette.*
- ✓ *egy kép városunk panorámájával még nem személyes adat, azonban, ha megjelöltük rajta nagy piros ikszel, hogy melyik házban lakik az általunk hőn szeretett vagy éppen végletekig utált politikus nagyon-nagyon közeli,*

[206] a munka törvénykönyvéről szóló 2012. évi I. tv. („Mt.”)
[207] a nemzeti köznevelésről szóló 2011. évi CXC. törvény („Nkt.”)
[208] az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény
[209] a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény („Szvtv.”)
[210] GDPR 4. cikk 1. pont

bizalmas és rettentő módon titkolni kívánt ismerőse, a semleges, személyes adatot nem tartalmazó információ (jelen esetben a panorámakép) máris személyes adattá válik. Ha pedig ez a közeli ismerős még a nagyon-nagyonnál is közelibb ismerős, akár ez az adat különleges adat is lehet, olyan például, amely a hőn szeretett vagy éppen utált politikus szexuális preferenciájára utal.

A GDPR ad néhány kapaszkodót, mi is az a személyes adat. Így személyes adat különösen

- ✓ a név,
- ✓ szám,
- ✓ helymeghatározó adat,
- ✓ online azonosító vagy
- ✓ a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező, amely alapján a személy azonosítható.

Ez azonban csak egy példálódzó felsorolás, a sort a végtelenségig folytathatnánk az adott személy kedvenc sütijétől kezdve az ölebének csipszámán keresztül egészen addig, hol és kivel meg mennyiért töltötte a jól megérdemelt szabadságát tavaly nyáron.

Az EUB gyakorlatából

„(…) az azonosítható személy olyan személy, aki nemcsak közvetlen, hanem közvetett módon azonosítható.
A „közvetlenül" kifejezés uniós jogalkotó által történő alkalmazása azt jelzi, hogy annak érdekében, hogy valamely adatot személyes adatnak lehessen minősíteni, nem szükséges, hogy ezen adat önmagában lehetővé tegye az érintett személy azonosítását.

(…) az elektronikus médiaszolgáltató által a nyilvánosság számára hozzáférhetővé tett internetes honlap valamely személy által történő felkeresésekor az e szolgáltató által rögzített dinamikus IP-cím az említett szolgáltató tekintetében a (…) személyes adatnak minősül, amennyiben jogszerű eszközök állnak a rendelkezésére az érintett személynek az e személy internet-hozzáférést nyújtó szolgáltatójának rendelkezésére álló további adatok révén történő azonosításához." (A 2016. október 19-i Breyer ítélet (C-582/14, EU:C:2016:779)[211]

„(…) valamely vizsgázó által egy szakmai vizsga során adott írásbeli válaszok és a vizsgáztatónak az e válaszokra vonatkozó esetleges megjegyzései (…) személyes adatoknak minősülnek" (a 2017. december 20-i Nowak ítélet (C-434/16, ECLI:EU:C:2017:994)[212]

[211] Az Európai Unió Bírósága Kutatási és Dokumentációs Igazgatóság: A személyes adatok védelme, Tematikus tájékoztató, 2020. július (11.o.)
[212] Az Európai Unió Bírósága Kutatási és Dokumentációs Igazgatóság: A személyes adatok védelme, Tematikus tájékoztató, 2020. július (13.o.)

Az, hogy egy adat személyes adat vagy sem, az elsősorban attól függ, hogy az a bizonyos adat vonatkozik-e egy adott személyre.

A WP 29. cikk szerinti adatvédelmi munkacsoport gyakorlatából

„egyénre vonatkozik az adat, ha az egyén azonosságára, tulajdonságaira vagy viselkedésére utal, vagy ha az ilyen információt annak meghatározására vagy befolyásolására használják, ahogyan az adott személyt kezelik vagy értékelik."[213]

Annak érdekében, hogy az adatot egyénre „vonatkozónak" lehessen tekinteni, „tartalom" elemnek, vagy „cél" elemnek, vagy pedig „eredmény" elemnek kell jelen lennie.

- ✓ A „tartalom" elem azokban az esetekben van jelen, ahol az információt egy adott személyről adjuk meg, tekintet nélkül adatkezelőként a mi vagy harmadik személy részéről fennálló bármiféle célra, vagy az információnak az érintettre gyakorolt hatására. Az információ akkor „vonatkozik" egy személyre, amikor az adott „személyről" szól
  - o a munkáltató nyilvántartásaiban a munkavállalóról szóló információk szerepelnek (bér, béren kívüli juttatások, ledolgozott órák száma stb.)
  - o a bankban a bank nyilvántartásában a bank ügyfeleiről szóló információk szerepelnek (bankszámlaszám, tranzakciók, hitellel kapcsolatos adatok stb.)
- ✓ A „cél" elemet akkor tekinthetjük meglévőnek, amikor az adatot – az eset valamennyi körülményét figyelembe véve – abból a célból használjuk fel vagy használjuk fel valószínűleg, hogy az érintett státuszát vagy viselkedését értékeljük, bizonyos bánásmódban részesítsük vagy befolyásoljuk.
- ✓ Az „eredmény" elem akkor van jelen, amennyiben az adat felhasználása valószínűleg hatással van egy adott személy jogaira és érdekeire, figyelembe véve az adott eset valamennyi körülményét. A lehetséges eredménynek nem feltétlenül kell jelentős hatásúnak lennie, az is elegendő, ha az érintettet az ilyen adatok kezelésének eredményeként a többiektől eltérő bánásmódban részesíthetjük.[214]

Ha kétségünk van, személyes adattal állunk-e szemben, íme néhány kérdés segítségül:

- ✓ az adott adat természetes személyre vonatkozik-e vagy sem?
- ✓ az adott adat közvetlenül az egyénről vagy a tevékenységéről szól-e?
- ✓ mi az adat kezelésével a célunk és mi az adott adatkezeléstől elvárt eredmény, illetve mi ezeknek az egyénre gyakorolt hatása?

Nem szabad meglepődnünk, ha egy-egy esetben nehéz meghatároznunk, hogy egy bizonyos adat személyes adat-e vagy sem. Bármilyen kétségünk is van, az még nem

[213] A munkacsoport 105. számú dokumentuma: „Munkadokumentum az RFID-technológiával kapcsolatos adatvédelmi kérdésekről", elfogadva 2005. január 19-én

[214] A 29. CIKK ALAPJÁN LÉTREHOZOTT ADATVÉDELMI MUNKACSOPORT: 4/2007 vélemény a személyes adat fogalmáról, 01248/07/HU WP 136, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf, utolsó letöltés 2022. 08. 19.

jogosít fel bennünket arra, hogy trehányul bánjuk ezzel a bizonyos adattal. És azt sem szabad egy pillanatig sem szem elől tévesztenünk, hogy a pontatlan, hibás adat is személyes adat akkor, ha az azonosítható személyre vonatkozik.

A norvég adatvédelmi hatóság (Datatilsynet) gyakorlatából

A Dragefossen AS (társaság) kamerát szerelt fel annak az épületnek a tetejére, amelyben működött. A kamera 360 fokban forgott és négy meghatározott szögben állt meg 15-15 másodpercre. A kamera minden egyes teljes forgáshoz körülbelül két percet használt fel. A társaság a felvétel minősége és távolsága miatt úgy ítélte meg, hogy a rendszámtáblák vagy az arcok nem lesznek felismerhetők. A felvételeket 14 napig tárolták, külön erre a célra fenntartott szerveren és több alkalommal megosztották a rendőrséggel a városközpontban történt eseményekkel kapcsolatban.

Az adatvédelmi hatóság egyetértett azzal, hogy a távolság és a felvétel minősége miatt nem valószínű, hogy a rendszámtáblák vagy az emberek arca felismerhetőek lennének, azonban kiemelte, hogy

- ✓ *felismerhető lenne, hogy valaki milyen autót vezet, milyen ruhát visel, milyen a hajszíne és a hozzávetőleges frizurája*
- ✓ *a napirendről, vásárlási szokásokról, az autóról vagy a kinézetről való előzetes ismeretek alapján a barátai, családtagjai vagy a kollégái képesek lennének azonosítani a felvételen szereplő személyt.*

Ezt támasztotta alá az is, hogy a rendőrség több alkalommal is hozzáférést kért a felvételekhez a városközpontban történt eseményekkel kapcsolatban.
Az adatvédelmi hatóság megállapította, hogy a felvételek az általános adatvédelmi rendelet 4. cikkének (1) bekezdése értelmében személyes adatokat rögzítenek. [215]

Az adatvédelmi tudatossággal kapcsolatos kutatásunkban résztvevők a személyes adatok közül számos fogalmat ismertek, leggyakrabban a lakcímet, a nevet, a születés dátumot és helyet, valamint a telefonszámot említették meg, mint személyes adatot. A megkérdezettek összesen 41 különböző fogalmat társítottak a személyes adatokhoz.

Említésre méltó, hogy a nevek esetében jellemzően az édesanya neve merült fel, mint személyes adat, az édesapát 160 főből csak 3 jelölte meg. Két megkérdezett pedig a személyes adatok között megemlítette a „nemzetbiztonsági" és „államtitok" kifejezést is.

[215] Datatilsynet (Norway) – 20/01627, https://www.datatilsynet.no/contentassets/bb8618c1ce604468b3b478676bf196c5/vedtak-om-overtredelsesgebyr---dragefossen-as.pdf, utolsó letöltés: 2022. 07. 17.

Ki az az azonosított személy?

Azonosított személy az, aki esetében egyértelmű, hogy kiről is beszélünk és mit mondunk róla – az azonosításhoz pedig olyan adatok szükségesek, amelyek úgy írnak le egy adott személyt, hogy az minden más személytől megkülönböztethető és önálló egyénként azonosítható.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„egy ilyen összetett adatkezelés esetén nem az határozza meg a személyes adat jelleget, hogy egy alrendszeren belül azonosítható-e az érintett. Az Ügyfélnek jogszerűen rendelkezésére álló valamennyi adatforrást vizsgálni szükséges ahhoz, hogy a közvetlen vagy közvetett azonosíthatóság feltétele fennáll-e. Az álnevesítés (pszeudonim azonosítók használata) adatbiztonságot növelő körülmény, de nem befolyásolja az egyedi azonosító jelleget és a személyes adat minőséget a harmadik személy érintett hívók vonatkozásában."[216]

Adatkezelőként tengernyi adatot kezelhetünk egy-egy személyről. Ott vannak például a természetes azonosító adatok, azaz a születési név, a születési időpont és hely, valamint az édesanya születési neve. Azonban egy adott személy ennél sokkal több, hiszen hús-vér emberként jön-megy és dolgozik, sportol, gyermekeit óvodába-iskolába járatja, az okos telefonján a neten böngész, okos fogkefével mos fogat és okos porszívóval szedetti fel a macskájának elhullajtott szőrét a parkettáról, ha ideje engedi barátkozik vagy épp vásárolgat, hétvégenként pedig családjával kirándul vagy kedvenc hobbijának hódol. Hogy mi adatkezelőként milyen adatokat tartunk nyilván egy adott érintettről az attól függ, milyen kapcsolatban állunk az adott személlyel – alkalmazottja-e a szervezetünknek vagy ügyfele, szolgáltatásaink után érdeklődik vagy a panaszával áraszt el minket.

Példa

- ✓ *egy szervezet HR munkatársaként szinte mindent tudhatunk egy-egy alkalmazottról (bankszámlaszám, másodállás, házastárs és gyermekek neve, kora, iskoláztatásra vonatkozó adatok, cafeteria preferenciák, betegség, védőoltások megléte, munkahelyen alkoholfogyasztás stb.)*
- ✓ *egy átlagos általános iskolai osztályfőnök sokkal többet tud meg a rá bízott diákokról és szüleikről, mint amennyit azok valaha is szeretnének (életmód, lakáskörülmények, tanulási nehézségek, testvérkapcsolatok minősége, világnézet, politikai álláspont, szülők válása, családon belüli erőszak, gyermek sérelmére elkövetett bűncselekmények stb.)*
- ✓ *egy fitnesz alkalmazás fejlesztője megismeri a felhasználók lokációs és egészségügyi adatait, sportolási szokásait, közösségi médiás megosztásait stb.*
- ✓ *társkereső alkalmazás fejlesztője megismeri a szolgáltatásra bejelentkező életkorát, az önmagáról átadott információkat (kinézet, iskolai végzettség, foglalkozás, hobbik), preferenciáit (milyen tulajdonságokkal rendelkező*

[216] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: 2022. 07. 17.

társat keres), lokációs adatait, illetve számos különleges adatát is (világnézet, egészségi állapot, szexuális irányultság és preferenciák stb.)

Ezek az információk akár profilozásra is alkalmasak lehetnek és akadhat köztük számos olyan adat is, amelyeket az érintettek nagyon nem szeretnének nagy nyilvánosság elé tárni.

Vajon mennyire fog felháborodni egy munkatársunk, ha megtudja, mennyivel kevesebb/több fizetést kap ugyanazért a munkáért, mint a vele szemben ülő kollégája? Nagyon? Okozhat ez a kiszivárgott információ elégedetlenséget, munkahelyi feszültséget, nem kívánt fluktuációt, netalán üzleti/szolgálati titoksértést?

Mit szólna a munkatársunk felesége, ha megtudná, nem is túlórázott a férje, pedig otthon azt mondta? Milyen következtetéseket vonna le abból, hogy hazugságon kapta, még akkor is, ha csak annyi a bűne, hogy egy régen látott ismerősével beszélgetett teljesen ártalmatlan dolgokról és otthon csak azért nem mondta el, mert attól félt, úgysem hinnének neki?

A személyes adatok nem megfelelő kezelése (például jogosulatlan közlése) szinte felmérhetetlen nagyságrendű kárt okozhat nemcsak a családi és párkapcsolatokban hanem a helyi pletykafolyamba kerülve akár diszkriminációhoz, bizalomvesztéshez, az érintett megszólásához, kiközösítéséhez is vezethet. Adatkezelőként pedig nincs mentségünk, az ilyen esetekért – jogi, erkölcsi és anyagi – felelősséget kell vállalnunk.

Kik az azonosítható személyek?

Az, hogy ki számít azonosított személynek viszonylag még egyszerű kérdés, ám adatkezelőként kezelhetünk olyan adatokat is, amelyek nem azonosított személyekre vonatkoznak, azonban ettől még ezek az adatok egyáltalán nem biztos, hogy elvesztették a személyes adat minőségüket.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„a hívás mindkét szereplője egyértelműen azonosítható az Ügyfél által, amelyet az Ügyfél a rendszer normál működése során folyamatosan meg is tesz azok vonatkozásában, akiknek a rögzített hívásait visszahallgatják és utána ez alapján adott esetben vissza is hívják, vagy a telefonos ügyfélszolgálaton dolgozó munkavállalót értékelik ez alapján. Amennyiben ezt nem tenné meg az Ügyfél, de meg lenne rá a lehetősége, akkor is személyes adat lenne a Szoftver általi elemzés eredménye mindaddig, amíg visszafordíthatatlanul meg nem szűnik a kapcsolata adott azonosítható érintettekkel.”[217]

Mikor illeti meg ezeket az adatokat a személyes adatokat megillető védelem? Akkor, ha ezen adatok alapján azonosítható a természetes személy akár közvetlen, akár közvetett módon.

[217] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: 2022. 07. 17.

Az azonosíthatóság szempontjából a döntő az, hogy valószínű-e, hogy rendelkezésre fognak-e állni az azonosítás észszerű eszközei és az adatok előre tervezett felhasználói felhasználják-e azokat. Ebben az esetben nemcsak a saját tudásunkból és rendelkezésre álló eszközeinkből kell kiindulnunk, hanem a harmadik fél adatátvevőit is számításba kell vennünk.

Az egyén nem minősül „azonosíthatónak" abban az esetben, ha azonosítása észszerűtlenül sok időt, erőfeszítést vagy erőforrásokat igényel, ez azonban az új, innovatív technológiák (pl. Big Data, mesterséges intelligencia) használata miatt egyre ritkábban fordul elő.

Példa az azonosíthatóságra

- ✓ *egy munkahelyen van 50 ugyanolyan munkakörben dolgozó személy és elterjed a pletyka, miszerint az egyikük elő lesz léptetve vezetőnek. Ekkor még nem tudjuk, hogy kiről is van szó. Ám ha egy újabb adattal bővül a folyosói suttogás, miszerint a vörös hajú ez az illető és csak 5 ilyen személy van az ötven munkatárs között, azaz máris jelentősen leszűkült a szóba jöhető személyek száma. Ha pedig további adatok kerülnek elő, például a Szezám utcában lakik és Buksinak hívják a vizsláját, az adott személy máris pontosan beazonosított lesz anélkül, hogy a neve akár csak egyszer is elhangzana. Hasonló találgatások azonban nemcsak az előléptetéssel kapcsolatban lehetnek, hanem arról is, hogy ki lopta ki a Túró Rudit a közös hűtőből és ki járkál a jelenlegi vezető kikapós feleségéhez akkor, amikor a férje éppen a közeli búfelejtőben tölti az idejét.*
- ✓ *lokációs adatokból meglehetős pontossággal visszaazonosítható az adott eszköz és annak gazdája (pl. abból, hogy minden éjszaka ugyanott van az eszköz), illetve vészhelyzetet jelző eszköz is minden további nélkül megtalálható akkor is, ha a tulajdonosának fogalma sincs arról, hogy van ilyen funkciója a kütyüjének (pl. unoka ajándékba ad okosórát a nagyapának és az óra, amikor elájul a viselője aktiválja a segélykérő funkciót).*

Az adatkezelések során figyelemmel kell lennünk arra, hogy a Big Data és a mesterséges intelligencia új távlatokat nyit az azonosíthatóságban – hatalmas mennyiségű adat szinte korlátlan elemezhetőségével, például az anonimizált GPS adatokból pontosan kideríthető, hogy egy adott celeb szülinapi buliján pontosan milyen más celebek vettek részt, elég csak az adott időben egy helyen tartózkodó autók/telefonok jeleit visszakövetni.

Amikor több személyre vonatkozik ugyanaz az adat

Ugyanazon információ vonatkozhat több természetes személyre is, és ebben az esetben – feltéve, hogy azonosított vagy azonosítható személyekről van szó – ez az információ személyes adatnak minősül. Ilyen eset lehet például az, amikor az írásbeli vizsgán a vizsgázó válaszaihoz a vizsgáztató megjegyzéseket ír – ebben az esetben ezek a megjegyzések a vizsgázónak a vizsga során adott válaszaihoz hasonlóan az e vizsgázóra vonatkozó információnak minősülnek, mivel ezen megjegyzések a vizsgázó vizsga során nyújtott egyéni teljesítményére, közelebbről az érintett területen fennálló ismereteire és tudására vonatkozó véleményét vagy értékelését tükrözik.

„*Ugyanazon információ vonatkozhat (...) több természetes személyre is, és azok tekintetében, feltéve hogy azonosított vagy azonosítható személyekről van szó, (...) személyes adatnak minősül.*”[218]

Azonosítást nem igénylő adatkezelések

Ha azok a célok, amelyekből a személyes adatokat kezeljük, nem vagy már nem teszik szükségessé az érintett azonosítását, nem vagyunk kötelesek kiegészítő információkat megőrizni, beszerezni vagy kezelni annak érdekében, hogy pusztán azért azonosítsuk az érintettet, hogy megfeleljünk a GDPR előírásainak.

Amennyiben bizonyítani tudjuk, hogy nem vagyunk abban a helyzetben, hogy azonosítsuk az érintettet, abban az esetben erről lehetőség szerint őt megfelelő módon tájékoztatnunk kell. Ilyen esetekben a GDPR 15–20. cikkeit (hozzáférési, helyesbítésre és törlésre, korlátozásra, valamint az adathordozhatósági jogra vonatkozó cikkeket) nem kell alkalmaznunk, kivéve, ha az érintett abból a célból, hogy ezen cikkek szerinti jogait gyakorolja, kiegészítő információkat nyújt annak érdekében, hogy az azonosítását újra lehetővé tegye.

[218] EUB C-434/16. sz. ügy („Peter Nowak ítélet”), https://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=HU&mode=lst&dir=&occ=first&part=1&cid=3920846, utolsó letöltés 2022. 08. 20.

MILYEN FELTÉTELEKKEL KEZELHETÜNK SZEMÉLYES ADATOKAT?

Jogalapok

Milyen felvételekkel kezelhetünk személyes adatokat? A GDPR alapelveinek, például a jogszerűség elvének következetes betartásával. De hogyan tudunk adatkezelőként megfelelni a jogszerűség alapelvének?

Elsősorban úgy, hogy minden egyes adat kezelése esetén jogszerűen kell tudnunk hivatkoznia a GDPR 6. cikk (1) bekezdésében foglalt jogalapok egyikére, illetve különleges adatok kategóriájába tartozó, valamint a bűnügyi adatok esetében a különleges adatok kategóriájába tartozó adat kezelhetőségét lehetővé tevő feltételek (kivételek)[219] egyikére.

[219] Lásd GDPR 9. cikk (2) bekezdés

A GDPR hat jogalapot különböztet meg, csak ezek közül lehet választanunk. Még a tagállami szinten is tilos hetedik jogalapot kreálni, nemhogy adatkezelői szinten, a „mi így szoktuk" jogalap pedig nem létezik, bármennyire is szeretnénk, ahogy a „főnök ezt mondta", illetve „a központunk utasítása" sem. Erőből lehet ugyan próbálkozni, ám annak eredményességét számtalan – nyilvánosságra hozott – hatósági büntetés kérdőjelezi meg.

A GDPR 6. cikk (1) bekezdése az alábbiak szerint fogalmazza meg a jogalapokat:

> *(1) A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:*
> *a) az érintett **hozzájárulás**át adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;*
> *b) az adatkezelés olyan **szerződés** teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;*
> *c) az adatkezelés az adatkezelőre vonatkozó **jogi kötelezettség** teljesítéséhez szükséges;*
> *d) az adatkezelés az érintett vagy egy másik természetes személy **létfontosságú érdek**einek védelme miatt szükséges;*
> *e) az adatkezelés **közérdek**ű vagy az adatkezelőre ruházott **közhatalmi jogosítvány gyakorlás**ának keretében végzett feladat végrehajtásához szükséges;*
> *f) az adatkezelés **az adatkezelő vagy egy harmadik fél jogos érdekei**nek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.*
>
> *Az első albekezdés f) pontja nem alkalmazható a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre.*
>
> *(2) Az e rendeletben foglalt, adatkezelésre vonatkozó szabályok alkalmazásának kiigazítása érdekében, a tagállamok az (1) bekezdés c) és e) pontjának való megfelelés céljából fenntarthatnak vagy bevezethetnek konkrétabb rendelkezéseket, amelyekben pontosabban meghatározzák az adatkezelésre vonatkozó konkrét követelményeket, és amelyekben további intézkedéseket tesznek az adatkezelés jogszerűségének és tisztességességének biztosítására, ideértve a IX. fejezetben meghatározott egyéb konkrét adatkezelési helyzeteket is.*

Az érintett hozzájárulása [GDPR 6. cikk (1) bekezdés a) pont]

A magyar Alkotmánybíróság gyakorlatából

„Az egyén hozzájárulása esetén szabad akaratából gyakorolja önrendelkezési jogát, maga dönt magántitkainak feltárásáról, így e szabály nyilvánvaló, hogy nem korlátozza az önrendelkezési jogot, hanem épp ellenkezőleg: az önrendelkezést teszi lehetővé. Az információs önrendelkezési jog – mint ahogy a nevéből is következik –

az érintettnek biztosít döntési lehetőséget személyes adatai sorsát illetően, az egyén szabadon dönthet magánszférájának ilyen formában történő feltárásáról (…)"[220]

A „hozzájárulás" jogalapot akkor használhatjuk, ha az adatkezelésben érintett természetes személy hozzájárulását adja személyes adatai egy vagy több konkrét célból történő kezeléséhez. A hozzájárulásnak önkéntesnek, konkrétnak és megfelelő tájékoztatáson alapulónak kell lennie, valamint egyértelműen ki kell nyilvánítania a hozzájárulást adó személynek, hogy beleegyezését adja személyes adatai kezeléséhez.

Az osztrák adatvédelmi hatóság (DSB) gyakorlatából

Az utca túloldalán lévő irodára egy CCTV kamera volt irányítva. A hatóság érdeklődésére az adatkezelő azzal érvelt, hogy az utca használata a kamerás felvételhez való hozzájárulásnak minősül.
Az osztrák adatvédelmi hatóság úgy ítélte meg, hogy az utcán járás nem minősül egyértelmű hozzájárulásnak.[221]

A hozzájárulását adó személy jogosult arra, hogy ezt a hozzájárulást bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét és nekünk kell bizonyítanunk, hogy a hozzájárulásra hivatkozás esetén érvényes hozzájárulással rendelkeztünk.

Példa a hozzájárulásra hivatkozott adatkezelésre

- ✓ *hírlevelet küldünk természetes személyek számára és a szolgáltatásra feliratkozáskor a hozzájárulásukat kérjük az adataik kezeléséhez*
- ✓ *az általános iskolában felvételeket készítünk a gyerekekről és ehhez a szüleik hozzájárulását kérjük*
- ✓ *fitness appot üzemeltetünk és a felhasználóktól hozzájárulást kérünk ahhoz, hogy az adataikat a felhőnkben tároljuk*

A hozzájárulás követelményei

A GDPR kívánalmainak tökéletesen megfelelő hozzájárulás legfontosabb követelménye az, hogy az érintettnek a hozzájárulását szabad akaratából, konkrétan, megfelelő tájékoztatás alapján és egyértelműen kell megadnia. A „hallgatás beleegyezés" nem értelmezhető hozzájárulásként.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A tájékoztatás ahhoz szükséges, hogy az érintettek valóban éljenek az információs önrendelkezési jogukkal, és megfelelő információk birtokában valóban el tudják dönteni, hogy hozzájárulnak-e az adatkezeléshez. Egy hozzájáruló nyilatkozat

[220] 67/2011. (VIII. 31.) AB határozat, https://net.jogtar.hu/jogszabaly?docid=A11H0067.AB&txtreferer=99700047.TV, utolsó letöltés: 2022. 08. 27.
[221] DSB (Austria) – DSB-D123456, https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20210503_2021_0_285_169_00/DSBT_20210503_2021_0_285_169_00.html, utolsó letöltés: 2022. 07. 17.

aláírása megfelelő tájékoztatás hiányában nem jelenti a GDPR szerinti hozzájárulás meglétét."[222]

Az érintettnek a hozzájárulást nyilatkozattal vagy olyan egyértelmű megerősítő cselekedettel kell megadnia (például a honlapunkon egy négyzet kipipálásával), amely jelzi az adatkezeléshez való hozzájárulását. Ezt a hozzájárulást bármikor jogosult az érintett – következmények nélkül – visszavonni ugyanolyan könnyen, mint ahogy a hozzájárulását megadta, azaz nem kérhetünk az érintettől például plusz személyes adatot a visszavonáshoz. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelésünk jogszerűségét.

Ezen követelmények alapján mi adatkezelőként nem jelölhetjük be előre az „igen" négyzetet még akkor sem, ha az – véleményünk szerint – meggyorsítja vagy kényelmesebbé teszi a hozzájárulás megadását az érintett részéről, és az általános szerződéses feltételekbe (ÁSZF) sem rejthetjük bele sokadik pontként azt, hogy az ÁSZF elfogadása egyben hozzájárulás ahhoz, hogy marketing üzeneteket küldhessünk ki a szolgáltatásunkat igénybe vevőnek.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Az érintett hozzájárulása tehát akkor érvényes és az akkor lehet megfelelő jogalap, ha az önkéntes, tehát ha – az ehhez fűződő bármely hátrány vagy kár nélkül – dönthet úgy a diák vagy a tanár, hogy nem kíván szerepelni a képfelvételen. Az érvényesség további feltétele, hogy a konkrét és megfelelő tájékoztatáson alapuljon, amely feltétel akkor érvényesül, ha az érintett tisztában van legalább az adatkezelő kilétével és az adatkezelés céljával,[223] *mely konkrét esetben azt jelenti, hogy akkor, ha az iskola tájékoztatja az érintetteket a képfelvétel sorsáról, így arról, hogy azok szerepelni fognak az iskolai évkönyvben, adott esetben a nyomtatott sajtóban.*

Lényeges követelmény továbbá, hogy az érintettnek lehetősége legyen az egyes adatkezelési műveletekhez (a felvétel elkészítése, a felvétel iskolai évkönyvben történő közzététele, a felvétel nyilvános sajtófelületen történő közzététele) külön-külön hozzájárulni, így például a képfelvétel elkészítéséhez való hozzájárulás soha nem jelentheti egyben az annak további felhasználásához való hozzájárulást.
A hozzájárulás érvényességéhez továbbá kiskorú személyek esetén a Polgári Törvénykönyvről szóló 2013. évi V. törvény (Ptk.) a cselekvőképességre[224] *és szülői felügyeletre*[225] *vagy gyámságra vonatkozó szabályainak betartása szükséges.*

Ha az adatkezelés hozzájáruláson alapul, az adatkezelőnek (az iskolának) képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult. Megfelelő gyakorlat lehet, ha az iskola az év első napján tájékoztatja a diákokat (vagy szüleiket) és tanárokat, hogy a tanév során a különböző rendezvényeken képfelvételek készülnek, a tanév folyamán továbbá évkönyv is

[222] NAIH/2020/1866/5
[223] GDPR (42) preambulumbekezdés
[224] Ptk. 2:11.-2:14. §
[225] Ptk. 4:161. §

készül, és ehhez kéri az érintettek hozzájáruló nyilatkozatát (aláírását) írásos formában.

A kérdéses adatkezelésre alkalmazni kell a Ptk. képmáshoz való jogra vonatkozó rendelkezéseit is, miszerint egy képmás elkészítéséhez és felhasználásához az érintett személy hozzájárulása szükséges, kivéve tömegfelvétel és nyilvános közéleti szereplésről készült felvétel esetén.[226] *"*[227]

A „szabad akaratból" tett hozzájárulás csak akkor érvényes, ha a hozzájárulás megadása során valódi választási lehetősége volt az érintettnek és nem állt fenn a megtévesztés, megfélemlítés, kényszerítés vagy jelentős negatív következmények kockázata abban az esetben, ha megtagadja ezt a hozzájárulást.

Példa

- ✓ *amikor egyetlen hozzájárulásban több adatkezelési célt is megnevezünk az nem felel meg az önkéntesség követelményének, hiszen előfordulhat, hogy az érintett három, számára fontos cél miatt megadja a negyedik, neki egyébként nagyon nem tetsző adatkezeléshez is a hozzájárulását.*
- ✓ *Ha egy hivatalban többféle módon lehet ügyet intézni, például személyesen sorban állva, online időpontot foglalva, személyesen vagy email útján az ügyfélszolgálattól időpontot kérve, ebben az esetben az online foglalás esetén az ügyfél e-mail címét a hivatal kezelheti az érintett hozzájárulására hivatkozva, hiszen más lehetőséget is biztosít foglalásra, az ügyfél pedig szabadon dönt melyik út a neki legkényelmesebb. Azonban, ha a hivatal csak internetes felületen, bejelentkezés után fogad bárkit is, ez esetben nem hivatkozhat az érintett hozzájárulására ezen adatkezelés keretében, mert az ügyfélnek nincs más lehetősége, ha ügyet akar intézni.*

A hozzájárulás megadása semmiképpen sem tekinthető önkéntesnek, ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel és nem áll módjában a hozzájárulás anélküli megtagadása vagy visszavonása, hogy ez a kárára válna. Adatkezelőként nem gyakorolhatunk közvetlen vagy közvetett indokolatlan befolyásolást vagy nyomást (amely lehet gazdasági vagy más jellegű) annak érdekében, hogy megszerezzük a hozzájárulást és a hozzájárulás nem minősülhet szabad akaratból adottnak akkor sem, ha az érintettnek nincs valódi választása vagy nem tudja a hozzájárulását jogsérelem nélkül megtagadni vagy visszavonni.

A finn adatvédelmi hatóság (Tietosuojavaltuutetun toimisto) gyakorlatából

A finn adatvédelmi hatósághoz 11 panasz érkezett az Independent Consulting Oy közvetlen marketingkommunikációs gyakorlatával kapcsolatban. A cég közvetlen marketing célú SMS-eket küldött ki az érintetteknek. Az SMS tartalmazott ugyan utasításokat arra vonatkozóan, hogyan lehet lemondani a közvetlen marketing kommunikációról, azonban ez a funkció nem működött és az érintettek továbbra is

[226] Ptk. 2:48. § (1) – (2) bek.
[227] NAIH/2019/2528, https://www.naih.hu/adatvedelmi-allasfoglalasok?download=57:osztalykep-rendezvenyfoto-iskolai-evkonyvben-torteno-kozzetetele, utolsó letöltés: 2022. 08. 22.

kaptak marketing üzeneteket. A Consulting Oy azt állította, hogy a közvetlen marketingközlemények vállalatoknak szóltak, ezért nincs szükség előzetes hozzájárulásra.

Az adatvédelmi hatóság megállapította, hogy az üzenetek küldésére használt telefonszámok a munkavállalókra és nem a vállalatra vonatkoztak, valamint a marketing üzenetek nem kapcsolódtak az érintettek munkatevékenységéhez. A hatóság 7 ezer eurós bírságot szabott ki a társaságra előzetes hozzájárulás nélküli közvetlen marketingközlemények küldése és az érintettek jogainak figyelmen kívül hagyása miatt.[228]

A szabad akarat hiánya az alárendelt helyzetekben erősen kétséges lehet, például amikor nincs gazdasági egyensúly az adatkezelő és a hozzájárulást megadó érintett között. A munkáltató és a munkavállaló közötti függőségi viszonyból eredően szinte soha nincs a munkavállaló abban a helyzetben, hogy a hozzájárulását szabadon adja meg, tagadja meg vagy vonja vissza. Munkavállalóként az erőviszonyok egyenlőtlensége miatt csak kivételes esetekben értelmezhető az adatkezeléshez hozzájárulás önkéntesnek – általában akkor, amikor az ajánlat elfogadásához vagy elutasításához semmilyen következmény sem kapcsolódik.

Példa a munkavállaló hozzájárulására

- ✓ *a munkavállaló a gépjárművével be akar állni a cég parkolójába és ehhez meg kell adnia a rendszámának kezeléséhez a hozzájárulását. Ha akar, akkor hozzájárulhat az adatkezeléshez, azaz a későbbiekben használhatja a parkolót, ha nem akar hozzájárulni az adatkezeléshez, akkor parkol, ahol akar, maximum két háztömböt gyalogol vagy tömegközlekedik. Az adatkezelést ebben az esetben a munkavállaló következmények nélkül elkerülheti, mivel a munkáltató számára teljesen érdektelen, hogy a céges parkolót akarja-e használni vagy sem, és ha nem, annak mi az oka (nincs autója, nem akarja a rendszámát leadni, nem akarja, hogy a munkatársai megtudják, hogy milyen szakadt/ultra elegáns autóval jár dolgozni stb.)*

A szlovén adatvédelmi hatóság (IP) gyakorlatából

Egy társaság igazgatója úgy döntött, hogy videós üdvözlőlapot készít és küld el e-mailben az ügyfeleinek. A videót a munkavállalóknak otthon kellett felvenniük kötelező részvétel mellett. A szlovén hatóságnak abban kellett véleményt nyilvánítania, hogy kezelheti-e a munkáltató a munkavállalók személyes adatait hozzájárulásra hivatkozva?

A hatóság álláspontja szerint

[228] Tietosuojavaltuutetun toimisto – 3425/157/2019, 3578/157/2019, 3846/157/2019, 3871/157/2019, 3891/152/2019, 3918/157/2019, 4338/157/2019, 4666/154/2019, 5973/157/2019, 6773/157/2019 ja 7022/157/2019, https://finlex.fi/fi/viranomaiset/tsv/2020/20200632, utolsó letöltés 2022. 07. 17.

- ✓ *munkaviszonyban fennálló hatalmi egyenlőtlenségek miatt és a munkavállaló védelme érdekében az adatkezelés csak kivételes esetekben lehetséges, és feltéve, hogy az egyén megtagadhatja a hozzájárulást.*
- ✓ *az üdvözlő videón való részvétel csak önkéntes hozzájárulás esetén lehetséges, ami azt jelenti, hogy csak akkor, ha a munkavállaló negatív következmények nélkül megtagadhatja azt.*[229]

Az elszámoltathatóság elvének megfelelés érdekében a hozzájárulásokat nyilván kell tartanunk, különben nem tudunk azokra érvényesen hivatkozni, illetve értelemszerűen a hozzájárulás visszavonását sem tudjuk kezelni.

A görög adatvédelmi hatóság (HDPA) gyakorlatából

A görög adatvédelmi hatóság 20 ezer eurós bírságot szabott ki egy telefonokat értékesítő társaságra, mert ügyfelei személyes adatait azok előzetes hozzájárulása nélkül kezelte más termékek és szolgáltatások népszerűsítése céljából, valamint nem tartotta tiszteletben az „opt-out" (lemondás) kérésüket.

Három ügyfél panaszt nyújtott be a HDPA-hoz, mert a társaság a személyes adataikat más célból kezelte, mint amiért azokat eredetileg gyűjtötte. Az érintettek azt állították, hogy a személyes adataikat eredetileg áruvásárlás során gyűjtötte a társaság, a későbbiekben azonban a társaság más termékek és szolgáltatások népszerűsítése céljából vette fel velük a kapcsolatot anélkül, hogy tiszteletben tartotta volna az opt-out kérésüket. A Társaság ezzel szemben azt állította, hogy az érintettekkel egy ügyfél-elégedettségi felmérés céljából vette fel a kapcsolatot, miután megkapta a hozzájárulásukat.

A HDPA megállapította, hogy

- ✓ *a vevők adatainak kezelése más szolgáltatások és áruk népszerűsítése céljából a személyes adatok eredeti gyűjtési céltól eltérő célú felhasználásának minősül, és bár a társaság azzal érvelt, hogy az áruk értékesítése során megszerezte az ügyfelek szóbeli hozzájárulását az ilyen jellegű adatkezeléshez, ezt nem tudta bizonyítani.*
- ✓ *a vevőket az adatgyűjtési szakaszban nem tájékoztatták megfelelően az adatkezelő személyéről, valamint arról, hogy személyes adataikat további célra is felhasználhatják.*
- ✓ *a társaság – az opt-out kérelmek eseténben – nem tartotta tiszteletben az érintettek tiltakozását személyes adataik marketing célú további kezelése ellen, illetve a társaság nem tudott bemutatni megfelelő dokumentumokat vagy belső szabályzatokat annak igazolására, hogy az ilyen kérelmeket érdemben megválaszolják.*

Az eset érdekessége, hogy az adatkezelő azt állította, hogy a személyes adatokat marketing célokra (termékek promóciójára) kezelte az érintettek szóbeli hozzájárulása alapján, amelyet a termékvásárlás során szerzett be. Az adatvédelmi hatóság azonban nem talált bizonyítékot arra, hogy ez a hozzájárulás ténylegesen

[229] IP – 07121-1 / 2020/2260, https://www.ip-rs.si/mnenja-gdpr/6048a64137abb, utolsó letöltés 2022. 07. 17.

megtörtént, ezért nem fogadta el, hogy a hozzájárulás az adatkezelés jogalapja. A HDPA álláspontja szerint a jogos érdekre hivatkozás elfogadható lett volna, tekintettel az „opt-in" kivételre (a tiltakozás lehetőségére). Azonban arra, hogy az adatkezelésre más célból került sor, mint amiért a személyes adatokat eredetileg gyűjtötték, legalább megfelelő tájékoztatást kellett volna nyújtani az érintetteknek az adatgyűjtés szakaszában, hogy az érintettek tudjanak arról, hogy személyes adataikat további célra fogják felhasználni, és ugyanakkor lehetőséget kellett volna biztosítani számukra, hogy élhessenek a tiltakozási jogukkal.[230]

Amennyiben olyan internetes szolgáltatásaink vannak, amelyeket közvetlenül a gyermekeknek kínáljuk, a GDPR 8. cikke alapján bizonyos többletkötelezettségekkel kell számolnunk, így például

- hozzájárulásra hivatkozott adatkezelésünk akkor lesz jogszerű, ha a gyermek elmúlt 16 éves (a tagállamok ennél alacsonyabb, de a 13. életévnél nem alacsonyabb életkort is megállapíthatnak)
- 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte. Ilyen esetben – figyelembe véve az elérhető technológiát – észszerű erőfeszítéseket kell tennünk annak érdekében, hogy ellenőrizzük, hogy a hozzájárulást a gyermek feletti szülői felügyeleti jog gyakorlója adta meg, illetve engedélyezte).

A GDPR ezen rendelkezése nem érinti a tagállamok (így hazánk) általános szerződési jogát, például a gyermek által kötött szerződések érvényességére, formájára vagy hatályára vonatkozó szabályokat.

A holland bírósági gyakorlatból

Az Overijsseli Elsőfokú Bíróság kimondta, hogy a tizenhat év alatti kiskorú törvényes gyámjának beleegyezését kell adnia ahhoz, hogy egy harmadik fél fényképeket vagy videókat tegyen közzé a kiskorúról. A bíróság megjegyezte, hogy lényegtelen az a tény, hogy az alperes és a kiskorú között közös kötelék áll fenn, és hogy az alperes gyermeke a kiskorú féltestvére.[231]

A sütik és a hozzájárulás

A süti a napjainkban használt eszközalapú nyomkövető technológia egyike, hasonló célt szolgálnak például a helyi tárolási objektumok (LSO), a szoftverfejlesztő készletek (SDK), a pixel trackerek vagy pixel gif-ek, a „like" és a közösségi megosztás gombok, valamint az eszköz-ujjlenyomat technológiák is.

A sütik a felhasználó (érintett) eszközén tárolt kis adatfájlok, amelyek a felhasználókat azonosítani tudják és képesek nyomon követni az internetes böngészés során. Ezeket

[230] HDPA (Greece) – 48/2021, https://www.dpa.gr/sites/default/files/2021-11/48_2021anonym.pdf, utolsó letöltés: 2022. 07. 24.
[231] ECLI:NL:RBOVE:2021:1506, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBOVE:2021:1506, utolsó letöltés: 2022. 08. 22.

a sütiket csoportosíthatjuk céljuk (funkció, teljesítmény, analitika, közösségi média stb.), időtartamuk (lejárat a böngészési munkamenet végén, lejárat három hónap múlva stb.) és eredetük (azaz első fél vagy harmadik fél) szerint.

A sütik rendeltetése lehet az adott eszköz rövid távú „memóriasegédje" az oldalak vagy a látogatások között (pl. használt nyelv megjegyzése), de akár viselkedési profilt is készíthetnek a felhasználóról.

Alapvetően két jogszabály vonatkozik a sütikre, az egyik az ePrivacy irányelv (és ez alapján hazánkban az Eht.), a másik pedig a GDPR.

Az ePrivacy irányelv alapján[232] a tagállamok gondoskodnak arról, hogy egy előfizető vagy felhasználó végberendezésében történő adattárolás, illetve az ott tárolt adatokhoz való hozzáférés csak azzal a feltétellel legyen megengedett, ha az érintett előfizető vagy felhasználó – többek között az adatkezelés céljairól szóló – egyértelmű és teljes körű tájékoztatás alapján ehhez előzetes hozzájárulását adta. Ez a rendelkezés nem akadályozza az olyan műszaki tárolást, illetve műszaki hozzáférést,

- ✓ amelynek kizárólagos célja az elektronikus hírközlő hálózaton keresztül történő közléstovábbítás, vagy
- ✓ amelyre az előfizető vagy felhasználó által kifejezetten kért, az információs társadalommal összefüggő szolgáltatás nyújtásához a szolgáltatónak feltétlenül szüksége van.

Ezen kivételes esetekben nincs szükség hozzájárulásra.

A GDPR szabályai irányadók abban az esetben, amennyiben a természetes személyek összefüggésbe hozhatók az általuk használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítókkal, például IP-címekkel és cookie-azonosítókkal, valamint egyéb azonosítókkal, például rádiófrekvenciás azonosító címkékkel. Ezekben az esetekben olyan nyomok keletkezhetnek, amelyek egyedi azonosítókkal és a szerverek által fogadott egyéb információkkal összekapcsolva felhasználhatók a természetes személyes profiljának létrehozására és az adott személy azonosítására.[233]

A magyar szabályozás alapján[234] *a szolgáltató – szükség szerint más szolgáltatókkal közösen –*

- ✓ *megfelelő műszaki és szervezési intézkedésekkel gondoskodni köteles a továbbított közlés és a közléshez kapcsolódó forgalmi adatok jogosulatlan lehallgatásának, tárolásának vagy megfigyelésének, valamint a közléshez és a közléshez kapcsolódó forgalmi adatokhoz történő jogosulatlan vagy véletlen hozzáférésnek a megakadályozásáról („közlés bizalmassága")*
- ✓ *csak úgy választhatja meg, és minden esetben úgy üzemeltetheti a szolgáltatás nyújtása során alkalmazott elektronikus hírközlő eszközöket, hogy biztosítani tudja a közlés bizalmasságát.*

[232] GDPR 5. cikk (3) bekezdés
[233] GDPR (30) preambulumbekezdés
[234] Az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.) 155.§

- ✓ *a továbbított közlések tartalmát csak olyan mértékben ismerheti meg és tárolhatja, amely a szolgáltatás nyújtásához műszakilag elengedhetetlenül szükséges.*
- ✓ *köteles tájékoztatni az érintett nemzetbiztonsági szolgálatot a szolgálat minősített adatot képező, védett telefonszámait érintő adatszolgáltatási megkeresésekről vagy adatkérésről (kivéve: a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 42. §-ában meghatározott adatszolgáltatás és adatbetekintés)*

Egy előfizetőnek vagy felhasználónak elektronikus hírközlő végberendezésén csak az érintett felhasználó vagy előfizető világos és teljes körű – az adatkezelés céljára is kiterjedő – tájékoztatását követő hozzájárulása alapján lehet adatot tárolni, vagy az ott tárolt adathoz hozzáférni.

A nyomozó hatóságok és a rendőrségről szóló törvényben meghatározott belső bűnmegelőzési és bűnfelderítési feladatokat ellátó, valamint terrorizmust elhárító szerv (nyomozó hatóságok), valamint a nemzetbiztonsági szolgálatok az Eht-ben foglaltak szerint, továbbá a Hivatal[235] *– az Eht. 11. § (3) bekezdésében előírt jogkör gyakorlása során – a közléseket megfigyelhetik, lehallgathatják, tárolhatják vagy a küldeménybe, közlésbe azok megfigyelése érdekében más módokon beavatkozhatnak.*

A sütik kérdése ma az egyik „legforróbb" téma az adatvédelem területén.

A 29-es számú adatvédelmi munkacsoport véleménye szerint[236] *– bizonyos feltételek mellett – az alábbi sütik mentesülhetnek a hozzájárulás alól (amennyiben nem használják fel azokat további célokra):*
„1) Felhasználói beviteli sütik (munkamenet-azonosító) a munkamenet időtartamára, vagy némely esetben, néhány órára korlátozott tartós sütik.
2) Hitelesítési sütik, amelyeket hitelesített szolgáltatások használnak, a munkamenet időtartamára.
3) Felhasználóközpontú biztonsági sütik, amelyeket a hitelesítési visszaélések felderítésére használnak, korlátozott fennmaradási időtartamra.
4) Multimédiatartalom-lejátszó munkamenet-sütik, így például flash-lejátszó sütik, a munkamenet időtartamára.
5) Terheléskiegyenlítő munkamenet-sütik, a munkamenet időtartamára
6) A felhasználói felület testreszabását segítő sütik a munkamenet időtartamára (vagy kissé hosszabb időre).
7) Külső közösségi tartalommegosztó sütik, a közösségi hálózatok bejelentkezett tagjai számára."[237]

[235] Nemzeti Média- és Hírközlési Hatóság Hivatala
[236] A 29. cikk szerinti adatvédelmi munkacsoport 2012/4. számú véleménye a sütikhez való hozzájárulás alóli mentességről, WP194, Elfogadás időpontja: 2012. június 7.
[237] A 29. cikk szerinti adatvédelmi munkacsoport 2012/4. számú véleménye a sütikhez való hozzájárulás alóli mentességről, WP194, Elfogadás időpontja: 2012. június 7.

Az EDPB gyakorlata

Példa: „A weboldal szolgáltatója olyan szkriptet alkalmaz, amely letiltja a tartalom láthatóvá válását, kivéve a sütik elfogadására irányuló kérést, valamint az arra vonatkozó információkat, hogy mely sütiket állítják be, és milyen célból dolgozzák fel az adatokat. A tartalomhoz csak a „Sütik elfogadása" gombra kattintva lehet hozzáférni. Mivel az érintettnek nincs valódi választási lehetősége, hozzájárulása nem minősül önkéntesnek.[238]

A sütifalak[239] szabályozása volt az egyik legvitásabb pont annak az elektronikus hírközlési adatvédelmi rendelettervezetnek az ötéves tárgyalása során, amelynek egyik legfontosabb célja a multinacionális vállalatok által már jól ismert, a sütikre vonatkozó széttagolt tagállami szabályozási megközelítéseket egységes uniós szintű álláspontba foglalása. A javaslat szerint a sütifalak megengedettek lennének, feltéve, hogy a felhasználóknak választási lehetősége lenne a következők közül:

- a sütik bizonyos célokra történő használatához való hozzájárulás
- ugyanannak a szolgáltatónak az „egyenértékű ajánlata", amely nem jár sütik használatával.

A sütik körüli bizonytalanságot csökkenteni kívánva a francia adatvédelmi hatóság (CNIL) 2022 májusában kiadott egy iránymutatást,[240] amely szerint a GDPR „szabad" hozzájárulás követelménye nem vezet a sütifalak gyakorlatának általános tilalmához, azok jogszerűségét arra tekintettel kell értékelni, hogy a felhasználóknak valós és kielégítő alternatívákat kínál-e arra az esetre, ha elutasítják a sütik elhelyezését a végberendezésükön.

A francia adatvédelmi hatóság (CNIL) sütifalra vonatkozó kritériumrendszere

1. kritérium: a szolgáltatónak (a webhely üzemeltetőjének) vagy harmadik félnek „valós és tisztességes alternatívát" kell nyújtania a „sütifalazott" tartalom vagy szolgáltatás helyett, azaz

- a szolgáltatónak valódi és tisztességes alternatívát kell kínálnia, amely lehetővé teszi a webhelyhez való hozzáférést, és amely nem jelenti azt, hogy az érintettnek mindenképpen bele kell egyeznie az adatai felhasználásához vagy

[238] EDPB 5/2020 Iránymutatás az (EU) 2016/679 rendelet szerinti hozzájárulásról, 1.1 verzió, Elfogadás időpontja: 2020. május 4. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_hu.pdf, utolsó letöltés 2022. 08. 22.

[239] A sütifal („cookie wall"), más néven nyomkövető fal („tracking wall") megköveteli a felhasználóktól, hogy egy adott weboldal használatához "elfogadják" az összes sütit és nyomkövetőt, azaz „hozzájáruljanak" a személyes adataik kezeléséhez. A sütifal nem ad lehetőséget a felhasználónak arra, hogy úgy használják a weboldalt, hogy a sütik egy részét vagy egészét elutasítsák ("fogadd el vagy hagyd el" / „"take it or leave it")

[240] Cookie walls : la CNIL publie des premiers critères d'évaluation, 16 mai 2022, https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookie-walls/la-cnil-publie-des-premiers-criteres-devaluation, utolsó letöltés: 2022. 08. 22.

- a szolgáltatónak képesnek kell lennie bizonyítani, különösen a felügyeleti hatóság felé, hogy egy másik szolgáltató ugyanilyen alternatívát kínál anélkül, hogy sütifalat állítana fel.

A sütifalat bevezető weboldal kiadójának óvakodnia kell attól, hogy az internetfelhasználó tekintetében olyan hatalmi egyensúlyhiány alakuljon ki, amely aláásná a választás szabadságát, ezért a szolgáltatónak biztosítania kell, hogy a felhasználó könnyen hozzáférjen a szolgáltatásokhoz vagy tartalmakhoz való hozzáférés alternatív módjához. Ilyen egyensúlyhiány például abban az esetben alakulhat ki, ha a szolgáltató kizárólagosságot élvez a kínált tartalom vagy szolgáltatás tekintetében, vagy ha a felhasználónak kevés vagy semmilyen alternatívája nincs a szolgáltatással kapcsolatban, és ezért nincs valódi választási lehetősége a sütik használata tekintetében sem (például domináns vagy alapvető fontosságú szolgáltatók).

2. kritérium: A „fizetőfal" árának észszerűnek kell lennie
A CNIL álláspontja szerint a szolgáltató kérheti vagy a sütik elfogadását vagy díjazást kérhet a nyújtott szolgáltatásokért, azaz nem tilos fizetős alternatívát kínálnia. Ennek az árnak azonban észszerűnek kell lennie, azaz nem lehet olyan magas, hogy megfossza a felhasználókat a valódi választási lehetőségtől, illetve a fizetőfalat bevezetni kívánóknak képesnek kell lenniük arra, hogy igazolják a felajánlott pénzbeli ellenszolgáltatás észszerűségét. A CNIL azt is ajánlja, hogy a szolgáltatók – az átláthatóság érdekében – az ilyen elemzést tegyék közzé.

3. kritérium: felhasználói fiók létrehozásának meghatározott céloknak kell megfelelnie.
Amennyiben egy weboldal vagy alkalmazás üzemeltetői, felhasználói fiók létrehozását írják elő a felhasználók számára, abban az esetben biztosítaniuk kell, hogy ez a kötelezettség indokolt legyen a kitűzött céllal kapcsolatban. A szolgáltatóknak a felhasználói fiók létrehozásával kapcsolatban:

- *tájékoztatniuk kell az adataik kezeléséről*
- *az adatgyűjtést csak a kitűzött célok eléréséhez szükséges adatokra kell korlátozniuk, valamint*
- *ha a szolgáltató a fiók létrehozása során gyűjtött adatokat más célokra kívánja újra felhasználni, erről előzetesen és egyértelműen tájékoztatnia kell a felhasználót, és szükség esetén be kell szereznie ezen új célokhoz a felhasználók hozzájárulását.*

4. kritérium: A fizető-, illetve a sütifalaknak meg kell felelniük a sütik meghatározott céljainak.
Amennyiben egy szolgáltató sütifalat alkalmaz, bizonyítania kell, hogy az olyan célokra korlátozódik, amelyek lehetővé teszik a kínált szolgáltatásért járó tisztességes díjazást. Tehát ha egy szolgáltató úgy véli, hogy a szolgáltatásának díjazása a célzott reklámokból származó bevételektől függ, akkor a szolgáltatáshoz való hozzáféréshez csak e célhoz szükséges hozzájárulás lehet, a más célokhoz való hozzájárulás megtagadása nem akadályozhatja a webhely tartalmához való hozzáférést.

5. kritérium: amennyiben a felhasználó a sütifal alternatíváját választja, akkor a szolgáltató csak korlátozott körülmények között helyezhet el sütiket a felhasználó végberendezésén.
Ebben az esetben a szolgáltató csak olyan sütiket / nyomkövetőket használhat, amelyek a kért szolgáltatás nyújtásához feltétlenül szükségesek. Emellett a szolgáltatók eseti alapon kérhetik a felhasználó hozzájárulását sütik vagy hasonló nyomkövetők használatához, ha ez utóbbiakra harmadik fél webhelyén elhelyezett tartalomhoz való hozzáférés érdekében van szükség (pl. egy harmadik fél webhelyén elhelyezett videó megtekintéséhez), feltéve, hogy a szükséges információkat a felhasználók rendelkezésére bocsátja, így többek között:

- *azt a tény, hogy a külső tartalom aktiválása célhoz kötött hozzájárulást igényel*
- *a külső tartalomszolgáltató adatvédelmi tájékoztatójának linkjét*
- *a hozzájárulás bármikor történő egyszerű visszavonásának lehetőségét és*
- *a hozzájárulás meg nem adásának következményét, azaz a szolgáltatáshoz való hozzáférés megtagadását.*

A CNIL kritériumrendszerét természetesen nem kötelező hazánkban figyelembe venni, ám mindenképpen segítségül hívhatjuk abban az esetben, ha olyan honlapot üzemeltetünk, amely sütiket alkalmaz. Fel kell azonban készülnünk arra, hogy nincs olyan „egyengyakorlat", amely minden honlap és alkalmazás esetében használható lenne, az értékelést eseti alapon kell elvégeznünk, például a „valós és méltányos alternatíva" (1. kritérium) bizonyításához össze kell hasonlítanunk a sütifalakat bevezető weboldalak (alkalmazások) versengő ajánlatait, illetve ezt az értékelést időről időre – a piac változásait követve – frissítenünk kell.

Az Európai Unió Bíróságának (EUB) gyakorlatából

Az információk valamely internetes oldal felhasználója végberendezésében telepített cookie-k segítségével történő tárolásához vagy az információkhoz cookie-k segítségével történő hozzáféréshez való hozzájárulás megadása nem tekinthető érvényesnek abban az esetben, ha az engedélyezés előre bejelölt négyzettel történik, függetlenül attól, hogy a szóban forgó információk személyes adatoknak minősülnek-e vagy sem.

Ezenkívül a szolgáltatónak tájékoztatnia kell a valamely internetes oldal felhasználóját a cookie-k működésének időtartamáról, valamint arról, hogy harmadik személyeknek lehetőségük van-e ezen cookie-khoz hozzáférni.

A Bíróság így kimondta, hogy

- ✓ *a hozzájárulás nem tekinthető érvényesnek abban az esetben, ha valamely internetes oldal felhasználója a végberendezésében mentett információk tárolását vagy az ott már tárolt információkhoz történő hozzáférést előre bejelölt négyzettel engedélyezi, és e bejelölést e felhasználónak a hozzájárulása megtagadásához törölnie kell.*
- ✓ *az, hogy egy felhasználó rákattint a szóban forgó nyereményjátékban való részvétel gombra, nem lehet elegendő ahhoz, hogy úgy lehessen tekinteni, hogy a felhasználó érvényesen hozzájárult a cookie-k telepítéséhez*

[A 2019. október 1-jei Planet49 ítélet (nagytanács) (C-673/17, EU:C:2019:801)][241]

Adatkezelés szerződés teljesítéséhez/előkészítéséhez szükséges [GDPR 6. cikk (1) bekezdés b) pont]

Ezt a jogalapot akkor használhatjuk, ha a következő két feltétel valamelyike teljesül:

- ✓ az adott adatkezelésünknek objektíve szükségesnek kell lennie az érintettel kötött szerződésünk teljesítéséhez, vagy
- ✓ az adatkezelésünknek objektíve szükségesnek kell lennie ahhoz, hogy az érintett kérésére a szerződéskötést megelőző lépéseket megtegyük.

Példa a „szerződésre", illetve „szerződés előkészítése" hivatkozásra

- ✓ *megadjuk a postai irányítószámunkat annak érdekében, hogy meggyőződjünk arról, hogy egy adott étterem-hálózat a környékünkön nyújt-e szolgáltatást*
- ✓ *árajánlatot kérünk a biztosítótól gépjármű felelősségbiztosítása tárgyában*
- ✓ *a munkavállalóval munkaszerződést kötünk és az abban foglaltak alapján számoljuk el a teljesítményét*
- ✓ *megadjuk a címet, hova kérjük az általunk megvásárolt termék kiszállítását*

Nem hivatkozhatunk erre a jogalapra például akkor, ha

- ✓ adatkezelőként a velünk szerződő partner nem természetes személy,
- ✓ az érintett a szerződő partnerünk képviselője,
- ✓ a nemteljesítés által előidézett további lépések esetén,
- ✓ a szerződés végrehajtásakor felmerülő egyéb események esetén, illetve akkor ha
- ✓ az adatkezelés valójában nem szerződés teljesítéséhez szükséges, hanem azt egyoldalúan az érintettre erőltetjük.

Amennyiben a szerződésben, illetve a szerződést előkészítő dokumentációban az adatok különleges kategóriájába tartozó adat is van, ebben az esetben a különleges adatok tekintetében nem hivatkozhatunk a szerződés előkészítése/teljesítése jogalapra.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A szerződéses jogalap nem vonatkozik olyan helyzetekre, ahol az adatkezelés valójában nem a szerződés teljesítéséhez szükséges, hanem azt az adatkezelő egyoldalúan az érintettre erőlteti."[242]

„A Hatóság megállapítása szerint a GDPR 6. cikk (1) bekezdés b) pontja szerinti jogalap – a szerződéskötést megelőző egyes lépések kivételével – csak akkor alkalmazható, ha az a szerződés teljesítéséhez szükséges, tehát nem lehet kiterjeszteni ezt a jogalapot olyan adatkezelésekre, amelyekre a szerződés érintett

[241] Az Európai Unió Bírósága Kutatási és Dokumentációs Igazgatóság: A személyes adatok védelme, Tematikus tájékoztató, 2020. július (42-43.o.)
[242] NAIH/2020/643/6. (NAIH/2019/5963.)

általi nemteljesítése miatt előidézett helyzet orvoslása érdekében a szerződő felek rendes együttműködési kötelezettségből fakadó lépéseken túlmutató cselekmények megtételéhez van szükség. A szerződés teljesítése körébe eshetnek még azok a lépések, amikor az adatkezelő, aki a szerződést megkötötte az érintettel – tehát aki a szerződésben a másik fél – teljesítési késedelem esetén felszólítja az érintettet a teljesítésre. Azonban a GDPR 6. cikk (1) bekezdés b) pontja szerinti szerződéses jogalap már nem vonatkoztatható arra az esetre, ha az adatkezelő az elmaradt teljesítés miatt az érintettel szembeni követelését követelésbehajtással foglalkozó vállalkozásra engedményezi (azaz a problémát már a szerződésen kívül kívánja megoldani). Ilyenformán a Kérelmezett és a Kérelmező között szerződéses jogviszony nem áll fenn."[243]

A holland bírósági gyakorlatból

A bíróság megállapította, hogy az az intézkedés, amely szerint az utasok csak hitelkártyával/betéti kártyával vásárolhatnak jegyet a buszokon, összeegyeztethető a szükségesség és az arányosság elvével, valamint a személyes adatok további kezelése szükséges a szerződés teljesítéséhez a [GDPR 6. cikke (1) bekezdésének b) pontja]. Ezért az adatkezelés összeegyeztethető a GDPR-ral.[244]

Amennyiben adatkezelésünk során szerződéses jogalapra hivatkozunk, az érintettet tájékoztatnunk kell arról, hogy

- a személyes adat szolgáltatása szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e,
- köteles-e a személyes adatokat megadni,
- milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása (például név megadása nélkül nem tudunk vele szerződést kötni), valamint
- élhet-e az adathordozhatósághoz való jogával.

Az adatkezelőre vonatkozó jogi kötelezettség teljesítése [GDPR 6. cikk (1) bekezdés c) pont]

Jogi kötelezettség esetében az adatkezelés az adatkezelőre, azaz ránk vonatkozó (saját tagállamunk által meghatározott vagy uniós) jogi kötelezettség teljesítéséhez szükséges.

A GDPR alapján a jogi kötelezettség teljesítése [GDPR 6. cikk (1) bekezdés c) pont], illetve, ha az adatkezelés közérdekű vagy adatkezelőre ruházott közhatalmi jogosítvány gyakorlása érdekében szükséges [GDPR 6. cikk (1) bekezdés e) pont], az adatkezelés jogalapját uniós jognak vagy azon tagállami jognak kell meghatároznia, amely hatálya alá adatkezelőként tartozunk.

[243] NAIH/2019/2566/8. https://www.naih.hu/files/NAIH-2019-2566-8-hatarozat.pdf, utolsó letöltés: 2022. 08. 22.
[244] Rb. Gelderland – AWB 19/2901, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBGEL:2020:619&showbutton=true&keyword=AVG, utolsó letöltés 2022. 07. 17.

Az adatkezelésünk célját e jogalapra hivatkozással kell meghatároznunk, illetve, ha adatkezelésünk során a GDPR 6. cikk (1) bekezdés e) pontjában említett jogalapra hivatkozunk, az adatkezelésünknek szükségesnek kell lennie valamely közérdekű vagy adatkezelőként ránk ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához. Ez a jogalap tartalmazhat a GDPR-ban foglalt szabályok alkalmazását kiigazító rendelkezéseket, ideértve

- az adatkezelő általi adatkezelés jogszerűségére irányadó általános feltételeket,
- az adatkezelés tárgyát képező adatok típusát,
- az érintetteket,
- azokat a jogalanyokat, amelyekkel a személyes adatok közölhetők, illetve
- az ilyen adatközlés céljait,
- az adatkezelés céljára vonatkozó korlátozásokat,
- az adattárolás időtartamát és
- az adatkezelési műveleteket, valamint
- egyéb adatkezelési eljárásokat, így a törvényes és tisztességes adatkezelés biztosításához szükséges intézkedéseket is, ideértve a GDPR IX. fejezetében meghatározott egyéb konkrét adatkezelési helyzetekre vonatkozóan.

Az uniós vagy tagállami jognak közérdekű célt kell szolgálnia, és arányosnak kell lennie az elérni kívánt jogszerű céllal.[245]

Az Infotv. alapján[246] az általános adatvédelmi rendelet 6. cikk (1) bekezdés c) és e) pontjában meghatározott adatkezelések („kötelező adatkezelések") esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.

Kizárólag állami vagy önkormányzati szerv kezelheti az állam bűncselekmények megelőzésére, felderítésére és üldözésére irányuló, valamint közigazgatási és igazságszolgáltatási feladatainak ellátása céljából kezelt bűnügyi személyes adatokat, valamint a szabálysértési, a polgári peres és nemperes ügyekre, valamint a közigazgatási peres és nemperes ügyekre vonatkozó adatokat tartalmazó nyilvántartásokat.

Amennyiben a kötelező adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény, helyi önkormányzat rendelete vagy az Európai Unió kötelező jogi aktusa nem határozza meg, az adatkezelés megkezdésétől legalább háromévente felül kell vizsgálnunk, hogy az általunk, illetve a megbízásunkból vagy rendelkezésünk alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e. Ezen felülvizsgálatunk körülményeit és eredményét dokumentálunk kell, és ezt a dokumentációt a felülvizsgálat elvégzését követő tíz évig meg kell őriznünk és azt a Nemzeti Adatvédelmi és Információszabadság Hatóság kérésére a Hatóság rendelkezésére kell tudnunk bocsátanunk.

[245] GDPR 6. cikk (3) bekezdés
[246] Infotv. 5.§ (3)-(5) bekezdés

Egy harmadik ország jogszabályában foglaltak végrehajtása során nem hivatkozhatunk a ránk vonatkozó jogi kötelezettségre, mint jogalapra (például az Amerikai Egyesült Államokban a 2002. évi Sarbanes–Oxley törvény szerinti belső visszaélésjelentési rendszerek létrehozására irányuló kötelezettségre) csak akkor, ha az adott jogszabályt az államunk elismerte és beépítette azt a jogrendszerünkbe például nemzetközi megállapodás formájában. Egyéb esetekben a jogos érdekre hivatkozhatunk az adatkezelésünk során, és érdekmérlegelési tesztünk egyik legfőbb adatkezelői érdeke ezen jogszabálynak való megfelelőségünk lesz.

Példa az adatkezelőre vonatkozó jogi kötelezettségre

- ✓ *ha egy állatorvos veszettség elleni oltást ad egy kutyának, akkor a kutyának és a gazdának az adatait is regisztrálnia kell az ebnyilvántartásban*
- ✓ *nem használhatjuk a jogi kötelezettség teljesítésére hivatkozó jogalapot amikor egy amerikai egyesült államokbeli multinacionális cég anyaországbeli kötelező erejű szabályai miatt az unió területén bejegyzett leányvállalatától is elvárt bizonyos pénzmosás elleni szabályoknak megfelelés. Ekkor a leányvállalat nem jogi kötelezettség, hanem az anyavállalat jogos érdeke alapján kezelheti az előírásoknak megfeleléshez szükséges adatkezelés során a személyes adatokat.*

Az, hogy ilyen esetekben hivatkozhatunk jogi kötelezettségre, nem mindig egyszerű eldöntenünk. Vannak olyan esetek, amikor a jogszabály felhatalmazást ad az adatkezelésre, de a részletekről nem rendelkezik, ilyen például a Munka törvénykönyvében a munkavállaló ellenőrzésének lehetősége. Ebben az esetben például a munkavállaló ellenőrzését (munkára képes állapot, munkaidő stb.) jogos érdekre hivatkozva végezhetjük el.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„(…) az ajánlások nem minősülnek jogszabálynak, azok jogi kötelezettséget nem keletkeztethetnek.”[247]

„A Hatóság álláspontja szerint az alábbi indokokra figyelemmel ezen jogalapok közül kizárólag az általános adatvédelmi rendelet 6. cikk (1) bekezdés c) pontja, illetve ehhez kapcsolódóan a Pmt.[248] *rendelkezései minősülnek adatkezelési, illetve –tárolási jogalapnak.*

A Kötelezett a Pmt. 56. § (1)-(2) bekezdésére tekintettel a kölcsönszerződési jogviszony megszűnésétől – 2018. december 19. napjától – számított nyolc évig köteles tárolni a Pmt. 7. § (1) bekezdése alapján a Kérelmező ügyfél-átvilágítási célból kezelt személyes adatait – illetve az azokat tartalmazó okiratokat – azaz: családi és utóneve, születési családi és utóneve, állampolgársága, születési helye, ideje, anyja születési neve, lakcíme, ennek hiányában tartózkodási helye, illetve

[247] NAIH/2019/3107/7. https://www.naih.hu/files/NAIH-2019-3107-hatarozat.pdf, utolsó letöltés: 2022. 08. 22.
[248] a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény (Pmt.)

azonosító okmányának típusa és száma személyes adatait. Tehát a Pmt. rendelkezései alapján a Kérelmező ezen személyes adatainak Kötelezett általi nyilvántartása adatvédelmi szempontból nem kifogásolható.

A Kérelmező jogi kötelezettség címén tárolt további személyes adatai, mint legmagasabb iskolai végzettsége, munkahelyének neve, címe, telefonos elérhetősége, beosztása, belépésének dátuma, havi nettó igazolt jövedelme, illetve jövedelmének típusa, gépjárművének rendszáma, alvázszáma, motorszáma, illetve törzskönyv száma személyes adatai kezelésére sem a Pmt., sem a további jogalapként hivatkozott jogszabályok, jogszabályi rendelkezések alapján nem jogosult a Kötelezett. (…)
Az általános adatvédelmi rendelet 21. cikk (1) bekezdése szintén nem minősül adatkezelési jogalapnak, mivel az az érintettet megillető tiltakozáshoz való jogról rendelkezik.

A Hpt.[249] hivatkozott rendelkezései sem minősülnek jogalapnak személyes adatok kezelésére, mivel azok a hitelintézetek eszköz minősítéséről, illetve a kockázatvállalás korlátozásáról és az ügyleti szabályokról rendelkeznek

A 2/2014. és a 6/2013. számú Polgári jogegységi határozat szintén nem biztosít jogalapot személyes adatok kezelésére. A jogegységi határozatok a jogalkalmazás egységes biztosításának eszközei, amelyek a bíróságokra nézve kötelezőek, de nem teremtenek jogi kötelezettséget személyes adatok kezelésére. Az az adatkezelés, amely az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges, a jogi kötelezettséget meghatározó jogszabályból, döntően törvényből ered. Ebből kifolyólag a jogegységi határozatok tehát nem minősülnek jogalapoknak. A Hatóság megjegyzi továbbá, hogy a két hivatkozott jogegységi határozat semmilyen adatvédelmi szempontú megállapítást nem tartalmaz.

Az MNB rendelet[250] 5. §-a sem adatkezelési jogalap, mivel az úgynevezett jövedelemarányos törlesztőrészlet mutatóról rendelkezik.
A KHR[251], mint a Kérelmező munkahelyre vonatkozó személyes adatai kapcsán jogalapként hivatkozott jogszabály sem minősül jogalapnak, tekintettel arra, hogy ezen személyes adatok kezeléséről, illetve a központi hitelinformációs rendszerbe történő továbbításáról a törvény nem rendelkezik.

A Vht[252],. mint a bírósági végrehajtási eljárás szintén nem tekinthető a pénzintézetek személyes adatok kezelésének jogalapjaként.

A Kötelezett jogos érdekére hivatkozva kezeli a Kérelmező vezetői engedélye száma, neme, családi állapota, közös háztartásban élők száma, mobiltelefonszáma

[249] a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény (Hpt.)
[250] 32/2014. (IX. 10.) MNB rendelet a jövedelemarányos törlesztőrészlet és a hitelfedezeti arányok szabályozásáról (továbbiakban: MNB rendelet)
[251] a központi hitelinformációs rendszerről szóló 2011. évi CXXII. törvény (a továbbiakban: KHR)
[252] a bírósági végrehajtásról szóló 1994. évi LIII. törvény (a továbbiakban: Vht.

személyes adatait. Ezen személyes adatok kezelése szükségességét azonban nem támasztotta alá sem érdekmérlegeléssel, sem más dokumentummal, így a Kötelezett a Kérelmező ezen személyes adatai kezelésére sem jogosult.

Minderre tekintettel a Hatóság megállapítja, hogy a Kötelezett a Kérelmező engedményezés keretében történő személyes adatainak továbbítását (teljes neve, születési neve, anyja neve, születési helye és ideje, személyi igazolványának száma, állandó lakcíme, gépjármű rendszáma, levelezési címe, mobiltelefonszáma, munkahelyi telefonos elérhetősége) követően megfelelő adatkezelési cél és jogalap hiányában tárolja a Kérelmező Pmt. által nem megőrzendőnek minősülő személyes adatait, megsértve ezzel az általános adatvédelmi rendelet 6. cikk (1) bekezdését.

A Kötelezett az engedményezést követően a Pmt. szabályaira tekintettel a Kérelmezőnek csupán a családi és utóneve, születési családi és utóneve, állampolgársága, születési helye, ideje, anyja születési neve, lakcíme, ennek hiányában tartózkodási helye, illetve azonosító okmányának típusa és száma személyes adatait, illetve az azokat tartalmazó okiratokat őrizheti meg. Ugyanakkor a Kötelezett a Kérelmező ezen okiratokon, illetve az okiratokban található személyes adatokon az őrzésen kívül más adatkezelési műveletet nem végezhet, ide nem értve az esetleges jogi kötelezettségekből eredő, más hatóságok részére történő bemutatásukat."[253]

Létfontosságú érdek védelme [GDPR 6. cikk (1) bekezdés d) pont]

Ebben az esetben az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges. Leegyszerűsítve ezt a jogalapot csak akkor használhatjuk, amikor a másik ötöt nem tudjuk *(„más természetes személy létfontosságú érdekeire hivatkozással személyes adatok kezelésére akkor kerülhet sor, ha a szóban forgó adatkezelés egyéb jogalapon nem végezhető.")*[254].

Példa:

- ✓ *az ügyfélterünkben egy ügyfél rosszul lett, eszméletét vesztette és mentőt kell hívnunk hozzá, vagy megpróbáljuk elérni a közeli hozzátartozóját.*

Ha bármelyik másik jogalapra érvényesen tudunk hivatkozni, nem folyamodhatunk a „vitális érdekhez".

[253] NAIH/2019/1837/, https://naih.hu/files/NAIH_2019_1837_hatarozat.pdf, utolsó letöltés: 2022. 08. 22.
[254] NAIH/2020/643/6. (NAIH/2019/5963.)

Az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása [GDPR 6. cikk (1) bekezdés e) pont]

Ebben az esetben az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.

Ezen jogalap esetében – ugyanúgy, mint az adatkezelőre vonatkozó jogi kötelezettség során – az adatkezelés jogalapját az uniós jognak vagy azon tagállamnak a joga kell, hogy megállapítsa, amely hatálya alá az adatkezelő tartozik.

Ez a jogalap olyan helyzetekre terjed ki, amikor az adatkezelő

- ✓ maga rendelkezik közhatalmi jogosítvánnyal vagy
- ✓ van közérdekből elvégzendő feladata, és az adatkezelés ennek a feladatnak az elvégzéséhez szükséges.

Ezt a jogalapot használhatják például az önálló bírósági végrehajtók tevékenységük folytán, illetve az önkormányzat az épületében üzemeltett kamerarendszere tekintetében, míg az alkalmazottak megfigyelésének nem lehet ez a jogalapja még akkor sem, ha közfeladatot lát el az adott adatkezelő.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

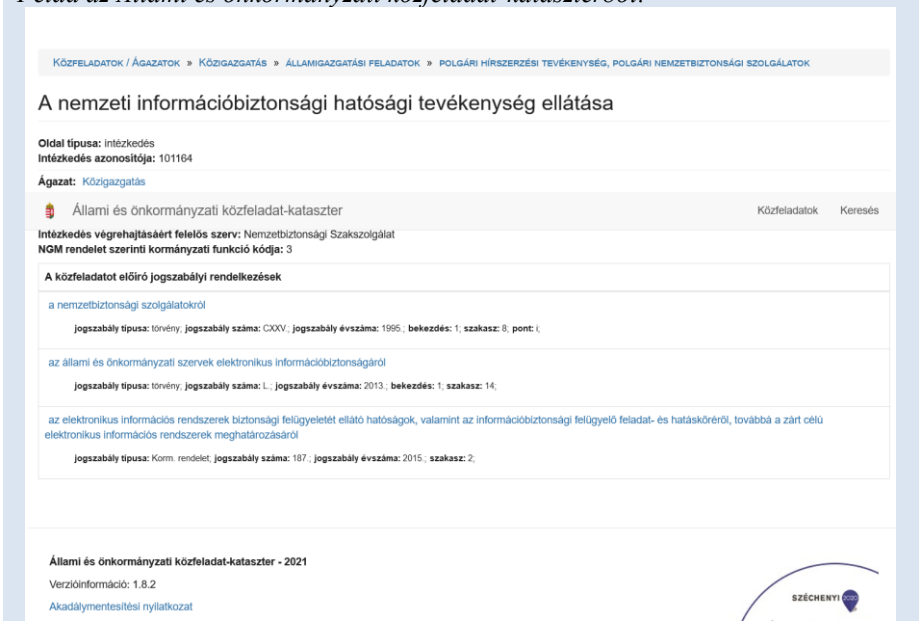
„A közérdekű feladat ellátásához és közhatalom gyakorlásához szükséges adatkezelés mint adatkezelési jogalap kapcsán, (…) e jogalap alkalmazásához feltétel, hogy az adatkezelő közhatalmi feladat- és hatáskörének gyakorlásához, vagy egyéb közérdekből elvégzendő feladata végrehajtásához szükséges adatkezelési tevékenységét közérdeken alapuló célból jogszabály, vagy uniós norma alapozza meg. Ezen jogszabályi rendelkezés ugyanakkor sok esetben csak az adatkezelő közfeladatát, eljárási mozgásterét és kötelezettségét határozza meg, az ehhez kapcsolódó adatkezelési műveletek részletes szabályait nem.

Az adatkezelő közfeladatait meghatározó jogszabályi rendelkezéseken alapuló adatkezelések jogalapja tehát a GDPR 6. cikk (1) bekezdés e) pontja. (…) egy közhatalmi tevékenységet vagy egyéb közfeladatot ellátó szerv – mint költségvetési szerv – minden közjogi és magánjogi jogviszonyának, és az ahhoz járulékosan kapcsolódó adatkezelési jogviszonyainak kizárólag közfeladatai ellátásával összefüggésben lehet alanya, ettől eltérő minősége fogalmilag kizárt. Ebből fakadóan e jogalap, mintegy magába olvasztja, elnyeli a további adatkezelési jogalapokat. E felfogást tükrözi – az általános adatvédelmi rendelettel szemben a magánszféra adatkezelésére tárgyi és szervi hatálya folytán egyáltalán nem alkalmazandó – bűnügyi adatvédelmi irányelv is, ahol az adatkezelés jogalapja kizárólag az irányelv hatálya alá tartozó tevékenység, mint közfeladat lehet [8. cikk].”[255]

[255] A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2018. évi tevékenységéről, B/4542, https://naih.hu/files/Beszamolo-2018-MR.PDF, utolsó letöltés: 2022. 08. 22.

Az, hogy mi a közfeladat, nem mindig egyszerű eldönteni – az egyik támpont lehet az Állami és önkormányzati közfeladat-kataszter.[256]

Példa az Állami és önkormányzati közfeladat-kataszterből:[257]



A közfeladatot ellátó adatkezelők ezt a jogalapot használhatják például olyan esetekben, mint

- ✓ a helyiségek videokamerás megfigyelése biztonsági okokból,
- ✓ az e-mail forgalom elektronikus ellenőrzése, illetve
- ✓ az alkalmazottak értékelése,

amikor ezekre a tevékenységekre a közfeladat ellátása érdekében van szükség. Ebből a szempontból ez a jogalap hasonlóságot mutat a jogos érdekre hivatkozással, és ebben az esetben is megilleti az érintettet az adatkezelés elleni tiltakozás joga.

A jogos érdekre hivatkozás nem alkalmazható a közhatalmi szervek közfeladataik ellátása során végzett adatkezelésre.

Példák a „közérdekre" és „közfeladatra"

- ✓ *óvoda/iskola közfeladatának ellátása keretében kezeli a gyermekek és szüleik adatait*
- ✓ *az adóhatóság feldolgozza a hozzá benyújtott adóbevallásokat*
- ✓ *a kamara etikai eljárást folytat a tagja ellen*
- ✓ *az önkormányzat az épületében kamerarendszert működtet*

Az Infotv. a kötelező adatkezeléssel kapcsolatban tartalmaz olyan szakaszokat, amelyeket a GDPR kiegészítéseként alkalmazandók.

[256] https://kfk.pest.gov.hu/kozfeladat
[257] https://kfk.pest.gov.hu/kozfeladat/36679/36680/36803/101164

Eszerint

- ✓ a GDPR 6. cikk (1) bekezdés c) és e) pontjában meghatározott adatkezelés („kötelező adatkezelés") esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.
- ✓ kizárólag állami vagy önkormányzati szerv kezelheti az állam bűncselekmények megelőzésére, felderítésére és üldözésére irányuló, valamint közigazgatási és igazságszolgáltatási feladatainak ellátása céljából kezelt bűnügyi személyes adatokat, valamint a szabálysértési, a polgári peres és nemperes ügyekre, valamint a közigazgatási peres és nemperes ügyekre vonatkozó adatokat tartalmazó nyilvántartásokat.
- ✓ ha a kötelező adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény, helyi önkormányzat rendelete vagy az Európai Unió kötelező jogi aktusa nem határozza meg, az adatkezelőnek az adatkezelés megkezdésétől legalább háromévente felül kell vizsgálnia, hogy az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e. Ezen felülvizsgálat körülményeit és eredményét dokumentálni kell és e dokumentációt a felülvizsgálat elvégzését követő tíz évig megőrizni és azt a NAIH kérésére a NAIH rendelkezésére kell tudni bocsátani.
- ✓ a tudományos kutatást végző szerv vagy személy személyes adatot nyilvánosságra hozhat, ha az a történelmi eseményekről folytatott kutatások eredményeinek bemutatásához szükséges.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Az Egyetem arra hivatkozott, hogy a hozzájárulás önkéntessége megítélésük szerint abban nyilvánul meg, hogy maga a pályázat leadása önkéntes. E szempont természetesen a Korm. rendelet[258] 11. § (3) bekezdésében is megjelenik, ugyanis a szociális alapú ösztöndíj esetére rögzíti, hogy az hallgatói kérelemre adható. De ez pusztán annyit jelent, hogy az Egyetem nem kötelezi – és nem is kötelezheti – a hallgatót arra, hogy szociális alapú ösztöndíjat pályázzon meg, amennyiben arra feltehetően jogosult lenne, hanem kizárólag a hallgató döntésétől függ, hogy kíván-e leadni pályázatot vagy sem.

A GDPR szerinti hozzájárulás – mint adatkezelési jogalap – azonban akkor állhat fenn, ha a hallgató nem pusztán arról dönthet, hogy részt kíván-e venni egy – adatkezeléssel is együtt járó – folyamatban, azaz jelen esetben arról, hogy benyújt-e pályázatot vagy sem, hanem arról is, hogy önkéntesen dönthet arról is, hogy milyen adatainak kezelését kívánja, és mely adatainak kezeléséhez nem járul hozzá, anélkül, hogy ebből bármilyen hátrány érné. Bár a hallgató szabadon dönthet arról, hogy bizonyos igazolást nem bocsát az Egyetem rendelkezésére, azonban ennek következtében az a hátrány fogja érni, hogy kevesebb pontot kap pályázatára, ami miatt kevesebb ösztöndíjra lesz jogosult vagy adott esetben elesik attól a

[258] A felsőoktatásban részt vevő hallgatók juttatásairól és az általuk fizetendő egyes térítésekről szóló 51/2007. (III. 26.) Korm. rendelet

támogatástól, amelyre egyébként a Korm. rendelet alapján – az ott meghatározott szempontok fennállása esetén – jogosult lenne.

Fentiek alapján a leadott pályázatokban szereplő valamennyi adat kezelésének jogalapja kizárólag a GDPR 6. cikk (1) bekezdés e) pontja lehet. Amennyiben az Egyetem olyan adatot is kezel, amely kezelése nem szükséges a Korm. rendelet által meghatározott szempontok figyelembevételéhez, illetve ezen felül új szempontokat is meghatároz, akkor adatkezelése jogalap nélküli, azaz a GDPR 6. cikkét sérti."[259]

Jogos érdek [GDPR 6. cikk (1) bekezdés f) pont]

A jogos érdek (illetve fordítástól függően „jogszerű érdek"[260]) jogalapra hivatkozás esetében az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Az Európai Adatvédelmi Testület (EDPB) gyakorlatából

A 3/2019. számú iránymutatás szerint a jogos érdeknek valóban fenn kell állnia és ténylegesen léteznie kell (vagyis nem lehet kitalált vagy feltételezett). A megfigyelés megkezdése előtt tényleges veszélyhelyzetnek kell felmerülnie, amely lehet például korábbi káresemény vagy súlyos incidens. Az elszámoltathatóság elvére tekintettel az adatkezelőnek javasolt írásban rögzítenie az ilyen incidenseket (dátum, módszer, pénzügyi veszteség). Az írásban rögzített incidensek meggyőző bizonyítékként szolgálhatnak a jogos érdek fennállására vonatkozóan. A jogos érdek fennállását és a megfigyelés szükségességét rendszeres időközönként (a körülményektől függően például évente egyszer) újra kell értékelni.[261]

Az érdeket minden esetben egyértelműen kell megfogalmaznunk, valamint valós és fennálló érdeket kell meghatároznunk, olyat, amely megfelel a jelenlegi tevékenységünknek vagy a közeljövőben várható előnyöknek.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„(…) nem az érintett, valamint nem a Hatóság feladata és felelőssége egy hatósági eljárás során az adatkezelő helyett az adatkezelés céljának és a jogos érdekeinek azonosítása és indokolása. Azt, hogy milyen célból és milyen jogos érdekei miatt kíván személyes adatot kezelni, az adatkezelőnek kell konkrétan, adat- és célszintre lebontva egyértelműen indokolni, mérlegelni és ennek garanciáit megteremteni.

[259] NAIH/2020/54/4. https://www.naih.hu/hatarozatok-vegzesek?download=325:1-rendszeres-szocialis-osztondijakkal-kapcsolatos-adatkezeles-a-budapesti-muszaki-es-gazdasagtudomanyi-egyetemen-modositasokkal-egyseges-szerkezetben, utolsó letöltés 2022. 08. 21.
[260] A 29. cikk szerinti adatvédelmi munkacsoport 6/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról, WP 217, Elfogadás időpontja: 2014. április 9., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf
[261] EDPB 3/2019. számú iránymutatás 20. bekezdés

Ezen garanciák kell, hogy biztosítsák többek között azt, hogy az érintett tisztában legyen az adatkezeléssel, és azzal szemben tiltakozni tudjon még az adatkezelést megelőzően, mivel az adatkezelést követően – különösen egy rövid ideig tartó vagy egyszeri adatkezelésnél – már kiüresedik a tiltakozási joga, így valójában nem biztosított ezen jog a számára."[262]

Jogos érdekre hivatkozva csak akkor kezelhetünk adatokat, ha előtte gondosan mérlegeltük az adott adatkezeléssel kapcsolatban felmerülő érdekeket és megfelelő garanciákat állítottunk fel, azaz érdekmérlegelési tesztet végeztünk.

Példák a „jogos érdekre"

- ✓ *munkavállalónak munkavégzés céljára kiadott notebook-ot ellenőrizzük, tényleg csak munkavégzésre használja-e*
- ✓ *munkavállalót ellenőrizzük, munkavégzésre képes állapotban van-e („megszondáztatjuk")*
- ✓ *üzleti partnerünk képviselőjének adatait nyilvántartjuk az üzleti partnerrel kötött szerződés teljesítése és a teljesítéshez szükséges kommunikáció biztosítása érdekében*
- ✓ *munkavállalóknak használatra kiadott céges autó rendeltetésszerű használatát ellenőrizzük*

A jogos érdek elsőre igazi jolly joker jogalapnak tűnhet, azonban a jogos érdek fennállásával adatkezelőként hatalmas felelősséget veszünk magunkra, mivel esetről esetre körültekintően

- ✓ meg kell határoznunk a saját vagy a harmadik fél jogos érdekeit,
- ✓ meg kell határoznunk az érintettek érdekeit, illetve alapvető jogait és szabadságait érő hatásokat (kockázatokat)
- ✓ valamint meg kell teremtenünk a megfelelő egyensúlyt az érdekek között és az ehhez szükséges biztosítékokat be kell építenünk az adatkezelésünk folyamatába.

A norvég Adatvédelmi Fellebbviteli Testület (Personvernnemnda) gyakorlatából

Egy szépségszalont 10 ezer euróra bírságoltak azért, mert az ügyvezető telefonos mobilalkalmazáson keresztül folyamatosan élőben hozzáférhetett az üzlet videokamera rendszere kép- és hangfelvételéhez úgy, hogy erről tájékoztatta volna az alkalmazottakat vagy az ügyfeleket.
Az ügyvezető a kamera felszerelését nem beszélte meg előzetesen a munkavállalókkal.

A Testület véleménye szerint egy munkahely folyamatos megfigyelése nagyon tolakodó a munkavállalók és az ügyfelek számára is, mivel nem volt megfelelő jelzés vagy tájékoztatás a megfigyelésről.[263]

[262] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: 2022. 07. 17.
[263] PVN-2021-20 Kameraovervåking i virksomhet – overtredelsesgebyr, (20/01648) https://pvn.no/pvn-2021-20, utolsó letöltés: 2022. 07. 14.

Ahhoz, hogy a hivatkozott érdek (akár a mienk, akár a harmadik félé) jogszerű legyen, három feltételnek kell megfelelnie:

- ✓ törvényesnek kell lennie (meg kell felelnünk az uniós és tagállami jognak),
- ✓ kellően egyértelműnek (konkrétnak) kell lennie, valamint
- ✓ valós és fennálló érdeket kell képviselnie (nem lehet elméleti érdek).

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A jogos érdek jogalappal kapcsolatban fontos hangsúlyozni, hogy az nem arra szolgál, hogy egyéb lehetőség hiányában az adatkezelő bármikor és bármilyen indokkal az egyéb jogalapok alkalmazhatóságának hiányában, a 6. cikk (1) bekezdés f) ponthoz fordulva kezeljen személyes adatokat. Bár látszólag a legrugalmasabb jogalapnak tűnik, annak alkalmazásával az adatkezelő jelentős felelősséget vállal – nem csak szűk értelemben a személyes adatok kezelésével, hanem az ahhoz kapcsolódó egyéb garanciális kötelezettségek teljesítésének felvállalásával is. Szorosan kapcsolódik ugyanis a jogos érdek jogalaphoz az általános adatvédelmi rendelet 5. cikk (2) bekezdésében foglalt elszámoltathatóság elve, mely az adatkezelőre a személyes adatkezelés átláthatóságát, pontosságát és tisztességességét szolgáló adminisztrációs terhek teljesítésének kötelezettségét jelenti. Nem „lepapírozásról" van tehát szó itt, hanem érdemi feladatról, mely megállapítás különösen igaz olyan adatkezelések esetében, ahol az adatkezelő és az érintett nincsenek közvetlen ügyféli vagy egyéb jogi kapcsolatban. A megfelelő garanciák hiányában ugyanis az érintetti jogok sérelmének veszélye olyan mértékű, hogy az érdekmérlegelés eredménye csak az lehet, hogy a harmadik fél jogos érdekét felülírják az érintetti jogai az adatkezeléssel járó kockázatok miatt (…)"

„Nagyon fontos azzal tisztában lennie az adatkezelőknek, hogy nem az érintett, valamint nem a Hatóság feladata és felelőssége egy hatósági eljárás során az adatkezelő helyett az adatkezelés céljának és a jogos érdekeinek azonosítása és indokolása. Azt, hogy milyen célból és milyen jogos érdekei miatt kíván személyes adatot kezelni, az adatkezelőnek kell konkrétan, adat- és célszintre lebontva egyértelműen indokolni, mérlegelni és ennek garanciáit megteremteni. Ezen garanciák kell, hogy biztosítsák többek között azt, hogy az érintett tisztában legyen az adatkezeléssel, és azzal szemben tiltakozni tudjon még az adatkezelést megelőzően, mivel az adatkezelést követően – különösen egy rövid ideig tartó vagy egyszeri adatkezelésnél – már kiüresedik a tiltakozási joga, így valójában nem biztosított ezen jog a számára."[264]

A szükségesség követelménye alapján

- ✓ a személyes adatok kezelésének az adatkezelő vagy harmadik fél jogos érdekének érvényesítéséhez szükséges kell, hogy legyen,
- ✓ meg kell fontolnunk, hogy kevésbé privát szférába hatoló eszközök is rendelkezésére állnak-e ugyanerre a célra.

[264] NAIH-2857-20/2021

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A munkaviszony időtartama alatt ez alapján a munkáltató gazdasági tevékenységének megfelelő működése érdekében a munkavállalók magánszféráját – hozzájárulásuk nélkül – bizonyos, pontosan körülhatárolt esetekben, garanciális követelmények megtartása mellett korlátozhatja.

Ez a legitim érdekek mérlegelése alapján történő adatkezelés elválaszthatatlan annak korlátaitól:

- *A munkáltatói ellenőrzés akkor tekinthető jogszerűnek, amennyiben az a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos [Mt. 9. § (2) bekezdés].*
- *A munkáltatói ellenőrzés és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével; illetőleg a munkavállaló a munkaviszonnyal összefüggő magatartása körében ellenőrizhető [Mt. 11/A. § (1) bekezdés].*
- *A munkavállalót előzetesen tájékoztatni kell az adatkezelés lényeges követelményeiről [Mt. 9. § (2) bekezdés és Mt. 11/A. § (1) bekezdés, általános adatvédelmi rendelet 13. cikk].*
- *Az adatkezelés akkor jogszerű, ha a munkáltató az adatkezeléssel kapcsolatban betartja az általános adatvédelmi rendelet alapvető rendelkezéseit: többek között a célhoz kötött és a tisztességes adatkezelés elvét [általános adatvédelmi rendelet 5. cikk (1) bekezdés a) és b) pont].*

Az Mt. rendelkezései általános felhatalmazást nyújtanak tehát a munkáltatói adatkezelésre, azonban ezen keretek tartalommal való megtöltése – az elszámoltathatóság elvével összhangban – a munkáltatóra hárul. A munkáltatónak az alkalmazott eszközökkel kapcsolatos részletszabályokat belső szabályzatban kell egyértelműen, érthetően, pontosan, részletesen meghatározni. Ennek kidolgozása során a munkáltatónak különös tekintettel kell lennie az arányosság követelményére valamennyi adatkezelési cél tekintetében."[265]

Mi lehet jogos érdek?

A jogos érdek az érdekek széles körét foglalhatja magában, legyenek azok jelentéktelenek vagy lényegesek, egyértelműek vagy ellentmondásosak.

Jogos érdek lehet

- ✓ *a szólás- vagy információszabadsághoz való jog gyakorlása (többek között a médiában és a művészetekben)*
- ✓ *a közvetlen üzletszerzés és a reklám hagyományos és egyéb formái*
- ✓ *nem kereskedelmi tárgyú kéretlen üzenetek (például politikai kampányokhoz vagy jótékonysági adománygyűjtéshez)*
- ✓ *jogi kérelmek végrehajtása (a peren kívüli eljárások útján történő követelésbehajtás is)*

[265] NAIH-3748-1/2021. Budapest, 2021. március 25, https://www.naih.hu/hatarozatok-vegzesek?download=380:kamerak-uzemeltetese-idosek-otthonaban, utolsó letöltés: 2022. 07. 14.

- ✓ *csalás, szolgáltatásokkal való visszaélés vagy pénzmosás megelőzése*
- ✓ *munkavállalók biztonsági vagy vezetési célú ellenőrzése*
- ✓ *belső visszaélés-bejelentési rendszer működtetése*
- ✓ *fizikai biztonság, informatikai és hálózati biztonság*
- ✓ *történelmi, tudományos vagy statisztikai célú adatkezelés*
- ✓ *kutatási célú adatkezelés (ideértve a piackutatást)*[266]

Az adatkezelő vagy a harmadik fél jogos érdeke az érdekek skáláján a jelentéktelentől a valamennyire fontos érdeken át egészen a lényegesig terjedhet. Az érintettek érdekeire és jogaira gyakorolt hatás ugyanígy lehet kevésbé vagy nagyon jelentős és a jelentéktelentől a nagyon komolyig terjedhet.

Az adatkezelő, illetve harmadik fél a jelentéktelenebb, vagy kevésbé lényeges jogos érdekeink általában csak akkor élvezhetnek elsőbbséget az érintettek érdekeivel és jogaival szemben, ha az említett jogokra és érdekekre gyakorolt hatás még ennél is elhanyagolhatóbb.

A spanyol adatvédelmi hatóság (AEPD) gyakorlatából

Az AEPD két bírságot szabott ki (2, illetve 3 millió euró értékben) a Banco Bilbao Vizcaya Argentaria (BBVA) SA-ra; a nagyobbik összegű bírságot a cég az adatkezelés jogszerűségének megsértése miatt kapta.

Az AEPD – többek között – felrótta a cégnek, hogy az adatkezeléseiről szóló tájékoztatásának hiánya miatt az érintettek nem tudták értékelni az adatkezelő által végzett, a jogos érdekkel kapcsolatos értékelést, és ezért nem kerülhetnek megfelelően tájékozott helyzetbe ahhoz, hogy tiltakozzanak a jogos érdeken alapuló adatkezelés ellen.

Ezen túlmenően a mérlegelés során figyelembe vett tényleges érdekekre vonatkozó információk hiánya azt jelenti, hogy a jogos érdek jogalapja nem érvényes; a mérlegelés hiányában nem lehet a jogos érdekre érvényes jogalapjaként hivatkozni. Mivel a BBVA mérlegelési gyakorlatára vonatkozó információk hiányoztak, ezért nehéz megítélni, hogy a cég érdekei jogosak voltak-e, és bár a gazdasági érdekek lehetnek jogosak, nem előzhetik meg az érintett alapvető jogait.

A hatóság még további körülményeket is figyelembe vett a döntésénél, többek között a jogos érdek alapján felhasznált adatok gyűjtésének módját, az adatgyűjtés túlzott mértékét, harmadik féltől az érintett tudta nélkül gyűjtött adatok felhasználását, az alkalmazott technikákat, a profilalkotás során alkalmazott logika átláthatóságának hiányát, az érintettek nagy számát, az érintettek adatait feletti ellenőrzésének elvesztését és az adatkezelő erőfölényét, valamint azt, hogy a BBVA nem alkalmazott további garanciákat, illetve intézkedéseket sem.

[266] A 29. cikk szerinti adatvédelmi munkacsoport 6/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról, WP 217, Elfogadás időpontja: 2014. április 9., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf

Mindezek alapján az AEPD úgy ítélte meg, hogy a BBVA adatkezelési gyakorlata nem értelmezhető úgy, hogy az az érintettek érdekeit szolgálta volna, és arra sem talált bizonyítékot, hogy a BBVA által hivatkozott jogos érdek érvényes lett volna, illetve elsőbbséget élvezne az érintettek érdekeivel, alapvető jogaival és szabadságaival szemben. A garanciák hiánya pedig azt eredményezte, hogy semmi sem tudta kiküszöbölni ezen személyes adatok kezelésével kapcsolatos egyensúlytalanságokat.
Ezért az adatvédelmi hatóság úgy ítélte meg, hogy a BBVA nem teljesítette a GDPR 6. cikk (1) bekezdésének f) pontjában foglalt feltételeket, azaz nem volt jogalapja az adatok kezelésének, amely állítólag jogos érdekre támaszkodott."[267]

Az érintetti érdekeket és jogokat tágabban kell értelmezni:

- ✓ az érintett valamennyi vonatkozó érdekét figyelembe kell venni,
- ✓ ha az adatkezelő vagy a harmadik fél bármilyen érdeket érvényesíthet, feltéve, hogy azok nem jogszerűtlenek, úgy az érintett szintén jogosult arra, hogy az érdekeinek valamennyi típusát figyelembe vegye az adatkezelő és összehasonlítsa a saját vagy a harmadik fél érdekeivel,
- ✓ az adatkezelő érdekeitől eltérően a „jogszerű" melléknév nem vonatkozik az érintettek érdekeire.

***A magyar adatvédelmi hatóság (NAIH) gyakorlatából** (munkavállalók ellenőrzése)*

„A legitim érdekek mérlegelése alapján történő adatkezelés elválaszthatatlan annak korlátaitól:
- A munkáltatói ellenőrzés akkor tekinthető jogszerűnek, amennyiben az a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos [Mt. 9. § (2) bekezdés].
- A munkáltatói ellenőrzés és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével; illetőleg a munkavállaló a munkaviszonnyal összefüggő magatartása körében ellenőrizhető [Mt. 11/A. § (1) bekezdés].
- A munkavállalót előzetesen tájékoztatni kell az adatkezelés lényeges követelményeiről [Mt. 9. § (2) bekezdés és Mt. 11/A. § (1) bekezdés, általános adatvédelmi rendelet 13. cikk]."[268]

Minden esetben, amikor a személyes adatok kezelését „jogos érdekek" alapján végezzük, az érintettnek bármikor joga van tiltakozni az adatkezelés ellen a saját egyéni helyzetével kapcsolatban. A tiltakozás alapján kötelesek vagyunk megszüntetni az adatkezelést kivéve akkor, ha igazoljuk, hogy annak folytatását kényszerítő erejű jogos okok indokolják.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A tiltakozási jog olyan alapvető garancia, amelynek hiánya minden más körülménytől függetlenül önmagában sikertelenné tehette volna a jogos érdek

[267] Procedimiento Nº: PS/00070/2019, https://www.aepd.es/es/documento/ps-00070-2019.pdf, utolsó letöltés 2022. 08. 27.
[268] NAIH-3748-1/2021.

elsőbbségének a megállapítását. Nem elegendő a jogos érdek fennállása, annak adott esetben meg kell előznie az érintetti jogokat, amely jelen esetben a megfelelő garanciák teljes hiányában nyilvánvalóan nem állhat fenn."[269]

Érdekmérlegelési teszt

A WP 29. cikk szerinti adatvédelmi munkacsoport gyakorlatából:

Az érdekmérlegelési teszt végzésének folyamata[270]
1. lépés: Melyik a potenciálisan alkalmazható jogalap a GDPR 6. cikk (1) bekezdés a)–f) pontja közül?
2. lépés: Az érdek jogszerűségének vagy jogszerűtlenségének megállapítása
3. lépés. Az adatkezelés az érdek érvényesítéséhez való szükségességének megállapítása
4. lépés: Ideiglenes egyensúly elérése annak mérlegelésével, hogy az adatkezelő érdekeivel szemben elsőbbséget élveznek-e az érintettek alapvető jogai vagy érdekei
5. lépés: Végleges egyensúly elérése a kiegészítő biztosítékok figyelembevételével
6. lépés: A megfelelés bizonyítása és az átláthatóság biztosítása
7. lépés: Mi történik, ha az érintett él a tiltakozási jogával?

Az érdekmérlegelés során

- ✓ azonosítanunk kell és részletesen le kell írnunk
  - az adatkezelésünk célját,
  - azonosítanunk kell az adatkezelésünk jogalapját,
  - a saját (adatkezelői), illetve a harmadik fél érdekeit (amennyiben harmadik fél jogos érdekeire hivatkozva kívánjuk kezelni az adatokat). A jogos érdekeket a lehető legpontosabban kell meghatároznunk. Mindig nekünk, az adatok kezelőjének kell megjelölnünk a jogos érdeket és azt nem elvileg és általában, hanem konkrét helyzetre, tevékenységre vonatkoztatva kell leírnunk. Az általános, konkrétumot nem tartalmazó meghatározás nem elegendő, ha így járunk el, azzal kiüresíthetjük az érdemérlegelési teszt intézményét és szembe megyünk a GDPR szellemével. Ahhoz, hogy az érdekünk jogos legyen,
    - ✓ törvényesnek kell lennie (vagyis meg kell felelnie az uniós és a tagállami jognak)
    - ✓ kellően egyértelműnek (konkrétnak) kell lennie
    - ✓ valós és fennálló érdeket kell képviselnie (nem lehet elméleti érdek).
  - az érintettek érdekeit, illetve azokat a körülményeket, amelyek indokolják az adatkezelést (azaz jogszerűvé teszik, hogy a saját

[269] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: 2022. 07. 17.
[270] 06/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról
Elfogadás időpontja: 2014. április 9. 844/14/HU WP 217, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf, utolsó letöltés: 2022. 08. 27.

érdekünk, illetve harmadik fél jogos érdeke felülírja az érintettek érdekeit). Azonban nemcsak a személyes adatokhoz való jogokat kell, mint érdeket megvizsgálnunk, hanem más olyan alapjogokat is, amelyeket például az Európa Unió Alapjogi Chartája, illetve az Alaptörvényünk tartalmaz (érintett magánszférához való joga, a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához való jog, a jóhírnév védelméhez fűződő jog, a gondolat-, a lelkiismereti és a vallásszabadság, a szabad véleménynyilvánításhoz való jog stb.). Nem tudjuk úgy összemérni az érdekeket, ha ezt a lépést kihagyjuk és csak a saját érdekeinkre összpontosítunk.

- ✓ el kell végeznünk az adatkezelésünk szükségességének és arányosságának vizsgálatát, mely során meg kell állapítanunk, hogy rendelkezésünkre állnak-e olyan alternatív megoldások, amelyeket alkalmazva a tervezett célunk az adott adatkezelés nélkül, illetve a tervezett adatkezelésünkhöz képest kevésbé korlátozó módon is megvalósítható. Ha ugyanazt a célt a személyes adatokhoz való jog kevésbé korlátozó módjával/eszközével is képesek vagyunk elérni (a racionalitás figyelembevételével), abban az esetben nem mondhatjuk ki, hogy fennáll a szükségesség, ezért aztán nem is hivatkozhatunk a jogos érdekre, mint jogalapra. A szükségesség vizsgálata során az alábbiakra kell kitérnünk:
  - az adott adatkezeléssel kapcsolatos helyzetünk konkrét, tényszerű leírása, például tevékenységi körünk, elhelyezkedésünk, ügyfélkörünk, iparági szokások, biztonsági problémáink stb. (pl. dominánsok vagyunk-e a területünkön?)
  - az általunk elérni kívánt konkrét cél meghatározása (akarunk profilozni? a célunk eléréséhez nagy mennyiségű adatra van-e szükségünk? stb.)
  - az érintetti kör adottságaira és arra, hogy milyen kapcsolatunk van velük (kiszolgáltatott rétegek, gyermekek, a mi anyanyelvünkön nem beszélő turisták, munkavállalóink stb.)
  - a tervezett adatkezelésünk miért és milyen mértékben korlátozza az érintettek magánszféráját (például időtartam, milyen típusú adatokra terjed ki, akarunk-e kezelni a különleges adatok kategóriájába tartozó vagy bűnügyi adatokat, van-e lehetőség elkerülni az adatkezelést stb.)
  - milyen forrásból jutunk az adatokhoz, az érintettek számíthatnak-e az adatkezelésünkre
  - milyen típusú adatokat gyűjtünk? („sima” személyes adat, különleges adat, „szenzitív” adat)
  - van-e az adatkezelésünknek kedvező hatása az érintettekre
  - kikérjük az érintettek véleményét? (például munkavállalók esetében az üzemi tanács véleményének kikérése)
  - hogyan kívánjuk érvényesíteni az érintettek tiltakozási jogát
  - használunk-e kockázatcsökkentő eljárásokat, például többfaktoros azonosítás, álnevesítés stb.
  - annak leírása, hogy a tervezett adatkezelésünk – szerintünk – miért hatékony és miért a legkevésbé korlátozó eszköz a célunk

eléréséhez, valamint a más, alternatív eszközök miért nem megfelelőek a számunkra.

- ✓ el kell végeznünk az érdekmérlegelést, azaz be kell mutatnunk, hogy a jogos érdekünk miért korlátozza arányosan az érintettek jogait. Nem csak arra kell kitérnünk, hogy nekünk miért jár megfelelő eredménnyel az adatkezelésünk, hanem az adatkezelésünkkel kapcsolatban valamennyi szempontot figyelembe kell vennünk és egyenként, valamint összességében és egymásra hatásukban is mérlegelnünk kell. Azt is meg kell vizsgálnunk, hogy miért nem döntöttünk más eszköz mellett, az általunk preferált módszer miért alkalmasabb a célunk elérésére, illetve az érintettek jogaira és szabadságaira nézve miért kedvezőbb, mint a többi lehetséges megoldás.
- ✓ részletesen meg kell határoznunk és le kell írnunk mindazokat a biztosítékokat (garanciákat), amelyek az adatkezelésünk által okozott behatásokat csökkentik, például
    - hogyan kívánjuk érvényesíteni a fokozatosság elvét
    - hogyan korlátozzuk az adatok tárolási idejét, az adatokhoz hozzáférők körét
    - hogyan csökkenthetjük az általunk használt adatok mennyiségét (adattakarékosság érvényesítése)
    - folyamodhatunk-e funkcionális szétválasztáshoz
    - hogyan használhatunk anonimizálási technikákat
    - hogyan segítjük az érintetti jogok gyakorlását (pl. tiltakozási jog) stb.
- ✓ részletes, minden körülményre kiterjedő dokumentációt kell készítenünk az érdekmérlegelési folyamatunkról és annak megállapításairól (ezzel megfelelve az elszámoltathatóság elvének is),
- ✓ gondoskodnunk kell az érintetti jogok tényleges érvényesüléséről
    - a tiltakozási jog „feltétlen”, mérlegelési jog nélküli érvényesülése (a GDPR-ban meghatározott esetekben), illetve van-e lehetőségünk arra, hogy ezt a feltétlen érvényesülést kiterjesszük a kötelező eseteken túlra is
    - egyéb esetekben annak biztosítása, hogy megfelelő és felhasználóbarát mechanizmust alkalmazzunk, amelyben az érintett tiltakozása esetén újraértékeljük az egyensúlyt, illetve leállítjuk az adatainak kezelését abban az esetben, ha az értékelésünk eredményeképpen az érintett érdekei elsőbbséget élveznek.
- ✓ nemcsak előre kell meghatároznunk, hogy mit szeretnénk csinálni, hanem arra is kell gondolnunk, hogy az adatkezelés megkezdése után milyen módon követjük figyelemmel az adatkezelésünk, illetve a környezetünk változásából adódó igényváltozásokat.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A Hatóság által tapasztalt leggyakoribb hibák kamerás ügyekben:

- *az adatkezelői jogos érdek meghatározásának általánossága, absztraktsága, elméletisége;*
- *az adatkezelői jogos érdek meg van ugyan határozva, de az eset konkrét körülményei nem igazolják a jogos érdek fennállását – az alkalmasság*

igazolásának hiánya (például vagyonbiztonsági cél megjelölése trafikban folyamatos munkavállalóra irányított rögzítés nélküli kamerával, amelyet a munkáltató „szúrópróbaszerűen" ellenőriz);

- *az adatkezelő helytelen vagy zavaros meghatározása (például magánszemély lakásán működő gazdasági társaság esetén nem derül ki, hogy háztartási adatkezelés vagy vagyonbiztonsági célú kamerás adatkezelésről van szó);*
- *a „szükségességi teszt" elhanyagolása – tényalapú, a konkrét esethez igazított mérlegelés hiánya annak figyelembevételével, hogy van-e kevésbé sértő beavatkozás az érintett magánszférájába."*[271]

Adatkezelőként adatkezelési célonként külön-külön érdekmérlegelési tesztet kell végeznünk, mely során:

- ✓ a tervezett adatkezelés megkezdése előtt át kell tekintenünk, hogy
  - a célunk elérése érdekében feltétlenül szükséges-e személyes adatok kezelése,
  - a személyes adatok kezelése tisztességes-e a leendő érintettekkel szemben, illetve
  - rendelkezésünkre állnak-e olyan alternatív megoldások, amelyek alkalmazásával személyes adatok kezelése nélkül is megvalósítható a tervezett célunk,
- ✓ meghatározzuk a saját vagy harmadik fél jogos érdekét,
- ✓ meghatározzuk, hogy mi az adatkezelés célja, milyen személyes adatok meddig tartó adatkezelését igényli a jogos érdek, illetve a tervezett adatkezelés átlátható-e,
- ✓ meghatározzuk, hogy az érintetteknek melyek lehetnek az érdekeik az adott adatkezelés vonatkozásában,
- ✓ meghatározzuk, hogy miért korlátozza arányosan a saját (adatkezelői) vagy harmadik fél jogos érdeke – és az ennek alapján végzett adatkezelés – az érintetti jogokat, illetve hogyan érvényesülhet a fokozatosság elve, valamint az érintettek jelenlétének biztosítása.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„(…) a munkahelyi kamerás megfigyelésnek abszolút korlátját jelenti az emberi méltóság tiszteletben tartása, ezért kamerákat a munkavállalók és az általuk végzett tevékenység állandó jellegű, kifejezett cél nélküli megfigyelésére működtetni nem lehet. Jogellenesnek tekinthető az olyan elektronikus megfigyelőrendszer alkalmazása is, amelynek célja a munkavállalók munkahelyi viselkedésének a befolyásolása, a munkavállalók kamerákkal történő állandó jellegű megfigyelése, ellenőrzése. Enne oka, hogy az ellenőrzési célú megfigyelés jellemzően sérti a szükségesség-arányosság elvét, hiszen a munkáltatónak számos más módja van arra, hogy éljen az Mt. 11/A. § (1) bekezdés szerinti ellenőrzési jogával. Ezért tehát nem lehet olyan kamerákat üzemeltetni, amelyek kizárólag a munkavállalókat és az általuk végzett tevékenységet figyelik meg állandó jelleggel. Kivételt képeznek az

[271] A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2020. évi tevékenységéről, B/14647, https://www.naih.hu/eves-beszamolok?download=349:naih-beszamolo-a-2020-evi-tevekenysegrol, utolsó letöltés: 2022. 08. 22.

olyan munkahelyiségek, ahol a munkavállalók élete és testi épsége közvetlen veszélyben lehet, így kivételesen működtethető kamera például a szerelőcsarnokban, kohóban, ipari üzemekben vagy más, veszélyforrást tartalmazó létesítményekben. Hangsúlyozni kell azonban azt, hogy csak abban az esetben működtethető kamera a munkavállalók élet- és testi épségének védelme céljából, ha a veszély ténylegesen fennáll és közvetlen, vagyis az eshetőleges veszély nem lehet alkotmányosan elfogadható adatkezelési cél. Mindezt azonban a munkáltatónak kell bizonyítania az érdekmérlegelési tesztben.

Vagyonvédelmi célú megfigyelés esetén szintén a munkáltatónak kell igazolnia az érdekmérlegelés során, hogy ténylegesen fennállnak olyan körülmények, amelyek indokolják az egyes kamerák elhelyezését és más módon nem biztosítható az elérendő cél. A vagyonvédelmi célú megfigyelés esetén további fontos követelmény, hogy a munkáltatónak különös figyelemmel kell lennie arra, hogy az adott kamera látószöge alapvetően a védendő vagyontárgyra irányuljon, és a fentiekből következően ne váljon a munkavállalók munkavégzésének megfigyelésére alkalmas eszközzé.

Emellett szintén nem lehet elektronikus megfigyelőrendszert alkalmazni olyan helyiségben sem, amely a munkavállalók munkaközi szüneténeк eltöltése céljából lett kijelölve. Ez alól kivételt jelenthet az az esetkör, ha ezen helyiségben valamilyen védendő, értékes vagyontárgy található, amellyel összefüggésben igazolható valamilyen munkáltatói érdek (például a munkavállalók többször megrongálták a berendezést és a károkat a munkáltatónak kellett állnia). Ebben az esetben e konkrét cél érdekében kamera helyezhető el a helyiségben, azonban ekkor a munkáltatónak – az adattakarékosság elvéből is következően – szintén különös figyelemmel kell lennie arra, hogy a kamera látószöge kizárólag a védendő vagyontárgyra irányulhat."[272]

Adatkezelőként különféle biztosítékokat építhetünk be az adatkezelésünkbe annak érdekében, hogy csökkentsük az érintettekre gyakorolt hatást, így például:

- ✓ szigorúan korlátozhatjuk az összegyűjtött adatok mennyiségét vagy törölhetjük az adatokat azonnal a felhasználásuk után,
- ✓ technikai és szervezeti intézkedéseket tehetünk annak biztosítására, hogy az adatokat ne lehessen az egyének vonatkozásában döntések meghozatalára vagy más lépések megtételére felhasználni („funkcionális szétválasztás", profilozás elkerülése stb.),
- ✓ anonimizálási technikákat használhatunk (például kikockázzuk a videofelvételt stb.),
- ✓ összesíthetjük az adatokat (aggregálás),
- ✓ folyamodhatunk a magánélet védelmét erősítő technológiákhoz,
- ✓ növelhetjük az átláthatóságot (például hatásvizsgálat lefolytatása, részletes és ismétlődő adatkezelési tájékoztatás nyújtása stb.),
- ✓ biztosítjuk az adatkezelés elleni tiltakozás általános és feltétel nélküli jogát,
- ✓ többfaktorú azonosítást vezethetünk be,

[272] NAIH-1006-3/2022, Budapest, 2022. március 29., https://www.naih.hu/hatarozatok-vegzesek?download=521:munkahelyi-kameras-megfigyeles-jogalapjanak-es-arrol-valo-tajekoztatasnak-jogszerusege, utolsó letöltés: 2022. 07. 14.

- ✓ gondoskodhatunk az adatok elkülönült tárolásáról, és a hozzáférés korlátozásáról.

Az Emberi Jogok Európai Bíróságának gyakorlatából

„A Bíróság által a Bărbulescu kontra Románia [GC] ügyben megállapított elvek értelemszerűen átültethetők azokra a körülményekre, amelyek között a munkáltató a munkahelyen videómegfigyelési intézkedéseket alkalmazhat. Ezeket a kritériumokat a munkaviszonyok sajátosságainak és az új technológiák fejlődésének figyelembevételével kellett alkalmazni, amelyek lehetővé tehetik a munkavállalók magánéletébe egyre inkább beavatkozó intézkedések meghozatalát. Ebben az összefüggésben a munkahelyi videokamerás megfigyelési intézkedések arányosságának biztosítása érdekében a hazai bíróságoknak a különböző egymással versengő érdekek mérlegelése során a következő tényezőket kellett figyelembe venniük:

- *a munkavállalót értesítették-e a videokamerás megfigyelés lehetőségéről a munkáltató által elfogadott intézkedések lehetőségéről és az ilyen intézkedések végrehajtásáról: míg a gyakorlatban a munkavállalókat különböző módon értesíthetik, az adott tagállamtól függően. az egyes esetek konkrét ténybeli körülményeitől függően, az értesítésnek általában egyértelműnek kell lennie. a megfigyelés jellegéről, és a végrehajtás előtt kell megadni;*
- *a munkáltató által végzett megfigyelés mértéke és a munkavállaló magánéletébe való beavatkozás mértéke: ebben az összefüggésben figyelembe kell venni a megfigyelt terület magánszféra-szintjét, valamint az időbeli és térbeli korlátozásokat és az eredményekhez hozzáférő személyek számát;*
- *hogy a munkáltató megalapozottan indokolta-e a megfigyelést, és annak mértékét: minél beavatkozóbb a megfigyelés, annál nagyobb súlya van annak az indokolásnak, amelyet a munkáltatónak szükséges megindokolnia;*
- *lehetséges lett volna-e kevésbé beavatkozó módszereken és intézkedéseken alapuló ellenőrzési rendszer létrehozása: ebben az összefüggésben az egyes esetek sajátos körülményei alapján kell értékelni, hogy a munkáltató által kitűzött célt el lehetett volna-e érni a munkavállaló magánéletébe való ilyen mértékű beavatkozás nélkül;*
- *a megfigyelés következményei az annak alávetett munkavállalóra nézve: figyelembe kell venni különösen azt, hogy a munkáltató hogyan használta fel a megfigyelés eredményeit, és hogy ezeket az eredményeket az intézkedés kitűzött céljának elérésére használták-e fel;*
- *hogy a munkavállaló megfelelő biztosítékokat kapott-e, különösen akkor, ha a munkáltató megfigyelési műveletei tolakodó jellegűek. Az ilyen biztosítékok többek között a következők lehetnek: az érintett munkavállalók vagy a személyzeti képviselők tájékoztatása a megfigyelés bevezetéséről és mértékéről; az ilyen intézkedésről egy független szervnek történő bejelentés; vagy a panasz benyújtásának lehetősége (López Ribalda and*

Others v. Spain [GC] – 1874/13 and 8567/13, Judgment 17.10.2019 [GC]).”[273]

Milyen eredményre juthatunk az érdekmérlegelési teszt elvégzése után?

- ✓ megállapíthatjuk a teljes megfelelést, azaz azt, hogy a kellő biztosítékok folyamatba építése után az adatkezelés érintettekre gyakorolt hatása úgy csökken, hogy kevésbé valószínű, hogy az érintettek érdekeit, alapvető jogait vagy szabadságait megzavarjuk (azaz alkalmazhatjuk a jogalapot),
- ✓ nem tudjuk megállapítani, hogy merre billen a mérleg, ezért további értékelést végzünk annak érdekében, hogy lehetséges-e további intézkedések bevezetése révén az adatkezelés érintettekre gyakorolt aránytalan hatást elfogadható szintre csökkentenünk,
- ✓ úgy is dönthetünk, hogy nincs vagy nem elegendő a megfelelés, ezért az adatkezelést nem folytathatjuk (más megoldást keresnünk, lemondunk az adott adatkezelésről stb.).

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Az érdekmérlegelés nem célonként külön történt, hanem minden célt összemos egy adatkezelésbe. Az adott adatkezelési cél elérésére alkalmasság és arányosság kérdését kellett volna vizsgálni, ehelyett az Ügyfél a mérlegelése során kizárólag a saját – vélt vagy valós – érdekei alapján vizsgálta, hogy arra szükséges és arányos-e az adatkezelés, és még ez is csak formális szempontok szerint történt. Az Ügyfél csak azt állapította meg, hogy az általa elérni kívánt érdeke érvényesítéséhez szükséges az adatkezelés, nem az érintetti jogokkal vetette össze az egyes célok esetén végzett tevékenységének hatását. Az arányosságot, az érintetti oldalt ténylegesen nem vizsgálta, bagatellizálta a jelentős alapjogi kockázatokat. Kifejezetten tényellenesen vette figyelembe a megfelelő tájékoztatás és tiltakozási jog garanciális hatását, amely jogokat a valóságban a rendszer felépítéséből adódóan nem biztosítanak az érintetteknek, teljes mértékben elvonva az érintetti önrendelkezési jogot. Így az érdekmérlegelés eredménye a fentiekben kifejtettek szerint alapvetően téves és félrevezető az alkalmasság és arányosság kérdésében, továbbá nem is azt veti össze egymással, amit kellene. (…)

Az adatkezelés megalapozatlan, illetve téves megtervezése és mérlegelése nem minősül az Ügyfél érdekkörén kívüli, elháríthatatlan oknak, az kizárólag az Ügyfél szándékos cselekménye, amely annak tudatában kezdte meg illetve folytatta az adatkezelést, hogy az alapvető hiányosságokban szenvedett, és az érdekmérlegeléssel nem volt ténylegesen alátámasztva, csak lepapírozva. Az Ügyfél nem igazolta, hogy bármely alternatívát ténylegesen megvizsgált volna. (…)

(…) az Ügyfél által elvégzett érdekmérlegelés nem ad valós, az általános adatvédelmi rendelet által elvárt elemzésen alapuló eredményt, így az arra alapított jogos érdek elsőbbsége az érintetti jogokkal és szabadságokkal szemben nem állapítható meg az adott adatkezelés során”[274]

[273] https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-12630%22]}

[274] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: 2022. 07. 17.

Az érdekmérlegelési tesztet az érintetteknek rendelkezésére kell tudnunk bocsátani.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„(…) Az Mt. 42. § (2) bekezdés a) pontja értelmében a munkaszerződés alapján a munkavállaló köteles a munkáltató irányítása szerint munkát végezni. Ezzel összhangban az Mt. 52. § (1) bekezdés b) és c) pontjai a munkavállaló alapvető kötelességeként határozták meg azt, hogy a munkavállaló köteles munkaideje alatt a munkáltató rendelkezésére állni és munkáját az általában elvárható szakértelemmel és gondossággal, a munkájára vonatkozó szabályok, előírások, utasítások és szokások szerint végezni. E törvényi kötelezettségek megtartása végett az Mt. 11/A. § (1) bekezdése lehetőséget biztosít arra, hogy a munkáltató a munkavállalót a munkaviszonnyal összefüggő magatartása körében ellenőrizze. Ez a jogosultság szükségszerűen együtt jár személyes adatok kezelésével.

A munkáltatói ellenőrzéshez kapcsolódó adatkezelés az Mt. rendelkezéseiből, a munkaviszony természetéből fakadó, a munkavállalói hozzájárulástól független adatkezelés. A hozzájárulással összefüggésben ugyanis meg kell jegyezni, hogy annak az általános adatvédelmi rendelet fogalommeghatározása szerint önkéntesnek kell lennie.

Az önkéntes hozzájárulás kapcsán ugyanakkor a már hatályon kívül helyezett adatvédelmi irányelv 29. cikke szerint létrehozott Adatvédelmi Munkacsoport (a továbbiakban: Adatvédelmi Munkacsoport) több állásfoglalásában is kifejtette, hogy a munkavállaló-munkáltató viszonyában megkérdőjelezhető az önkéntes hozzájárulás lehetősége. A munka világában az érintett hozzájárulása helyett ezért más jogalap, a munkáltató jogos érdekén alapuló adatkezelés alkalmazása indokolt. A (…) jogos érdek jogalapja értelmében tehát személyes adat kezelhető abban az esetben, ha az adatkezelés az adatkezelő (vagy harmadik fél) jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezen érdekeket megelőzi az érintettek személyes adatok védelméhez fűződő joga.

Lényeges, hogy a munkáltatónak, mint adatkezelőnek e jogalapra hivatkozáshoz érdekmérlegelést kell végeznie. Az érdekmérlegelés elvégzése egy többlépcsős folyamat, melynek során azonosítani kell az adatkezelő, azaz a munkáltató jogos érdekét, valamint a súlyozás ellenpontját képező adatalanyi, munkavállalói érdeket, érintett alapjogot, végül a súlyozás elvégzése alapján meg kell állapítani, hogy kezelhető-e személyes adat. Amennyiben az érdekmérlegelés eredményeként megállapítható, hogy a munkáltatói jogszerű érdek megelőzi a munkavállalók személyes adatok védelméhez fűződő jogát, úgy üzemeltethető kamerarendszer.
Az (…) „elszámoltathatóság elvéből" fakadóan azonban a munkáltatónak kell igazolnia azt, hogy az általa alkalmazott elektronikus megfigyelőrendszer összeegyeztethető a célhoz kötött adatkezelés elvével és az érdekmérlegelés kimenetele az adatkezelő jogos érdekének elsőbbrendűségét eredményezte. Ez a követelmény kijelöli annak kereteit, hogy munkahelyen milyen célból lehet elektronikus megfigyelőrendszert üzemeltetni.

A Hatóság ehelyütt azt is megjegyzi, hogy a lefolytatott érdekmérlegelés során az Ügyfélnek azt is figyelembe kell vennie, hogy a megfigyelni kívánt, osztatlan közös tulajdonban lévő ingatlan teljes területének megfigyelése miért elengedhetetlenül szükséges a meghatározott cél érdekében."[275]

[275] NAIH-1006-3/2022, Budapest, 2022. március 29., https://www.naih.hu/hatarozatok-vegzesek?download=521:munkahelyi-kameras-megfigyeles-jogalapjanak-es-arrol-valo-tajekoztatasnak-jogszerusege, utolsó letöltés: 2022. 07. 14.

ADATTÍPUSOK II.: AZ ADATOK KÜLÖNLEGES KATEGÓRIÁJÁBA TARTOZÓ ADATOK

A különleges adatok

Adatkezelőként minden személyes adatot meg kell védenünk, de vannak olyan adatok, amelyeket még jobban. Sőt, vannak olyan adatok, amelyeket olyan szinten véd a GDPR, hogy azokat alaphelyzetben nem is kezelhetjük csak akkor, ha a jogszabály által tételesen felsorolt plusz feltételek („kivételek") valamelyikét is teljesítjük.

Milyen adatokat védenek fokozottan az adatvédelemre vonatkozó jogszabályok? Egyrészt a személyes adatok különleges kategóriájába tartozó adatokat, másrészt a bűnügyi adatokat.

A GDPR (4) preambulumbekezdése alapján *„a személyes adatok védelméhez való jog nem abszolút jog, azt az arányosság elvével összhangban, a társadalomban betöltött szerepének függvényében kell figyelembe venni, egyensúlyban más alapvető jogokkal. Ez a rendelet minden alapvető jogot tiszteletben tart, és szem előtt tartja a Chartában elismert és a Szerződésekben rögzített szabadságokat és elveket, különösen ami a magán- és a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához és a személyes adatok védelméhez, a gondolat-, a lelkiismeret- és a vallásszabadsághoz, a véleménynyilvánítás szabadságához és a tájékozódás szabadságához, a vállalkozás szabadságához, a hatékony jogorvoslathoz és a tisztességes eljáráshoz, és a kulturális, vallási és nyelvi sokféleséghez való jogot illeti."*

Adatkezelőként számtalan módon juthat tudomásunkra különleges adat, például az ukrán származású munkavállalónk elmondja a véleményét a nem túl toleráns helyi polgármester politikai nézeteiről, miközben érdeklődik, merre van a környéken görög-keleti templom, amit szívesen meglátogatna, és vajon lenne-e következménye, ha a többi vendégmunkás érdekeit képviselve indulna a következő üzemi tanács választáson, egyébként pedig szívesen szolgáltat biometrikus adatot (ujjlenyomatot) a veszélyes anyag raktárba belépéshez, főleg mert már nem fáj a háta, így újra tud dolgozni. És még azt is megígéri, hogy legközelebb nem az öltözőben simogatja a titkárságról Titanilla kezét, hanem inkább elviszi moziba.

A személyes adatok különleges kategóriái

- ✓ a faji vagy etnikai származásra,
- ✓ politikai véleményre,
- ✓ vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint
- ✓ a genetikai adatok,
- ✓ a természetes személyek egyedi azonosítását célzó biometrikus adatok,
- ✓ az egészségügyi adatok és
- ✓ a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.[276]

[276] GDPR 9. cikk (1) bekezdés

Az osztrák bírósági gyakorlatból

Az Osztrák Posta (Österreichische Post AG) természetes személyek politikai pártokhoz való kötődésére vonatkozó adatokat értékesített ügyfeleinek. A témával kapcsolatos széleskörű médiavisszhangra való tekintettel az Osztrák Adatvédelmi Hatóság (Datenschutzbehörde – DSB) hivatalból vizsgálatot indított az Osztrák Posta ellen. Az Osztrák Posta fellebbezést nyújtott be a DSB határozata ellen az osztrák szövetségi közigazgatási bírósághoz (Bundesverwaltungsgericht – BVwG), az ügy DSB helytelen jogi értékelésére hivatkozva.

A BVwG megállapította, hogy

- ✓ *a „politikai párthoz kötődésre" vonatkozó adatok a GDPR 4. cikkének (1) bekezdése értelmében személyes adatnak minősülnek. Ez a kötődés egy személy érdeklődésének kiszámított valószínűsége egy bizonyos politikai párt hirdetése iránt abból a célból, hogy korlátozzák a címzettet nem érdeklő politikai pártok hirdetésének küldését. Ez többek között regionális választási eredményeken, társadalmi-demográfiai információkon és közvéleménykutatásokon alapul. Mivel egy konkrét azonosítható*

természetes személyhez van rendelve, a GDPR 4. cikkének (1) bekezdése értelmében személyes adatnak minősül.

- ✓ *a „politikai párthoz kötődésre" vonatkozó adatok a személyes adatok különleges kategóriáinak minősülnek, nevezetesen a politikai véleményre vonatkozó adatok. A GDPR 9. cikkének célja az érintettek védelme a (feltételezett) politikai véleményükön alapuló megkülönböztetéssel szemben. Annak ellenére, hogy a „politikai párthoz kötődés" csak egy valószínűséget fejez ki, lehetővé teszi az azon a tényen alapuló megkülönböztetést, hogy az érintettekről feltételezhető, hogy különösen érdeklődnek egy vagy több konkrét politikai párt iránt.*
- ✓ *a „politikai párthoz kötődésre" vonatkozó adatok kezelése nem alapulhat a GDPR 9. cikk(2) bekezdésének g) pontján, mivel nem áll fenn jelentős közérdek. A GDPR 9. cikkének (2) bekezdése szerinti egyéb kivételek szintén nem igazolhatják a „politikai párthoz kötődésre" vonatkozó adatok kezelését, ezért annak az érintett kifejezett hozzájárulásán kell alapulnia [GDPR 9. cikk (2) bekezdésének a) pontja]. Mivel az Osztrák Posta nem gyűjtött be ilyen kifejezett hozzájárulást, az adatkezelés jogellenes volt.*

A BVwG fenntartotta a DSB által elrendelt adatkezelési tilalmat, de azt úgy korrigálta, hogy az csak a „politikai párthoz kötődésre" vonatkozó adatok kezelésére vonatkozzon".[277]

Bűnügyi adat: a büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatok.[278]

Az Európa Unió Bíróságának (EUB) gyakorlatából

„74 (... a) GDPR 10. cikk célja, hogy fokozott védelmet biztosítson az olyan adatkezeléssel szemben, amely a szóban forgó adatok különösen érzékeny jellege folytán különösen súlyos beavatkozást jelenthet a magánélet tiszteletben tartásához és a személyes adatok védelméhez való, a Charta 7. és 8. cikkében biztosított alapvető jogokba (...).

75 Mivel ugyanis azok az adatok, amelyekre az általános adatvédelmi rendelet 10. cikke utal, a társadalom helytelenítésével járó magatartásokra vonatkoznak, az ilyen adatokhoz való hozzáférés biztosítása megbélyegezheti az érintett személyt, és ezáltal a magánéletébe vagy szakmai életébe való súlyos beavatkozást képezhet.

82 (...) az általános adatvédelmi rendelet semmilyen utalást nem tartalmaz a nemzeti jogokra az e rendelet 10. cikkében szereplő kifejezések, különösen a „bűncselekmények" és a „büntetőjogi felelősség megállapítására vonatkozó határozatok" kifejezések terjedelmét illetően.

[277] W258 2217446-1/35E, https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20201126_W258_2217446_1_00/BVWGT_20201126_W258_2217446_1_00.pdf, utolsó letöltés 2022. 07. 24.
[278] GDPR 10. cikk

83 (…) az általános adatvédelmi rendelet (10) preambulumbekezdéséből kitűnik, hogy e rendelet célja, hogy hozzájáruljon a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség megteremtéséhez azáltal, hogy a személyes adatok kezelésével összefüggésben biztosítja a természetes személyek következetes és magas szintű védelmét, ami feltételezi, hogy e védelem szintje minden tagállamban azonos és egységes legyen. Márpedig e céllal ellentétes lenne, ha az e rendelkezésben előírt fokozott védelem csupán bizonyos tagállamokban lenne alkalmazandó a közúti közlekedési jogsértésekkel kapcsolatos személyes adatok kezelésére, más tagállamokban azonban nem, kizárólag azon az alapon, hogy e jogsértések az utóbbi tagállamokban nem minősülnek bűncselekménynek. (…)

85 (…) a „bűncselekmény” fogalmát, (…), az Unió egész területén önállóan és egységesen kell értelmezni, figyelembe véve az e rendelkezés által követett célt, valamint azon összefüggést, amelybe e rendelkezés illeszkedik, anélkül hogy e tekintetben meghatározó lenne e jogsértések érintett tagállam általi minősítése, mivel e minősítés tagállamonként eltérő lehet (…).

87 A Bíróság ítélkezési gyakorlata szerint három kritérium releváns a jogsértés büntetőjogi jellegének értékelése során. Az első a jogsértés belső jog szerinti jogi minősítése, a második a jogsértés jellege, a harmadik pedig az érintett személlyel szemben kiszabható szankció súlya (…).

88 Még azon jogsértések esetében is, amelyek a nemzeti jog szerint nem minősülnek „büntető jellegűnek”, e jelleg megállapítására mindazonáltal a szóban forgó jogsértés jellegéből és a jogsértés miatt kiszabható szankció súlyából fakadóan is sor kerülhet (…).

89 A jogsértés jellegére vonatkozó kritérium kapcsán azt kell megvizsgálni, hogy a szóban forgó szankció célja kifejezetten a megtorlásra irányul-e, és pusztán az, hogy megelőzésre irányuló célt is követ, nem foszthatja meg azt a büntetőjogi szankcióként való minősítéstől. A büntetőjogi szankciók ugyanis a jellegüknél fogva egyaránt szolgálják a jogellenes magatartás megtorlását és megelőzését. Ellenben egy olyan intézkedés, amely csupán az adott jogsértéssel okozott kár megtérítésére korlátozódik, nem ölt büntető jelleget (…). Márpedig nem vitatott, hogy büntetőpontok közúti közlekedési jogsértések miatti kiszabása – csakúgy, mint az e jogsértések elkövetése miatt kiszabható bírságok vagy egyéb szankciók – nem csupán az említett jogsértések által esetlegesen okozott károk megtérítésére, hanem emellett megtorlásra is irányul.

90 Ami az ugyanezen jogsértések elkövetése miatt kiszabható szankciók súlyára vonatkozó kritériumot illeti, mindenekelőtt rá kell mutatni arra, hogy kizárólag a bizonyos súllyal rendelkező közúti közlekedési jogsértések vonják maguk után büntetőpontok kiszabását, és következésképpen az ilyen jogsértések miatt kiszabható szankciók bizonyos súllyal rendelkeznek. A büntetőpontok kiszabása emellett általában hozzáadódik az ilyen jogsértés elkövetése esetén kiszabott szankcióhoz, (…). Végül, az említett pontok összege önmagában is jogkövetkezményeket – például vizsga letételére vonatkozó kötelezettséget vagy akár járművezetéstől való eltiltást – von maga után.

93 (…) azok a közúti közlekedési jogsértések, amelyek büntetőpontok kiszabását eredményezhetik, az általános adatvédelmi rendelet 10. cikkében említett „bűncselekmények" fogalma alá tartoznak.

94 (…) az általános adatvédelmi rendelet 10. cikkét úgy kell értelmezni, hogy azt alkalmazni kell a gépjárművezetőkkel szemben közúti közlekedési jogsértések miatt kiszabott büntetőpontokra vonatkozó személyes adatok kezelésére."[279]

Az Infotv. alapján[280] a **bűnügyi személyes adat** a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.[281]

A bűnügyi személyes adatok kezelése esetén – ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusa ettől eltérően nem rendelkezik – a különleges adatok kezelésének feltételeire vonatkozó szabályokat kell alkalmazni.[282]

Milyen különleges személyes adatokat tudhatunk meg egy átlagos közösségi média felhasználóról? *Például*

- ✓ *sváb családba született és a német kisebbségi önkormányzat falunapján mulatott a rokonaival (faji vagy etnikai származás)*
- ✓ *szabad idejében szívesen ellátogat a Le a személyi jövedelemadóval párt üléseire és buzgón hirdeti annak tanait (politikai vélemény)*
- ✓ *hiszi, hogy a Föld nem lehet gömb alakú, mert a labdáról is lefolyik a víz (világnézeti meggyőződés)*
- ✓ *vasárnaponként a családjával templomba látogat, a gyülekezet által meghirdetett zarándokutakon is részt vesz rendszeresen és felháborodik azon, ha valaki nem tartja be szigorúan a böjtöt (vallási meggyőződés)*
- ✓ *lelkes tagja a ködszurkálók szakszervezetének (szakszervezeti tagság)*
- ✓ *gyakran jár az orvoshoz a derékfájásával miközben hangoztatja, hogy ő sem lesz már fiatalabb (egészségügyi adat)*
- ✓ *öröklött betegségéről tesz közzé információt (genetikai adat)*
- ✓ *bejárása van a munkahelyén a hét lakat alatt őrzött veszélyes anyagokat tároló raktárba, ahova csak hangazonosítás után juthat be (a felhasználó ebben az esetben természetes személyek egyedi azonosítását célzó biometrikus adat használatára utalás, a tényleges használat azonban nem a közösségi médiában, hanem munkahelyén történik)*
- ✓ *eldicsekszik, hogy bejönnek neki a vörös bögyösök és e tárgyban melyik honlapnak jó a felhozatala (szexuális életre vagy szexuális irányultságára vonatkozó személyes adat).*

[279] C-439/19. sz. ügy (B kontra Latvijas Republikas Satversmes tiesa), https://curia.europa.eu/juris/document/document.jsf?text=&docid=243244&pageIndex=0&doclang=HU&mode=req&dir=&occ=first&part=1&cid=4159272, utolsó letöltés 2022. 07. 09.
[280] Az Infotv. 2.§ (2) bekezdése alapján a GDRP rendelkezéseit az Infotv. 3.§ 4. pontjában és az 5.§ (7) bekezdésében foglalt kiegészítésekkel kell alkalmazni.
[281] Infotv. 3.§ 4. pont
[282] Infotv. 5.§ (7) bekezdés

„Szenzitív" adatok: vannak olyan adatok, amelyek bár nem számítanak különleges adatnak mégis fokozott figyelmet kívánnak, ilyenek például a pénzügyi adatok (bankszámlaszám, kölcsönnel kapcsolatos adatok stb.) vagy a személyes azonosító jelek (adóazonosító jel, társadalombiztosítási azonosító jel, személyi azonosító stb.). A „szenzitív" adatoknak nincs külön kategóriája sem a GDPR-ban sem az Infotv-ben, ám a felügyeleti hatóságok határozatait böngészve a büntetéseknél súlyosbító körülményként jelenhet meg az, ha az ilyen típusú adatok kezelésével kapcsolatban történt a jogsértés.

Példák a GDPR hatálya alá tartozó bűnügyi adatok kezelésére

- ✓ *Bizonyos foglalkozások esetén a felvételi eljárás keretében a felvételre jelentkezőnek be kell mutatnia az erkölcsi bizonyítványát bizonyítva, hogy semmi olyat nem követett el, ami akadályozná a foglalkoztatását (pl. pedagógusok),*
- ✓ *az Mt. felsorolja azokat a munkaköröket, amelyek esetében a foglalkoztatás erkölcsi bizonyítványhoz köthető,*
- ✓ *a munkavállaló részegen összetöri a céges autót,*
- ✓ *a munkavállaló a foglalkoztatója sérelmére sikkasztást követ el.*

Az egészségügyi, a genetikai és a biometrikus adatok

Egyes különleges adatok kategóriába sorolása viszonylag egyértelmű, illetve történelmi hagyományokat követ (pl. szakszervezeti tagság vagy vallási meggyőződés), míg más különleges adatkategóriák meglehetősen összetettek lehetnek. A GDPR egyes különleges adattípusokat konkrétan meghatároz, ilyen az egészségügyi, a genetikai és a biometrikus adat.

Egészségügyi adat: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.[283]

Példák

- ✓ *egészségügyi adat például egy baleset során szerzett sérülésünk, a COVID19 elleni védettségünk és a vér alkoholezrelékünk is*
- ✓ *a kutyánk ivartalanított állapota a személyes adatok védelme szempontjából nem egészségügyi adat, hanem egyrészt a mi olyan személyes adatunk, amely a négylábú barátunkkal (tulajdonukkal) kapcsolatos, másrészt az állatorvos olyan személyes adata, amely munkavégzésével (általa elvállalt feladat elvégzésével) kapcsolatos*
- ✓ *a macskánk törött lába nem a személyes adatok különleges kategóriájába tartozó adat, addig a mi törött lábunk már igen*

Van olyan adat, amely különleges adatnak minősülése kontextus függő, ilyen például a TAJ szám, mivel azt hazánkban nemcsak egészségügyi célból, hanem egyéb célból is használjuk (pl. társadalombiztosítási járulékkal kapcsolatos adatkezelés stb.)

[283] GDPR 4. cikk 15. pont

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Különösen jogsértő továbbá, hogy az Egyetem a jogszabályokon túlterjeszkedve további különleges adatok kezeléséről is döntött, azonban nem volt tudomása arról, hogy egy fogyatékosságról/krónikus betegségről/rokkantság fokáról szóló szakorvosi igazolásban szereplő adat különleges adatnak minősül, hiszen önmagában egészségügyi – és ezáltal különleges – adat az, hogy adott személy fogyatékossággal él, krónikus betegsége van vagy rokkant, így az Egyetem ezáltal akkor is különleges adatot kezel, ha az érintett minden további adatot kitakar az igazoláson."[284]

„A hangelemzés eredményét képező adatok közül egyedül az érzelem, pszichikai állapot az, amely adott körülmények között biometrikus adatnak vagy egészségügyi adatnak minősülhet. Jelen esetben a feltárt tényállás szerint a hangelemzés során nem az érintettet egyedileg azonosító adat jön létre, így a biometrikus adat ezen feltétele hiányzik. Az egészségügyi adatnál pedig azon feltétel nem áll fenn, hogy az érintett fizikai vagy mentális egészségügyi állapotára érdemi következtetést lehetne levonni a jelen ügy tárgyát képező adatkezelés eredményéből. Ettől függetlenül nem az alkalmazott módszer vagy maga az adat minősége miatt nem állnak fenn a feltételek, így adott esetben más ügyekben azonos körülmények mellett a hasonló adat minősülhet különleges kategóriájú személyes adatnak, ha az egyéb körülmények, további adatokkal összekapcsolás alapján – amely a jelen ügyben nem történt – teljesítik a fenti feltételeket."[285]

Genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered.[286]

Példa

- ✓ *ha arra vetemedünk, hogy genetikai alapon családfát kutató vállalkozásnak adunk önként és dalolva genetikai mintát, ne lepődjünk meg azon, ha a teljes lényünk bekerül egy olyan adatbázisba, amelyből aztán a különféle országok legkülönfélébb szervezetei és hatóságai bátran csemegézhetnek egy-egy különösen veszélyesnek ítélt elkövető felkutatása érdekében. És bár lehet, hogy a mi lelkiismeretünk patyolat tiszta, unokatestvérünket még simán lebuktathatjuk akár egy már majdnem elfeledett, kishíján elévült bűncselekmény elkövetése miatt.*

[284] NAIH/2020/54/4. https://www.naih.hu/hatarozatok-vegzesek?download=325:1-rendszeres-szocialis-osztondijakkal-kapcsolatos-adatkezeles-a-budapesti-muszaki-es-gazdasagtudomanyi-egyetemen-modositasokkal-egyseges-szerkezetben, utolsó letöltés 2022. 08. 21.
[285] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei
[286] GDPR 4. cikk 13. pont

A magyar adatvédelmi hatóság (NAIH) álláspontja a családfakutató (DNS-elemző) szolgáltatásokkal kapcsolatban:

„Az elmúlt időszakban megnövekedett azon, az interneten elérhető szolgáltatások száma, amelyek DNS-mintavétel alapján kínálnak segítséget családfájuk és etnikai származásuk után kutató személyeknek. (…)

Az ilyen szolgáltatásokat nyújtó vállalkozások székhelye és tevékenységi helye (…) jellemzően nem az Európai Unióban található, így annak ellenére, hogy egyes esetekben tevékenységük a GDPR hatálya alá tartozik, az érintetteket megillető jogok gyakorlása és érdekeik hatékony érvényesítése nehézségekbe ütközhet.

Tipikus jellemzője e szolgáltatásoknak, hogy az érintett által rendelkezésre bocsátott genetikai mintákat, megszerzett adatokat az adatkezelők a szolgáltatás nyújtását követően is megőrzik, azokat számos esetben más felhasználó részére értékesítik és továbbítják. Noha ezen adattovábbításra jellemzően a genetikai adat eredetéhez kapcsolódó személyazonosító adatok nélkül kerül sor, a genetikai adatok jellege miatt azonban azok későbbi felhasználása során más adatokkal (pl. ismert személyazonosságú rokonok által megadott mintákból származó adatok) összekapcsolva visszanyerik személyazonosításra alkalmas természetüket.

(…) Az adatkezelők részére rendelkezésre álló eszközökkel ezen adatok alapján a szolgáltatást igénybe vevő személyekkel rokoni kapcsolatban álló további érintettek személyazonosságára, örökölt vagy szerzett genetikai jellemzőire – többek között egészségi állapotára, etnikai hovatartozására – is következtetés vonható le, ezen további érintettek tudta és hozzájárulása hiányában is.

Mindezekből fakadóan a NAIH nem javasolja, hogy a genetikai adat meghatározására alkalmas minták és genetikai adatok kezelésével kapcsolatosan az adatkezelő által biztosítandó, többek között az adatkezelés körülményeit, az esetleges adattovábbítás címzettjeit, az adatkezelés időtartamát és az érintettek jogainak ismertetését részletesen tartalmazó megfelelő tájékoztatás és genetikai adatok biztonságos kezelését célzó garanciák hiányában az érintettek DNS-minta elemzésén alapuló szolgáltatásokat vegyenek igénybe.”[287]

Biometrikus adat: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat.[288]

[287] A Nemzeti Adatvédelmi és Információszabadság Hatóság közleménye a DNS-elemző szolgáltatások igénybevételének veszélyeiről, 2019. március 23. https://www.naih.hu/dontesek-adatvedelem-tajekoztatok-koezlemenyek?download=83:a-nemzeti-adatvedelmi-es-informacioszabadsag-hatosag-kozlemenye-a-dns-elemzo-szolgaltatasok-igenybevetelenek-veszelyeiro, utolsó letöltés: 2022. 08.19

[288] GDPR 4. cikk 14. pont

A biometrikus technikáknak három fő kategóriája van:

- ✓ a fizikai és fiziológiai alapú technikák, amelyek egy személy fizikai és fiziológiai jellemzőit mérik, ilyen például az ujjlenyomat-ellenőrzés, az ujjkép-elemzés, az íriszfelismerés, a retinaelemzés, az arcfelismerés, a kézkörvonal-minták, a fülforma-felismerés, a testszagészlelés, a hangfelismerés, a DNS-mintázat elemzése és a verejtékpórus-elemzés stb.,
- ✓ viselkedésalapú technikák, amelyek a személy viselkedését mérik, és ezek közé tartozik a kézzel írt aláírás ellenőrzése, a gépírás elemzése, a járás elemzése, a járásmód vagy a mozgás módja, a valamilyen tudatalatti gondolatra, például hazugságra utaló mintázatok stb. elemzése.,
- ✓ pszichológiai alapú technikák, például a konkrét helyzetekre adott válaszok mérése, illetve a pszichológiai profilnak való megfelelés érdekében végzett speciális tesztek stb.[289]

Példa

- ✓ *az emberi szövetből vett – DNS-t tartalmazó – sejtminták is lehetnek biometrikus adatok kinyerésére alkalmas források, amennyiben az adatok az öröklött vagy szerzett genetikai jellemzőinkre vonatkoznak, egyedi információkat szolgáltatnak az egészségi vagy fiziológiai állapotunkról és a személyünkből nyert biológiai minta elemzésének az eredményei.*

A laikusok számára a „sima" személyes adat és a különleges adat közötti határ néha összemosódik, azonban ha be kell azonosítanunk egy adatot, abban az esetben az elhatároláshoz zsinórmértékként használhatjuk a feldolgozás módját (eszközét).

Példák

- ✓ *az arckép (fénykép, videófelvétel) önmagában „sima" személyes adat. Azonban akkor már biometrikus adat lesz, ha azt speciális eljárás keretében (például arcfelismerő szoftverrel kezelve) egyedi azonosítás céljára használjuk fel,*
- ✓ *a hangfelvétel esetében, ha ügyfélszolgálat készít hangfelvételt a hívásról az még nem biometrikus adat, azonban, ha egy hangfelvételt hangalapú azonosításhoz használunk, akkor már annak számít,*
- ✓ *a toborzás során az online interjú felvétele „sima" személyes adat, azonban, ha a felvételt érzelemfelismerésre alkalmas szoftverrel elemzik/kezelik, abban az esetben már biometrikus adat lesz.*

A biometrikus adatok biometrikus rendszerben történő feldolgozásának tipikus folyamatai:

- ✓ biometrikus felvétel: mindazok a folyamatokat értjük alatta, amelyeket egy biometrikus rendszeren belül a biometrikus adatok valamely biometrikus forrásból való kinyerése és azoknak egy egyénhez való kapcsolása érdekében

[289] 29. cikk szerinti adatvédelmi munkacsoport 3/2012. sz. vélemény a biometrikus technológiák terén történt fejleményekről, 2012. április 27, 00720/12/HU WP193, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_hu.pdf, utolsó letöltés: 2022.08.19

végzünk. A felvett adatok mennyiségének és minőségének megfelelőnek kell lenniük ahhoz, hogy lehetővé tegye az egyén pontos azonosítását, hitelesítését, kategorizálását vagy ellenőrzését úgy, hogy egyben megfeleljünk az adattakarékosság elvének is;
A felvételhez a legtöbb esetben az érintett személyes közreműködése szükséges ilyen például az ujjlenyomatvétel;

- ✓ biometrikus tárolás: a megszerzett biometrikus adatokat későbbi felhasználás céljából tárolhatjuk helyben, vagy az érintett által magánál tartott valamely eszközön (például egy intelligens kártyán), illetve központosított adatbázisban is tárolhatjuk az adatot;
- ✓ biometrikus megfeleltetés: a felvételkor rögzített biometrikus adatokat/sablont összevetjük egy új mintából gyűjtött biometrikus adatokkal/sablonnal azonosítás, ellenőrzés/hitelesítés vagy kategorizálás céljából.

A biometrikus adatok egyre fontosabbak lesznek és mára már eljutottunk oda, valójában egy államnak sincs fogalma arról, hogy az állampolgárai biometrikus adatai mely kontinensen és milyen adatbázisban találhatóak meg. Komoly gondot jelenthet a közösségi oldalak gigászi méretű (több milliárd személyre kiterjedő) biometrikus adathalmaza, amelyek nemcsak felnőttek, hanem gyermekek adatait (felvételeit) is tartalmazzák. Az arcfelismerés mellett az érzelemfelismerésen alapuló rendszerek egyre elterjettebbek, és az ujjlenyomatos azonosítás is belopózott a hétköznapjainkba (lásd okostelefon zárolása).

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Az arcfelismerő funkció – fent hivatkozott módon történő – alkalmazásával egy arcképről tárolt bélyegkép alapján végzett adatbázis művelet végrehajtásával, az arcképpel megjelölt személy további felvételeken is egyedileg könnyen azonosítható. Mivel a rendszer a nyilatkozatok szerint nincs összekapcsolva egyéb nyilvántartásokkal (pl: személyiadat- és lakcímnyilvántartás), ezért az érintett személyhez ekkor még nem köthetők természetes személyazonosító adatok. Ettől függetlenül az arckép és az annak alapján történt keresés, illetőleg találatok eredményeként a kiválasztott személy a felvételeken szereplő további személyektől elkülöníthetővé, tulajdonképpen egyedileg azonosíthatóvá, ezt követően pedig a rendszerben adott időben tárolt felvételeken könnyen követhetővé, megfigyelhetővé válik. A rendszer saját adatbázisban az arcfelismerésre képes mesterséges intelligencia révén történő keresés és a kiválasztott arckép mint személyes adat, további felvételekről történő kiválasztása értelemszerűen az adott személy egyedi azonosítását célzó biometrikus adatkezelést jelent. Mindez független attól, hogy természetes személyazonosító adatok vagy egyéb személyi azonosítók által az érintett személyazonosságának megállapítását önmagában ez a rendszer nem képes elvégezni.

Az arcfelismerésre képes mesterséges intelligencia kamerarendszer keretében történő használata – a fentebb kifejtettek és a törvényi rendelkezések alapján – egyértelműen biometrikus adatok, így különleges adatok kezelését eredményezi."[290]

Mi az a biometrikus sablon?

A biometrikus sablon az a számítógépes reprezentáció, amely az adott biometrikus adatot egy standardizált formában ábrázolja. A biometrikus sablonok matematikai algoritmusokat használnak az adatok összehasonlítására és az azonosítás vagy ellenőrzés céljából. A biometrikus adatokhoz képest a biometrikus sablonok általában kompaktabbak, mivel csak a lényeges információkat tartalmazzák, amelyek szükségesek az azonosításhoz vagy annak ellenőrzéséhez.

Összefoglalva, a biometrikus adat az eredeti mérhető jellemzők, míg a biometrikus sablon az ezeket az adatokat reprezentáló formátum vagy reprezentáció. A biometrikus sablonokat gyakran használják azonosítási és hitelesítési folyamatokban, mivel a kompaktabb formátum lehetővé teszi a hatékonyabb tárolást és összehasonlítást a biometrikus adatokkal.

Hogyan képzeljük el a biometrikus sablon előállítását és visszafejthetetlenségét? Mint amikor főzünk.

Példa

- ✓ *ha ugyanazon recept alapján ugyanazon alapanyagok és mennyiségek használatával ugyanolyan eljárást követve minden egyes alkalommal ugyanazt főzzük, akkor a végeredmény újra és újra ugyanaz lesz. Amennyiben a gulyáslevesbe mindent beleteszünk, amit bele kell tenni, felkockázott marhahúst, hagymát, paprikát, paradicsomot, sárgarépát, krumplit meg minden mást, amit csak a recept előír, pontosan betartva annak minden betűjét a végeredmény ugyanaz a gulyásleves lesz akárhányszor csak elkészítjük. A gulyásleves egy visszafordíthatatlan folyamat (a hámozás, aprítás, főzés, fűszerezés) lezárása lesz, azaz bármit is próbálunk csinálni a levesünkkel, azt nem változtathatjuk vissza nyers hússá, meg krumplivá és a sárgarépakarikák sem állnak össze újra egész répákká.*

A biometrikus sablon lényege ugyanaz, mint a főzésé.

Példa

- ✓ *az ujjlenyomatos azonosítás során a rendszer a leolvasónak megmutatott ujjlenyomat alapján egy alfanumerikus kódot generál. A rendszer magát az ujjlenyomatot (az ujjlenyomat képét) nem tárolja csak az alfanumerikus kódot és minden egyes alkalommal az újra és újra megmutatott ujjlenyomat alapján végzi el az azonosításhoz szükséges újrakódolást – ahogy a gulyásleves esetén mindig ugyanahhoz a gulyásleveshez jutunk. A*

[290] NAIH-963-10/2022. https://www.naih.hu/hatarozatok-vegzesek?download=495:biometrikus-adatkezeles-arcfelismero-kamerak-a-siofoki-kozteruleti-terfigyelo-rendszerben, utolsó letöltés: 2022. 07. 17.

végeredmény pedig? Ebből a kódból ugyanúgy nem lehet visszafejteni az eredeti ujjlenyomatot, mint ahogy a gulyáslevest sem lehet visszavarázsolni az eredeti alkotórészekké.

Hogyan lehet mégis egy alfanumerikus kódot visszafejteni? Ebben az esetben nem a visszafejtés a megoldás, hanem a próbálgatás, azaz sok-sok rendelkezésre álló ujjlenyomat kódolásával meg lehet találni azt az egyet, amelyikből a sablonnal megegyező alfanumerikus kód lesz – a megfejtés sebessége pedig attól függ, hogy milyen technológiát alkalmazunk (pl. mesterséges intelligencia) és mekkora szénakazalban (adatbázisban) keressük a tűt.

A biometrikus azonosítás

Az azonosítás („identifikáció") az egyén azonosításának folyamata egy csoporton belül, mely során az azonosítandó egyén adatait összehasonlítjuk a csoportban lévő összes egyén adataival.

A hitelesítés („authentikáció") az egyén által állított személyazonosság bizonyításának (valóságnak megfeleltetésének) folyamata, mely során az egyén adatait hasonlítjuk össze az állítólagos személyazonosság adataival.

***Az erős hitelesítési rendszer** legalább kettőt választ a következők közül:*

- ✓ *valami, amit tudunk (például jelszó),*
- ✓ *valami, amivel rendelkezünk (például hardware kulcs, beléptető kártya), illetve*
- ✓ *valami, ami mi vagyunk (biometrikus adat).*

Ezen követelmények alapján a csak biometrikus adaton alapuló hitelesítés gyengébb védelem, mint a beléptető kártya + jelszó használata. További hátránya a biometrikus azonosításnak, hogy amennyiben a „jelszavunk" (pl. hangunk, ujjlenyomatunk, íriszünk) kompromittálódik (ellopják), nem tudunk újat kérni/generálni.

A technika fejlődésével egyre többször használunk biometrikus adatokat egy adott személy azonosításához, illetve hitelesítéséhez (ujjnyomat, arckép, hangazonosítás stb.).

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

Észrevételek az ügyfelek számára adminisztratív terheket tartalmazó egyes kormányrendeletek módosításáról szóló rendelet tervezetéhez:
„Az aláírás-minta, mint biometrikus adat kezelésének bevezetését akkor tartom adatvédelmi szempontból támogathatónak, ha az aláírás-minta nem csak hitelesítéshez, hanem az érintett azonosításához is felhasználható lesz. E nélkül az a helyzet állna elő, hogy a kormányhivatal nyilvántartaná az aláírás-mintát is és egyéb személyazonosításra alkalmas adatokat is, miközben műszaki értelemben az aláírás-minta alkalmas lenne a személyazonosítás elvégzéséhez is, tehát az azonosításhoz az aláírás-mintán kívül más adat nyilvántartása nem lenne szükséges. Ez nem állna összhangban az Európai Unió általános adatvédelmi

rendelet 5. cikk (1) bekezdés c) pontjában rögzített adattakarékosság elvével sem, amely szerint a személyes adatok az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („adattakarékosság”).”[291]

A biometrikus azonosítás/hitelesítés jellegzetességei:

- ✓ a „sima” adathoz (például jelszóhoz, kulcshoz stb.) képest mindig többletinformációt hordoz az adott személyről,
- ✓ a pontossága nem éri el az olyan azonosítási/hitelesítési folyamatok pontosságát, mint ami például jelszót vagy egyéb hitelesítési folyamatot használ, így mindig megvan a hamis pozitív (fel nem hatalmazott személyt fogad el) illetve hamis negatív eredmény esélye (felhatalmazott személyt utasít el),
- ✓ a rokonsági kapcsolat megzavarhatja a biometrikus azonosítást/hitelesítést,
- ✓ nem alkalmas minden egyes ember azonosítására (például baleset, egészségi állapot, genetikai adottság miatt),
- ✓ a biometrikus azonosítást is ki lehet játszani,
- ✓ nem feltétlenül biztonságosabb és humánusabb, mint az egyéb azonosítási/hitelesítési módszerek, sőt időnként veszélyesebbek is az érintettek számára, illetve kompromittálódás (adatvédelmi incidens) esetén nem lehet megváltoztatni úgy, mint egy jelszót.

A biometrikus rendszerek működése sem 100 %-ban hibamentes, a hibák adódhatnak például környezeti viszonyokból (eltérő megvilágítás stb.) és a használt eszközök különbözőségéből is. Egy adott rendszer megbízhatóságát a leggyakrabban használt teljesítményértékelési mérőszámok segítségével mérhetjük fel:

- ✓ hibás elfogadási arány[292]: annak a valószínűsége, hogy a biometrikus rendszer tévesen azonosít valakit, vagy nem utasít el egy jogosulatlan felhasználót (hamis pozitív arány),
- ✓ hibás elutasítási arány[293]: annak a valószínűsége, hogy a rendszer hibás elutasítást végez, azaz jogosult felhasználót utasít el (hamis negatív arány).

A katalán adatvédelmi hatóság (APDCAT) gyakorlatából

Egy badalonai állami iskola olyan biometrikus azonosításra alkalmas rendszert telepített a diákok jelenlétének ellenőrzésére, amely a középiskola 1. évfolyamának arcvektorait gyűjtötte össze (csak ennél az évfolyamnál használták), kiegészítve az ikrek ujjlenyomatadataival tekintettel arra, hogy az arcuk azonos, de az ujjlenyomatuk különböző volt. A rendszerhez olyan adatfeldolgozót vettek igénybe, akivel nem kötöttek adatfeldolgozói megállapodást és az iskola azt sem tudta bizonyítani, hogy eleget tett a szülők tájékoztatáshoz való jogának.

[291] NAIH/2020/7549/2. sz. véleménye, 2020. október 30. https://naih.hu/files/NAIH-7549-2-2020-201030.pdf, utolsó letöltés 2022. 08. 19.
[292] False Accept Rate, FAR
[293] False Reject Rate, FRR

Az iskola a diákok szüleinek hozzájárulására hivatkozott, és amennyiben a szülő nem járult hozzá, a jelenléti adatokat nem ezen a rendszeren keresztül, hanem kézzel gyűjtötték össze.

Az APDCAT megállapította, hogy az iskola megsértette:

- ✓ *a GDPR 5. cikk (1) bekezdésének a) pontját, mivel úgy kezelte az adatokat, hogy volt kevésbé invazív lehetőség is (például a hagyományos ellenőrzési módok, amelyeket ez az iskola is alkalmazott)*
- ✓ *a GDPR 9. cikk (2) bekezdését, mert érvényes kivételre hivatkozás nélkül kezelt biometrikus adatokat*
- ✓ *a GDPR 13. cikkét, mivel nem tájékoztatta megfelelően a szülőket az adatok kezeléséről*
- ✓ *a GDPR 28. cikkét, mivel nem kötöttek adatfeldolgozási megállapodást az adatfeldolgozóval.*

Az iskola azonnal felhagyott a rendszer használatával, amikor az APDCAT vizsgálatot indított, ezért a hatóság csak figyelmeztetésben részesítette.[294]

Biometrikus adat a munkahelyen és egyéb helyeken

Napjainkban a biometrikus adatok gyűjtése és felhasználása az egyik legingoványosabb terület az adatvédelem területén, elég csak az arcfelismerésen alapuló rendszerek körüli vitákra és indulatokra gondolnunk. Éppen ezért például a GDPR e téren enged bizonyos nemzeti eltéréseket, például tagállami szinten ezen adatok kezelésének részleges vagy teljes tiltását.

Miért van szükség ilyen megszorításokra? Mert a biometrikus adatok kezelése mélyen behatol a természetes személyek privát szférájába, ráadásul gyakran olyan módon, hogy arra (azaz az adott adatkezelésre) nem is számítanak az érintettek.

Milyen főbb követelményeknek kell megfelelnünk, ha biometrikus adatokkal kapcsolatos adatkezelést kívánunk folytatni?

Meg kell vizsgálnunk, hogy az adatkezelésünk célja alapján a kezelt adatok minden kategóriája arányos-e. Biometrikus adatokat csak akkor kezelhetünk, ha megfelelőek, relevánsak és nem túlzott mértékűek, és azt is értékelnünk kell, hogy a kezelt adatok szükségesek és arányosak-e, valamint azt, hogy a kitűzött célunkat elérhetnénk-e kisebb beavatkozással járó módon is. Még az adatkezelésünk megkezdése előtt mérlegelnünk kell tehát, hogy

- ✓ a rendszer szükséges-e az adott igényünk kielégítéséhez, azaz használata elengedhetetlen-e, vagy inkább csak a legkényelmesebb, vagy legköltséghatékonyabb utat választottuk,
- ✓ a rendszerünk elég hatékony lesz-e az adott igényünk kielégítése terén, tekintettel a bevezetni kívánt biometrikus technológia sajátos jellemzőire (például a várható hibák aránya),

[294] APDCAT (Catalonia) – PS 49/2019, https://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Resolucions/Documents/ca_ps_2019_049.pdf, utolsó letöltés: 2022. 07. 25.

- ✓ arányos-e az elvárt előnyökkel, ha a rendszerünk miatt sérül az érintettek magánéletének védelme,
- ✓ az általunk elérni kívánt cél elérhető-e az érintettek magánéletébe kisebb mértékben beavatkozó módszerekkel.

Előfordulhat az is, hogy bizonyos személyek nem alkalmasak a mi általunk tervezett biometrikus rendszerben arra, hogy érintettek legyenek, vagy megalázó számukra a rendszer használata (például beszédhibás személy hangalapú azonosításon alapuló rendszer használata esetén), éppen ezért megfelelő tartalékeljárásokra lehet szükségünk annak érdekében, hogy meg tudjuk oldani az adatfelvételi folyamatot sikeresen elvégezni nem tudó egyének az emberi méltóságának és jogainak valamint szabadságainak tiszteletben tartását, azaz ne frusztráljuk őket feleslegesen a mi rendszerünk technikai „tökéletlensége" miatt.

Példák

- ✓ *a technológia még kiforratlan és több kárt okoz a használata, mint hasznot. Mert mire jó az olyan arcfelismerő program, amely bizonyos érintetti kör (nők, színes bőrű érintettek) esetében 90%-os hibahatárral dolgozik? Nem sok mindenre,*
- ✓ *az adatkezelő kiszolgáltatott réteg, például a munkavállalók biometrikus adatait kívánja kezelni azonosítás vagy egyéb megkülönböztetés céljából. Van olyan multinacionális cég, amelynek távol-keleti gyárában olyan arcfelismerő rendszer működik, amelyik csak azt a munkavállalót engedi be a munkaterületre, aki a kamerába mosolyog.*

Hazai példák a biometrikus azonosításra

- ✓ *A Munka törvénykönyve alapján a munkáltató a munkavállalók azonosítása céljából biometrikus adatot csak akkor kezelhet, ha ez valamely dologhoz vagy adathoz történő olyan jogosulatlan hozzáférés megakadályozásához szükséges, amely*
  - *a) a munkavállaló vagy mások élete, testi épsége vagy egészsége, vagy*
  - *b) törvényben védett jelentős érdek*

  súlyos vagy tömeges, visszafordíthatatlan sérelmének a veszélyével járna. Mi lehet ez a jelentős védett érdek? A jogalkotó taxatív felsorolása alapján jelentős védett érdek különösen
  - *a) a legalább „Bizalmas!" minősítési szintű minősített adatok védelméhez,*
  - *b) a lőfegyver, lőszer, robbanóanyag őrzéséhez,*
  - *c) a mérgező vagy veszélyes vegyi vagy biológiai anyagok őrzéséhez,*
  - *d) a nukleáris anyagok őrzéséhez,*
  - *e) a Büntető törvénykönyv szerint legalább különösen nagy vagyoni érték (minimum ötvenmillió-egy forintnyi érték) védelméhez*

  fűződő érdek.
- ✓ *A sporttörvény akkor engedi a biometrikus adatok kezelését, ha az adatkezelés célja a sportrendezvények biztonságának garantálhatóságának elősegítése – senki sem lepődhet meg ha egy bajnoki*

focimeccsre csak úgy mehet be, ha előtte alávetette magát a vénaszkenneres adatkezelésnek.

- ✓ *Az E-ügyintézés tv.*[295] *is lehetőséget ad a videótechnológiával történő azonosításra.*

Bűnügyi adatok kezelése

A bűnügyi személyes adatok kezelése kiemelten fontos lehet az adatkezelők számára.

Példák

- ✓ *miért is engednénk például olyan személyt a bankszámlánk vagy a pénztárunk közelébe, akit már többször elítéltek lopásért/sikkasztásért?*
- ✓ *adminisztrátornak sem alkalmaznánk szívesen olyan munkavállalót, akit rajta kaptak már közokirat- vagy pénzhamisításon.*
- ✓ *elkerülhetetlen a bűnügyi adat kezelése, ha a munkavállaló ittasan, másnak kárt, netalán sérülést okoz a céges gépjárművel.*

A bűnügyi személyes adatok kezelése esetén – ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusa ettől eltérően nem rendelkezik – a különleges adatok kezelésének feltételeire vonatkozó szabályokat kell alkalmaznunk.[296]

Példák

- ✓ *a Munka Törvénykönyve a tizennyolcadik életévét be nem töltött személy nevelését, felügyeletét, gondozását, gyógykezelését végző, illetve tizennyolcadik életévét be nem töltött személy részére szabadidővel, szórakozással, sportolással összefüggő szolgáltatást nyújtó munkáltató esetében meghatározza, hogy a munkáltató kit nem alkalmazhat „előélete" miatt. Azt a tényt, hogy megfelel az „előéleti" követelményeknek,*
  - *a) munkaviszonyt létesíteni kívánó személy a munkaviszony létrejötte előtt, vagy*
  - *b) munkavállaló a munkaviszony fennállása alatt a munkáltató írásbeli felhívására, a felhívástól számított tizenöt munkanapon belül, ha e határidőn belül a munkavállalón kívül álló ok miatt nem lehetséges, az ok megszűnését követően haladéktalanul*

  hatósági bizonyítvánnyal igazolja. (Mt. 44/A.§)
- ✓ *A Munka törvénykönyve alapján a munkáltató a munkavállaló vagy a munkáltatóval munkaviszonyt létesíteni szándékozó személy bűnügyi adatát annak vizsgálata céljából kezelheti, hogy törvény vagy jogszabályi felhatalmazás alapján a munkáltató a betölteni kívánt vagy a betöltött munkakörben nem korlátozza vagy nem zárja-e ki a foglalkoztatást.*
  A munkáltató korlátozó vagy kizáró feltételt akkor határozhat meg, ha az adott munkakörben a foglalkoztatás
  - *a) a munkáltató jelentős vagyoni érdeke,*
  - *b) törvény által védett titok, vagy*

[295] az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény
[296] Infotv. 5.§ (7) bekezdés

c) a törvény által védett érdek (a lőfegyver, lőszer, robbanóanyag őrzése, a mérgező vagy veszélyes vegyi vagy biológiai anyagok őrzése, illetve a nukleáris anyagok őrzése) sérelmének veszélyével járna.

A munkáltatónak a bűnügyi személyes adat kezelését megalapozó korlátozó vagy kizáró feltételt és a bűnügyi személyes adat kezelésének feltételeit előzetesen írásban meg kell határoznia, tehát nem rendelheti el azt visszamenőlegesen vagy éppen hasra ütés alapon.

MILYEN FELTÉTELEKKEL KEZELHETÜNK KÜLÖNLEGES SZEMÉLYES ADATOKAT?

Különleges adatok kezelése esetén először is be kell azonosítanunk azt, hogy melyek a különleges adatok kategóriájában tartozó adatok az általunk kezelt adatok közül. Van, amikor ez egyszerű, ám némely esetben azért nem annyira egyértelmű, hogy fokozottan védendő személyes adattal van-e dolgunk, illetve az adatkezelés során nem mindig számítunk arra, hogy különleges adat kerülhet a birtokunkba.

Példa

- ✓ *A biztonsági szolgálat a kapuban mindenki szeme láttára ellenőrzi az alkalmazott táskáját és abból olyan valami kerül elő, ami az adott személy nagy nyilvánosság előtt hangosan hirdetett világnézeti meggyőződésének az ellenkezőjét tanúsítja. Ráadásul ennek az adatnak a napvilágra kerülése akár megbélyegzést és kiközösítést is eredményezhet.*
- ✓ *Kényelmetlen lehet az alkalmazott számára, ha a táskájából az ellenőrzés során olyan valami kerül elő, ami a szexuális életével vagy irányultságával kapcsolatos, különösen, ha az ellenőrzés szemtanúi között olyan személy is van, aki esetében bizton számíthat az adott személy arra, hogy a látottakat elpletykálja az ő párjának, szüleinek vagy bárki olyannak (pl. gyülekezet tagjának, gyermeke osztályfőnökének, kocsmahaveroknak stb.), aki előtt életének ezen részét nagyon nem szeretné felfedni.*

Éppen ezért a táskaellenőrzés az egyik legjobban a privát szféránkba hatoló adatkezelés, hiszen az ellenőrzött személy legféltettebb titkai (azaz különleges adatai) is ott lapulhatnak a pakkja alján.

Különleges adatot adatkezelőként csak abban az esetben kezelhetünk, ha a GDPR 9. cikkének (2) bekezdésében felsorolt lehetőségek egyikére tudunk hivatkozni. Azaz nem elegendő az, hogy blöffölünk egy nagyot, miszerint a c) pontban megfogalmazott feltétel (kivétel) tuti megfelelő az adott helyzetben, ezt alá is kell támasztanunk.

Különleges adatok kezelése esetén az alábbi tíz feltétel egyikét kell tudnunk teljesíteni:

- ✓ az érintett kifejezett hozzájárulását adta a különleges személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha uniós vagy tagállami jogszabály úgy rendelkezik, hogy a kezelési tilalom nem oldható fel az érintett hozzájárulásával *[GDPR 9. cikk (2) bekezdés a) pont]*

Példa

- ✓ *csapatépítő tréninget szervezünk, ahol közös ebédet és vacsorát is tervezünk, ehhez pedig meg szeretnénk kérdezni, kinek van szüksége különleges ételre (pl. allergia miatt stb.)*
- ✓ *az iskola tanárijában szeretnénk kitenni a súlyosan allergiás gyermekek fényképeit, hogy bármelyik tanár gyorsan tudjon intézkedni, ha allergiás rohama lenne az adott diákoknak, és ehhez a közzétételhez a szülők hozzájárulását kérjük*

- ✓ az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi. *[GDPR 9. cikk (2) bekezdés b) pont]*

Példa
- ✓ *adatkezelőként erre a feltételre hivatkozva ellenőrizhetjük a munkavállalóink körében a munkavégzésre alkalmas állapotot (azaz szondáztathatunk) és kezelhetjük a befolyásoltság mértékére vonatkozó (egészségügyi) adatot*
- ✓ *járvány idején ezen feltételre hivatkozva tarthatjuk nyilván a munkavállalók védettségi adatait annak érdekében, hogy a munkavállalók számára biztosítani tudjuk az egészséges és biztonságos munkavégzési körülményeket*

- ✓ az adatkezelés az érintettnek vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni *[GDPR 9. cikk (2) bekezdés c) pont]*

Példa
- ✓ *a bank ügyfélterében rosszul lesz egy ügyfél és segítséget hívunk hozzá. A diszpécser kérdéseire válaszolva elmondjuk, hogy milyen tünetei vannak a személynek, mivel ezzel tudjuk segíteni azt, hogy a lehető legoptimálisabb segítséget kapja (pl. milyen mentőt küldjenek hozzá és milyen gyorsan stb.).*

- ✓ az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára. *[GDPR 9. cikk (2) bekezdés d) pont]*

Példa
- ✓ *egy gyülekezet kezelheti a tagjai adatait*
- ✓ *a laposföld hívők egyesülete regisztrálhatja a tagjait világnézetük alapján (a Föld valójában egy tányér, amelyet egy teknős visz a hátán stb.)*

- ✓ az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott. *[GDPR 9. cikk (2) bekezdés e) pont]*

Példa

- ✓ *amennyiben a tánccsoport német/román nemzetiségi tánccsoportként jelentkezik be egy fesztiválra, akkor a tánccsoport tagjaira mindenki úgy fog tekinteni, mint német/román nemzetiségű személyre*
- ✓ *egy interjúban egy közszereplő elmondja, hogy református családban született és a múlt évben azért volt beteg mert szívinfarktusa volt, de már jól van és újra dolgozik*
- ✓ *egy rendezvényen egy színész „coming out"-ol és erről egy újság tudósít*

Fontos, hogy a nyilvánosságra hozás magától az érintettől származzon (ne pedig harmadik féltől), illetve ne véletlenül vagy tévedésből kerüljön ki az adat a nyilvánosság elé.

Annak ténye, hogy az érintett nyilvánosságra hozta a különleges személyes adatát még nem mentesít minket a GDPR-ban foglalt kötelezettségünk alól, így például a célhoz kötöttség és adattakarékosság elve vonatkozik azokra a személyes adatokra is, amelyeket nyilvánosan hozzáférhetővé tett az érintett.

Példa

- ✓ *azért mert valaki elmondta, hogy hívő keresztény még nem küldözgethetünk neki zarándok utakról szóló ajánlatot utazási irodánk nevében*

- ✓ az adatkezelés jogi igények megállapításához, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el, *[GDPR 9. cikk (2) bekezdés f) pont]*

Példa

- ✓ *munkáltatóként kezelhetjük a munkavállalónk munkahelyi balesetével kapcsolatos sérülésadatait annak érdekében, hogy bíróság előtt bizonyítsuk, hogy nem a mi hibánk, hogy munkahelyi balesetben tartós egészségkárosodást szenvedett*

A dán adatvédelmi hatóság (Datatilsynet) gyakorlatából:

A dán adatvédelmi hatóság megállapította, hogy a TV 2 egy belső vizsgálat során jogalap nélkül kezelt különleges adatokat egy alkalmazottjával szembeni szexuális visszaéléssel kapcsolatos vádakkal szemben.

A TV 2 2020 szeptemberében vizsgálatot indított a TV állomáson belüli egészségtelen (szexista) kultúra miatt, melybe bevonta a Norrbom Vinding ügyvédi irodát és arra kérte a korábbi és jelenlegi alkalmazottakat, hogy jelentsék a jogsértéseket, valamint osszák meg a TV 2-nél tapasztalható szexista kultúrával kapcsolatos tapasztalataikat. Két bejelentés érkezett, és az ügy kivizsgálása után a TV 2 úgy döntött, hogy az érintett nem lehet többé műsorvezető a csatornánál.

Az érintett azzal érvelt, hogy nem voltak olyan konkrét tények, amelyek a TV 2 vizsgálatát indokolták volna, illetve ő nem járult hozzá kifejezetten semmilyen adatkezeléshez, ezért a TV 2 és a Norrbom Vinding jogalap nélkül kezelte a különleges személyes adatait.

Az adatvédelmi hatóság véleménye szerint

- ✓ *a TV 2 és a Norrbom Vinding nem hivatkozhatott az adatkezelőre vonatkozó jogi kötelezettségre az érintettek személyes adatainak kezelése során, mivel a vonatkozó törvényben meghatározott jogi kötelezettségek nem eléggé egyértelműek és pontosak ahhoz, hogy a GDPR 6. cikk (1) bekezdésének c) pontja szerinti adatkezelés alapjául szolgáljanak. Azonban az adatkezelők hivatkozhatnak a jogos érdekre, mint jogalapra, mivel a vizsgálat célja, „az egészségtelen kultúra megszüntetése" jogos volt, és ez a cél felülírta az érintett érdekeit.*
- ✓ *az adatkezelők nem hivatkozhattak a GDPR 9. cikk (2) bekezdésének b) pontjában meghatározott kivételre, mivel a vonatkozó törvényben meghatározott jogi kötelezettségek nem eléggé egyértelműek és pontosak. Továbbá nem hivatkozhattak a GDPR 9. cikk (1) bekezdésének f) pontjára sem, mivel a különleges adatok gyűjtése nem volt kellően korlátozott, és olyan személyekre is vonatkozott, akik már nem dolgoztak az állomáson, azaz e személyekre vonatkozó különleges adatok kezelése nem volt szükséges a jogi igény (például munkaügyi vagy szerződéses szankció) érvényesítéséhez. Ezért a hatóság arra a következtetésre jutott, hogy a TV 2 és a Norrbom Vinding jogalap nélkül kezelte az érintett különleges személyes adatait.*[297]

- ✓ az adatkezelés jelentős közérdek miatt szükséges, uniós vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő, *[GDPR 9. cikk (2) bekezdés g) pont]*

A francia bírósági gyakorlatból

A marseille-i közigazgatási bíróság megszüntettette két középiskolában indított arcfelismerő rendszer tesztelést, mert a tizenévesek biometrikus adatait jogalap nélkül kezelték.

Provence-Alpes-Côte d'Azur francia régió (PACA régió) engedélyezte egy új, arcfelismerő technológiát használó beléptető rendszer kísérleti alkalmazását két középiskolában, melynek a célja a biztonság ellenőrzése és garantálása volt. Négy egyesület megtámadta a határozat jogszerűségét a közigazgatási bíróság előtt.

[297] Alvorlig kritik af TV 2 og Norrbom Vinding, Journalnummer: 2021-31-4751, https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/feb/alvorlig-kritik-af-tv-2-og-norrbom-vinding, utolsó letöltés: 2022. 08. 23.

A bíróság megállapította, hogy a tesztelést engedélyező határozat jogellenes volt:

- ✓ *az arcfelismerő rendszer a kiskorúak biometrikus adatait önkéntes és tájékozott hozzájárulás nélkül kezelte;*
- ✓ *a vitatott határozatban említett, az iskolák beléptetésével és biztonságával kapcsolatos adatkezelési célok nem tartozhatnak a GDPR 9. cikk (2) bekezdésének g) pontja alá, ezért a bíróság megsemmisítette azt a határozatot, amely engedélyezte a beléptető rendszer tesztelését a két középiskolában.*[298]

- ✓ az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében (plusz követelmény: a szakember titoktartási kötelezettség alatt áll) *[GDPR 9. cikk (2) bekezdés h) pont]*

A görög adatvédelmi hatóság (HDPA) gyakorlatából

Egy idősek otthonában dolgozó munkavállaló panaszt nyújtott be a HDPA-hoz, mivel az otthonban felszerelt kamerák tolakodó módon filmezték a helyiségeket, beleértve az alkalmazottakat és a lakókat is.

A hatóság megállapította, hogy

- ✓ *az adatkezelő megsértette a GDPR 9. cikk (2) bekezdésének h) pontját, mely szerint a különleges adatok kezelése akkor megengedett, ha az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges. Az ilyen típusú adatkezelés megkezdése előtt azonban az adatkezelőnek engedélyt kell kapnia, jelen esetben az illetékes orvosi és ápolói személyzetből álló bizottság határozatának formájában. Az idősotthon a bizottság előzetes jóváhagyása nélkül szerelte fel a kamerákat;*
- ✓ *a kamerák telepítésére és működtetésére a munkavállalók előzetes írásbeli vagy elektronikus formában történő tájékoztatása nélkül került sor, és hogy az érintettek korlátozott tájékoztatása nem felelt meg a GDPR 13. cikkében foglalt követelményeknek (a tájékoztatás túl általános volt, illetve a megadott adatkezelési cél nem kapcsolódott egyértelműen a hivatkozott jogalaphoz és az adatok kategóriáihoz, azaz az adatok különleges kategóriáihoz);*

[298] TRIBUNAL ADMINISTRATIF DE MARSEILLE, N° 1901249, https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf, utolsó letöltés: 2022. 08. 23.

- ✓ *az idősotthon megsértette az adattakarékosság elvét, mivel a munkavállalók mozgását és helyzetét rögzítették;*
- ✓ *az idősotthon ugyan végzett megfelelő adatvédelmi hatásvizsgálatot, azonban annak megállapításaival nem foglalkozott megfelelően.*

A HDPA utasította az idősotthont, hogy

- ✓ *állítsa át a konyhákban felszerelt kamerákat úgy, hogy azok kizárólag a be- és kijárati területekre fókuszáljanak, valamint*
- ✓ *semmisítse meg a már rögzített felvételeket.*[299]

✓ az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechnikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan *[GDPR 9. cikk (2) bekezdés i) pont]*

Példa

- ✓ *az adatkezelésre az egészségügyi ellátás biztosításához szükséges a COVID-19 betegséget túlélő személyek bevonásával végzett kutatás miatt kerül sor (Szlovénia)*[300]
- ✓ *a COVID-19 járvány során az iskolákban a be nem oltott tanulóknak a tesztről szóló igazolás bemutatására vagy helyszíni tesztelésre való kötelezése (Németország)*[301].

✓ az adatkezelés a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő. *[GDPR 9. cikk (2) bekezdés j) pont]*

Az olasz adatvédelmi hatóság (Garante per la protezione dei dati personali) gyakorlatából

Az olasz adatvédelmi hatóság megítélése szerint, az egészségügyi adatok tudományos célú feldolgozása kifejezett hozzájárulás nélkül is elvégezhető, ha az adatgyűjtés aránytalan erőfeszítéssel járna, vagy az kutatási célokat sértené [GDPR 9. cikk (2) bekezdés j) pontja alapján]

[299] ΑΠΟΦΑΣΗ 41/2021, https://www.dpa.gr/sites/default/files/2021-09/41_2021anonym.pdf, utolsó letöltés: 2022. 08. 23.
[300] IP - 07120-1/2020/358. https://www.ip-rs.si/mnenja-gdpr/6048a57a33a11
[301] VGH München - BeckRS 2021, 36742. https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2021-N-36742?hl=true

Az adatkezelő (egy kórház) célja a COVID-19 korlátozások és a gyermekek mentális betegségeinek számának emelkedése közötti összefüggés vizsgálata volt, melyhez több ezer beteg gyermek egészségügyi adatait kellett összegyűjtenie. Az adatkezelés megkezdése előtt a kórház adatvédelmi hatásvizsgálatot végzett, melynek során arra a megállapításra jutott, hogy a gyermekek és családtagjaik hozzájárulásának begyűjtése aránytalanul nagy erőfeszítést jelentene a kórház számára, illetve ez a művelet veszélyeztetné a tudományos kutatás érvényességét is. A kórház szerint a hozzájárulás begyűjtése elkerülhetetlenül szelekciós torzítást eredményezne, mivel csak a jobb társadalmi-gazdasági háttérrel rendelkező családok adnának beleegyezést, mivel ők tudnak néhány órát szánni arra, hogy elmenjenek a kórházba és aláírják a dokumentumokat.

Az adatvédelmi hatóság helyt adott a kórház érvelésének, miszerint a hozzájárulás kérése ebben az esetben aránytalan erőfeszítést jelentene, azonban irrelevánsnak tekintették azt a tényt, hogy a hozzájárulás begyűjtése megváltoztathatná a kutatás eredményeit, mivel a hatóság véleménye szerint a hozzájárulás mindig szelekciós torzítást eredményez a tudományos kutatásban.[302]

Bűnügyi adatok kezelése

A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatoknak a GDPR 6. cikk (1) bekezdése alapján történő kezelésére kizárólag abban az esetben kerülhet sor, ha az közhatalmi szerv felügyelete alatt történik, vagy ha az adatkezelést az érintett jogai és szabadságai tekintetében megfelelő garanciákat nyújtó uniós vagy tagállami jog lehetővé teszi. A büntetőjogi felelősség megállapítására vonatkozó határozatok teljes körű nyilvántartása csak közhatalmi szerv által végzett adatkezelés keretében történhet.[303]

Bűnügyi személyes adatok kezelése esetén – ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusa ettől eltérően nem rendelkezik – a különleges adatok kezelésének feltételeire vonatkozó szabályokat kell alkalmazni.[304]

A fentiek alapján tehát miután a GDPR 9. cikk (2) bekezdése alapján a kezelhetőséghez szükséges feltételt beazonosítottuk, akkor – visszatérve az egyébként szokásos ügymenetünkhöz – választanunk kell egyet a GDPR 6. cikk (1) bekezdésben található jogszerűséghez szükséges jogalapok közül és rendelkeznünk kell a szükséges dokumentumokkal, illetve garanciákkal (pl. jogszabályi hivatkozás, szerződés, érdekmérlegelési teszt stb.).

[302] Garante per la protezione dei dati personali (Italy) – 9875254. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9875254
[303] GDPR 10. cikk
[304] Infotv. 5.§ (7) bek.

Amennyiben úgy döntünk, hogy az Európa Unión kívülre továbbítjuk az adatok különleges kategóriájába eső adatokat, bajlódnunk kell a plusz garanciákkal és biztosítékokkal is (lásd nemzetközi adattovábbítás).

A különleges adatok kezelése gyakran extra kockázatot és ebből eredően extra feladatokat is jelenthet az adatkezelők számára, például

- ✓ *kötelesek lehetünk DPO kinevezésére (ha egyébként nem lennénk rá kötelesek);*
- ✓ *szükségünk lehet az adatkezelésünk megkezdése előtt adatvédelmi hatásvizsgálatra;*
- ✓ *amennyiben adatvédelmi incidens történik és az érinti a különleges adatot is, az incidenst nagy valószínűséggel be kell jelentenünk az illetékes hatóságnak (azaz nem sorolhatjuk bejelentésmentes kategóriába az incidenst) és a legtöbb esetben az érintetteket is értesítenünk kell a baj megtörténtéről.*

ADATTÍPUSOK III.: EGYÉB ADATOK

Közérdekű és közérdekből nyilvános adatok

„Magyarország Alaptörvényének VI. cikk (3) bekezdése kimondja, hogy mindenkinek joga van a közérdekű adatok megismeréséhez és terjesztéséhez. Az információszabadság elsődleges rendeltetése az állam, a közpénzek felhasználásának átláthatósága."[305]

Az Infotv. alapján a közfeladatot ellátó szerveknek lehetővé kell tenniük, hogy a kezelésükben lévő közérdekű adatot és közérdekből nyilvános adatot – az Infotv-ben meghatározott kivételekkel – erre irányuló igény alapján bárki megismerhesse.

A **közérdekű adat**[306]

- ✓ az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy,
- ✓ kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett,
- ✓ a személyes adat fogalma alá nem eső,
- ✓ bármilyen módon vagy formában rögzített információ vagy ismeret,
- ✓ függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől,
- ✓ így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

A közérdekű adat nem lehet személyes adat.

A **közérdekből nyilvános adat**[307]

- ✓ a közérdekű adat fogalma alá nem tartozó minden olyan adat,
- ✓ amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét,
- ✓ törvény közérdekből elrendeli.

A közérdekből nyilvános adat tehát olyan személyes adat, melyet törvény nyilvánított közérdekből nyilvánosnak, nyilvánosságra hozatala esetén pedig az adatvédelmi szabályoknak is meg kell felelni.

[305] NAIH: Tájékoztató a modellváltó egyetemek közérdekű adatokkal kapcsolatos kötelezettségei tárgyában, Budapest, 2022. január 21. https://naih.hu/dontesek-informacioszabadsag-tajekoztatok-kozlemenyek?download=481:tajekoztato-a-modellvalto-egyetemek-kozerdeku-adatokkal-kapcsolatos-kotelezettsegei-targyaban
[306] Infotv. 3.§ 5. pont
[307] Infotv. 3.§ 6. pont

Az Alkotmánybíróság gyakorlatából

„Az Alkotmánybíróság állandó gyakorlata, hogy a demokratikus államélet és közvélemény érdekében az állami tisztségviselők és más közszereplő politikusok alkotmányosan védett magánszférája másokénál szűkebb; különösen ki kell tenniük magukat mások kritikájának [legutóbb 36/1994. (VI. 24.) AB határozat, ABK 1994. június, 277.]. Ehhez azonban személyes adataik ismeretére is szükség lehet, amennyiben azok funkciójukkal vagy közszereplésükkel összefüggenek. A közhatalmat gyakorlók vagy a politikai közszereplést vállalók esetében a személyeknek – különösen a választópolgároknak – a közérdekű adatok megismeréséhez fűződő joga elsőbbséget élvez az előbbiek olyan személyes adatainak védelméhez képest, amelyek köztevékenységük és annak megítélése szempontjából jelentősek lehetnek.

Az e körbe eső személyes adatok megismerhetőségére nem csupán az állami és a politikai közélet informált megvitatása érdekében van szükség, hanem az állami szervek helyes megítéléséhez és a működésükbe vetett bizalom megalapozásához is.”[308]

A közérdekű és közérdekből nyilvános adatokkal kapcsolatban az Infotv. tartalmaz részletes rendelkezéseket. Külön kiemelendőek a környezeti adatok, ezekkel kapcsolatban az aarhusi egyezményben foglaltak az irányadóak.[309]

Minősített adatok

A minősített adatokkal kapcsolatos alapelvek:

- ✓ **szükségesség és arányosság elve:** a közérdekű adat nyilvánosságához fűződő jogot minősítéssel korlátozni csak a minősített adatokra vonatkozó törvényben[310] meghatározott feltételek fennállása esetén, a védelemhez szükséges minősítési szinttel és a feltétlenül szükséges ideig lehet
- ✓ **szükséges ismeret elve**: minősített adatot csak az ismerhet meg, akinek az állami vagy közfeladata ellátásához feltétlenül szükséges
- ✓ **bizalmasság elve**: minősített adat illetéktelen személy számára nem válhat hozzáférhetővé vagy megismerhetővé
- ✓ **sérthetetlenség elve**: a minősített adatot kizárólag az arra jogosult személy módosíthatja vagy semmisítheti meg
- ✓ **rendelkezésre állás elve**: annak biztosítása, hogy a minősített adat az arra jogosult személy számára szükség szerint elérhető és felhasználható legyen.

[308] 60/1994. (XII. 24.) AB határozat, https://www.abtl.hu/jogsz_ab_hatarozat_60_1994, utolsó letöltés: 2022. 08. 20.
[309] a környezeti ügyekben az információhoz való hozzáférésről, a nyilvánosságnak a döntéshozatalban történő részvételéről és az igazságszolgáltatáshoz való jog biztosításáról szóló, Aarhusban, 1998. június 25-én elfogadott Egyezmény kihirdetéséről szóló 2001. évi LXXXI. törvény
[310] a minősített adat védelméről szóló 2009. évi CLV. törvény (Mavtv.)

Nemzeti minősített adat[311]

A *minősítéssel védhető közérdek*ek körébe tartozó,

- ✓ a minősítési jelölést az e törvényben, valamint Mavtv. felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat,
- ✓ amelyről – a megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy
- ✓ az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele
- ✓ a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja),
- ✓ és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza.

Külföldi minősített adat[312]:

a) A megjelenési formájától függetlenül az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza,

b) a Magyar Honvédség nemzetközi műveletei és gyakorlatai keretében keletkezett, illetve felhasznált olyan adat, amelyhez történő hozzáférést a műveletben résztvevő felek – a művelet vagy gyakorlat követelményei szerinti minősítéssel – korlátozzák, attól függetlenül, hogy a részes felek által képviselt államokkal Magyarországnak van-e az a) alpontban foglaltaknak megfelelő megállapodása a minősített adat védelmére és cseréjére, és a minősített adat kezelésére vonatkozó rendelkezéseket a Magyar Honvédség, illetve a műveletet vagy a gyakorlatot irányító más részes fél határozza meg.

Minősítéssel védhető közérdek

Minősítéssel védhető közérdek Magyarország

a) szuverenitása, területi integritása,
b) alkotmányos rendje,
c) honvédelmi, nemzetbiztonsági, bűnüldözési és bűnmegelőzési tevékenysége,
d) igazságszolgáltatási, központi pénzügyi, gazdasági tevékenysége,
e) külügyi vagy nemzetközi kapcsolatai,
f) állami szerve illetéktelen külső befolyástól mentes, zavartalan működésének biztosítása.

Az adat minősítéssel csak akkor védhető, ha

[311] Mavtv. 3.§ (1) bekezdés a) pont
[312] Mavtv. 3.§ (1) bekezdés b) pont

a) a keletkezett adat minősítéssel védhető közérdekek körébe tartozik,
b) az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele károsítja a minősítéssel védhető közérdeket, és
c) az adat nyilvánosságát és arra feljogosított személyen kívüli megismerhetőségét meghatározott ideig korlátozni szükséges.

Amennyiben az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele
a) rendkívül súlyosan károsítja a minősítéssel védhető közérdeket, akkor „Szigorúan titkos!" (érvényességi idő legfeljebb 30 év)
b) súlyosan károsítja a minősítéssel védhető közérdeket, akkor „Titkos!" (érvényességi idő legfeljebb 30 év)
c) károsítja a minősítéssel védhető közérdeket, akkor „Bizalmas!" (érvényességi idő legfeljebb 20 év)
d) hátrányosan érinti a minősítéssel védhető közérdeket, akkor „Korlátozott terjesztésű! (érvényességi idő legfeljebb 10 év) minősítési szintű.

A minősítési szint meghatározásához szükséges kármérték[313]

1. **Rendkívül súlyos kárnak minősül és „Szigorúan titkos!" minősítési szint alkalmazása indokolt**, ha az adat érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele közvetlenül és tartósan sérti vagy veszélyezteti Magyarország szuverenitását, területi integritását, törvényes rendjét, belső stabilitását. Visszafordíthatatlanul jelentős károkat okoz az ország honvédelmi, nemzetbiztonsági, bűnüldözési, igazságszolgáltatási, központi pénzügyi és gazdasági érdekeiben, külügyi és nemzetközi kapcsolataiban, a szövetséges tagállamokkal közös biztonsági érdekeiben.
Rendkívül súlyosnak minősülhet a kár akkor is, ha annak elkerülhetetlen enyhítése nagyszámú emberi élet közvetlen veszélyeztetésével, vagy az ország gazdasági helyzetének egészére hátrányosan kiható ellenintézkedésekkel érhető el.
Rendkívül súlyos a kár többek között, ha tartósan gyengíti az ország honvédelmi képességeit, különösen a hadműveleti tervek és fegyverrendszerek hatékonyságát, jelentősen gyengíti az ország hírszerző és elhárító képességeinek folyamatos hatékonyságát, felfedi a nemzeti rejtjeltevékenység titkosítási rendszereit, nagyszámú embert érintő közvetlen életveszéllyel jár, jelentősen veszélyezteti a nemzetközi biztonságot, előmozdítja a nukleáris, vegyi és biológiai fegyverek elterjedését, lényegesen veszélyezteti a nukleáris és vegyi létesítmények biztonsági rendszereit.

2. **Súlyos kárnak minősül és „Titkos!" minősítési szint alkalmazása indokolt**, ha az adat érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére

[313] Mavtv. 1. számú melléklet

hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele által az 1. pontban okozott sérelem nem küszöbölhető ki, de enyhíthető, továbbá, ha ellehetetleníti vagy lényegesen akadályozza az állami vagy közfeladatot ellátó szerv rendeltetésszerű működését és ezáltal közvetlenül Magyarország törvényben meghatározott érdekeit sérti, az állampolgárok biztonságának és alkotmányos jogainak komoly sérelmével jár, közvetlen életveszélyt okoz, jelentősen hátráltatja a honvédelmi és nemzetbiztonsági tevékenység folyamatos hatékonyságát, feszültséget okoz Magyarország más országokkal fennálló kapcsolataiban, a szövetséges tagállamokkal közös biztonsági érdekeiben, Magyarország pénzügyi és gazdasági érdekeinek sérelmével számottevő vagyoni kárt okoz.

3. **Kárnak minősül és „Bizalmas!" minősítési szint alkalmazása indokolt**, ha az adat érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele okozta érdeksérelem vagy veszélyeztetés ellenintézkedésekkel lényegesen enyhíthető, és az nem jár jelentős anyagi, pénzügyi ráfordításokkal. Továbbá, ha az állam érdekérvényesítő képességeit hátráltatja, vagy jelentősen zavarja, a diplomáciai kapcsolatok tényleges sérelmét eredményezi, aminek következménye hivatalos tiltakozás vagy enyhébb szankció lehet, sérti az állampolgárok biztonságát és alkotmányos jogait, jelentősen sérti a nemzetgazdasági szempontból kiemelt jelentőségű gazdasági szervezet működését, hátráltatja a honvédelem és a nemzetbiztonsági tevékenység, illetve a szövetséges tagállamokkal közös biztonsági érdekek védelmének hatékonyságát, gátolja valamely legalább öt évi szabadságvesztéssel büntetendő bűncselekmény felderítését vagy elősegíti valamely ilyen bűncselekmény elkövetését, megzavarja az állami vagy közfeladatot ellátó szerv működési rendjét, feladat- és hatáskörének gyakorlását és ezáltal közvetve Magyarország törvényben meghatározott érdekeit sérti.

4. **Hátrányosan érinti az állam érdekeit és „Korlátozott terjesztésű!" minősítési szint alkalmazása indokolt**, ha az adat érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele megzavarja az állami vagy közfeladatot ellátó szerv működési rendjét, feladat- és hatáskörének gyakorlását és ezáltal közvetve Magyarország törvényben meghatározott érdekeit hátrányosan érinti, a hátrány azonban az elhárítására tett intézkedésekkel lényegesen enyhíthető vagy kiküszöbölhető. Az államnak az 1-3. pontba nem tartozó pénzügyi veszteséget okoz, továbbá, ha az állampolgárok vagy a gazdálkodó szervezetek részére jogtalan nyereséget vagy előnyszerzést tesz lehetővé.

A minősítéssel kapcsolatos részletes szabályokat a Mavtv. tartalmazza.

Üzleti titok

Az üzleti titok védelméről szóló törvény[314] alapján

- ✓ **üzleti titok** a gazdasági tevékenységhez kapcsolódó, titkos – egészben, vagy elemeinek összességeként nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető -, ennélfogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Azon információk, melyekkel kapcsolatban az érintett a hozzáférési jogát gyakorolhatja, így például a banki ügyintézővel folytatott telefonbeszélgetése nem minősülhetnek üzleti titoknak tekintettel arra, hogy azokat az érintettek, így a Kérelmező már megismerte, mivel vele folyt a beszélgetés, továbbá utólag az általános adatvédelmi rendelet szerint jogosult másolatban beszerezni a Kérelmezettől, márpedig a Üzleti titok tv. 1. § (1) bekezdés alapján üzleti titok a gazdasági tevékenységhez kapcsolódó, titkos – egészben, vagy elemeinek összességeként nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető -, ennélfogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja. A GDPR 15. cikk (4) bekezdés tartalmaz egy olyan rendelkezést, hogy a hozzáférési kérelem úgy teljesíthető, hogy az mások jogait és szabadságait ne érintse hátrányosan. (…) Az nem is képzelhető el, hogy ügyfeleknek ügyintézésre fenntartott telefonszámot tárcsázva a Kérelmezett az üzleti titkait osztja meg az érintettekkel, a banki ügyfelekkel.”[315]

- ✓ **védett ismeret (know-how)** az üzleti titoknak minősülő, azonosításra alkalmas módon rögzített, műszaki, gazdasági vagy szervezési ismeret, megoldás, tapasztalat vagy ezek összeállítása.

Az üzleti titok egyben lehet személyes adat is, ezen esetben az adatvédelemről szóló, vonatkozó jogszabályokat is alkalmazni kell.

[314] 2018. évi LIV. törvény az üzleti titok védelméről, https://net.jogtar.hu/jogszabaly?docid=A1800054.TV

[315] NAIH-55-11-2022, https://naih.hu/hatarozatok-vegzesek/file/540-uzleti-titokra-valo-hivatkozassal-hanganyag-korlatozott-felhasznalhatosaggal-torteno-rendelkezesre-bocsatasa, utolsó letöltés: 2022-07-28

A belga adatvédelmi hatóság (ADP/GBA) gyakorlatából

Egy informatikai vállalat (volt) alkalmazottja másolatot kért a róla kezelt összes adatról: e-mailekről, képekről és videókról, informatikai naplókról és HR-értékelésekről. A munkáltató megtagadta a hozzáférést ezek egy részéhez, így nem adta át a munkavállaló személyes aktájának másolatát (beleértve az említett aktában szereplő bizonyos megjegyzéseket és megjegyzéseket), valamint a munkavállalóra vonatkozó IT-naplók másolatát.

A belga adatvédelmi hatóság megállapította, hogy

- ✓ *a munkáltató megsértette a GDPR 15. cikkének (1) és (3) bekezdését, amikor megtagadta a munkavállalótól a személyes aktájához való hozzáférés jogát. A DPA kötelezte a munkáltatót, hogy a hozzáférési kérelem teljesítésével orvosolja ezt a jogsértést.*
- ✓ *az informatikai naplókhoz való hozzáférés biztosítása aránytalan terhet jelentene a munkáltató számára, és ez indokolja, hogy a munkáltató ezek esetében megtagadta a hozzáférést.*
- ✓ *az e-mailek másolatának kiadását nem lehet megtagadni azon az alapon, hogy a munkavállaló hozzáférhetett az e-mailekhez. Az elutasítás azonban alapozható potenciálisan üzleti titokra, ehhez azonban a munkáltatónak kell bizonyítania, hogy az említett e-mailek rendelkezésre bocsátása potenciálisan veszélyezteti az üzleti titkot. Ennek a kockázatnak az értékelését eseti alapon kell megítélni.*[316]

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A Kérelmezett nyilatkozatai szerint a betekintés során sem ismerhetné meg a Kérelmező az eredeti, módosítás nélküli felvételeket, csak azokat, amelyeken már a védendő adatok és információk kitakarásra kerültek. A kitakarás keretében a Kérelmezettnek arra is lehetősége van, hogy harmadik személyek személyes adatain túl azon információkat kitakarja, amelyek álláspontja szerint az üzleti titkát képezik. Az üzleti titkot képező információk kitakarásával a felvételek elvesztik az üzleti titok jellegüket, mivel önmagában a Kérelmező bankfiókban való mozgása nem tekinthető üzleti titoknak, mivel ezen információ semmiféle vagyoni értékkel nem bír. A bankfiókok ügyfélforgalom számára nyitva álló részének a berendezése, az ügyfélteret figyelő kamerák elhelyezése szintén nem minősül üzleti titoknak, mivel az az érintett gazdasági tevékenységet végzők számára is könnyen hozzáférhető információ.”[317]

[316] N° de dossier : DOS-2018-06125, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-15-2021.pdf, utolsó letöltés 2022. 07. 23.
[317] NAIH/2019/1859 határozat, Budapest, 2019. május 31.

Jogszabályok

GDPR

Az adatkezelés jogszerűsége [GDPR 6. cikk, (40)-(50) és (155) preambulumbekezdések]
A hozzájárulás feltételei [GDPR 7. cikk, (32)-(33) és (42)-(43) preambulumbekezdések]
A gyermek hozzájárulására vonatkozó feltételek az információs társadalommal összefüggő szolgáltatások vonatkozásában [GDPR 8. cikk, (38) preambulumbekezdés]
A személyes adatok különleges kategóriáinak kezelése [GDPR 9. cikk, (51)-(56) preambulumbekezdések]
A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok kezelése [GDPR 10. cikk]
Cookie-azonosítók [GDPR 4. cikk 1. pont, (30) preambulumbekezdés]

ÉRINTETTI JOGOK

„(…) az alapjog védelmét szolgáló érintetti jogok szükségtelen korlátozása, ellehetetlenítése közvetlen anyagi veszteség nélkül is jelentős alapjogi sérelmet okoz”[318]

A GDPR a természetes személyek alapvető jogait és szabadságait és különösen a személyes adatok védelméhez való jogukat védi,[319] az érintetti jogok pedig az információs önrendelkezési jog érvényesülését segítik elő.

Adatkezelésünk tekintetében kik lehetnek ezek a „természetes személyek”?

Azok az azonosított vagy azonosítható természetes személyek (érintettek), akikre az adott információ (adat) vonatkozik. Például:

- ✓ *munkavállalók/alkalmazottak (beosztástól, munkakörtől függetlenül, legyenek asszisztensek vagy akár vezérigazgatók)*
- ✓ *természetes személy szerződéses partnerek (beszállítók, árut és/vagy szolgáltatást nyújtók és igénybe vevők, megbízásos konstrukcióban dolgozók)*
- ✓ *szerződéses partnerek képviselői (kontaktszemélyek, utazó ügynökök, futárszolgálat futárra stb.)*
- ✓ *látogatók, azaz bárki, aki betér a területünkre (üzletünkbe, székhelyünkre, telephelyünkre stb.) szándékosan, vagy csak véletlenül*
- ✓ *álláskeresők (önmagukat írásban ajánlók, meghirdetett állásra jelentkezők, interjúra behívottak, fejvadászok adatbázisaiba regisztrálók stb.)*
- ✓ *munkavállalók/alkalmazottak hozzátartozói (gyermekek, házastársak, egyéb közeli hozzátartozók)*
- ✓ *különféle hivatalok és hatóságok képviselői stb.*

Az érintettek a GDPR alapján számos joggal rendelkezhetnek, így például

- ✓ tájékoztatáshoz való jog [13-14. cikk]
- ✓ hozzáférési jog [15. cikk]
- ✓ helyesbítéshez való jog [16. cikk]
- ✓ a törléshez való jog („az elfeledtetéshez való jog”) [17. cikk]
- ✓ az adatkezelés korlátozásához való jog [18. cikk]
- ✓ az adathordozhatósághoz való jog [20. cikk]
- ✓ a tiltakozáshoz való jog [21. cikk]
- ✓ automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást [22. cikk]
- ✓ a felügyeleti hatósághoz címzett panasz benyújtásának joga [77. cikk]
- ✓ bíróság előtti jogorvoslat [78-79. cikk]

[318] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: 2022. 07. 17.
[319] GDPR 1. cikk (2) bekezdés

Nekünk, adatkezelőknek mindent meg kell tennünk annak érdekében, hogy biztosítsuk mindazoknak a jogait, akiknek az adatait így vagy úgy kezeljük és megfelelő intézkedéseket kell hoznunk azért, hogy minden információt megadjunk számukra a jogaikkal kapcsolatban. Ráadásul ez sokkal nagyobb feladat, mint amilyennek elsőre látszik, mivel mindezt

- ✓ tömör,
- ✓ átlátható,
- ✓ érthető és
- ✓ könnyen hozzáférhető formában,
- ✓ világosan és közérthetően megfogalmazva

kell nyújtanunk az érintetteknek.

Az információkat írásban vagy más egyéb módon kell megadnunk, de akár szóban is, ha az érintett személyazonosságát igazoltuk.

Beépített emberi jogok

A GDPR minket, adatkezelőket arra ösztönöz, hogy az adatkezelési műveletek tervezésének már a legkorábbi szakaszaiban olyan technikai és szervezési intézkedéseket hajtsunk végre, amelyek a kezdetektől fogva biztosítják a magánélet és az adatvédelem elveit („**beépített adatvédelem**”; „data protection by design”). Alapértelmezés szerint biztosítanunk kell, hogy a személyes adatok kezelése a magánélet legmagasabb szintű védelme mellett történjen, illetve a személyes adatokat

alapértelmezés szerint ne tegyük hozzáférhetővé korlátlan számú személy számára („**alapértelmezett adatvédelem**"; „data protection by default").

Azonban nemcsak az adatkezelés megkezdése előtt, hanem folyamatosan az adatkezelés teljes időtartama alatt meg kell valósítanunk a beépített és alapértelmezett adatvédelmet azáltal, hogy rendszeresen felülvizsgáljuk az általunk választott intézkedések és garanciák hatékonyságát. A beépített és alapértelmezett adatvédelmet azokban a már meglévő rendszereink esetében is alkalmaznunk kell, amelyek személyes adatokat kezelnek.

A „**beépített emberi jogok**" („human rights by design") elvárásrendszere a mesterséges intelligencia használatának térhódításával terjedt el. A koncepció lényege, hogy az adatkezelési műveletekbe (termékekbe, szolgáltatásokba) a beépített és alapértelmezett adatvédelem mellett emberi jogok védelme is be legyen építve.

A beépített emberi jogok négy alappillére:

- ✓ ***tervezés és mérlegelés**: a rendszereket úgy kell megterveznünk, hogy azok megfeleljenek a nemzetközi emberi jogi jogszabályoknak. A tervezési folyamatoknak megfelelő mechanizmusokat kell tartalmazniuk, például olyan nyilvános konzultációt az emberi jogokat nagymértékben veszélyeztető mesterséges intelligenciával működő rendszerek esetében, amely újra tervezéshez vagy enyhítő stratégiák beépítéséhez vezethet.*
- ✓ ***tesztelés és értékelés**: az emberi jogoknak való megfelelést rendszeresen tesztelnünk kell a kezdeti javaslat megfogalmazásától kezdve a tervezésen, a fejlesztésen, a prototípusok kialakításán és a valós megvalósításon keresztül. A mesterséges intelligencia rendszer bevezetését követően folyamatos nyomon követést és rendszeres felülvizsgálatot kell végeznünk.*
- ✓ ***független felügyelet, vizsgálat és szankcionálás**: független, külső, és megfelelő forrásokkal rendelkező, valamint szakmailag kompetens (állami, nemzetközi) szervet kell létrehozni, amely egy jogilag felhatalmazott intézményi struktúrában felügyeli a mesterséges intelligencia rendszerek emberi jogi megfelelését.*
- ✓ ***nyomon követhetőség, bizonyíthatóság és bizonyítékok**: a mesterséges intelligencia rendszereket úgy kell megterveznünk, hogy az ellenőrizhetőséget biztosítsák, illetve a rendszer érdemi felülvizsgálat tárgyát képezhesse és bizonyítani lehessen az emberi jogok folyamatos betartását.*[320]

[320] Karen Yeung, Andrew Howes and Ganna Pogrebna, 'AI Governance by Human Rights-Centred Design, Deliberation and Oversight: An End to Ethics Washing' in Markus D Dubber, Frank Pasquale and Sunit Das (eds), The Oxford Handbook of AI Ethics (Oxford University Press, 2020) 77.

Tájékoztatáshoz való jog

Akár akarjuk, akár nem, akár kíváncsiak rá az érintettek akár nem, jogszabály alapján tájékoztatást kell nyújtanunk az érintetteknek arról, hogyan kezeljük a személyes adataikat, ugyanis ez a tájékoztatás szükséges ahhoz, hogy a személyes adatok kezelését átláthatóvá tegyük. Az érintetteknek számára meg kell tudnunk mondanunk, hogy az adataikat hogyan gyűjtjük és használjuk fel, azokba hogyan, mi módon tekinthetnek be, ezen kívül számot kell adnunk az adatkezelésünkkel kapcsolatos kockázatokról, garanciákról és az érintettek jogairól is – ezen tájékoztatás hiányában ugyanis az érintettek nem tudnak élni az információs önrendelkezési jogukkal.

Az átláthatóság elve megköveteli, hogy a személyes adatok kezelésével összefüggő tájékoztatásunk könnyen hozzáférhető és közérthető legyen, valamint azt világosan és egyszerű nyelvezettel fogalmazzuk meg.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A munkahelyen alkalmazott kamerás megfigyelés kapcsán a kiindulópontot az Mt. jelenti, melynek 42. § (2) be-kezdés a) pontja értelmében a munkaszerződés alapján a munkavállaló köteles a munkáltató irányítása szerint munkát végezni. Ezzel összhangban a jogalkotó az Mt. 52. § (1) bekezdés b) és c) pontjában a munkavállaló alapvető kötelességeként határozta meg azt, hogy a munkavállaló köteles munkaideje alatt a munkáltató rendelkezésére állni és munkáját az általában elvárható szakértelemmel és gondossággal, a munkájára vonatkozó szabályok, előírások, utasítások és szokások szerint végezni. E törvényi kötelezettségek megtartása végett a jogalkotó az Mt. 11/A. § (1) bekezdésében lehetőséget biztosít arra, hogy a munkáltató a munkavállalót a munkaviszonnyal összefüggő magatartása körében ellenőrizze, akár technikai eszköz alkalmazásával is. Ez a jogosultság személyes adatok kezelésével járhat együtt.

Az Mt. 9. § (2) bekezdése kimondja továbbá, hogy a munkavállaló személyiségi joga akkor korlátozható, ha a korlátozás a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos. A személyiségi jog korlátozásának módjáról, feltételeiről és várható tartamáról, továbbá szükségességét és arányosságát alátámasztó körülményekről a munkavállalót előzetesen írásban tájékoztatni kell. (…)

Az Mt. 11/A. § (1) bekezdése alapján a munkáltató ellenőrizheti a munkavállalót a munkaviszonnyal összefüggésben, akár technikai eszközzel, azonban erről előzetesen írásban – az általános adatvédelmi rendelet 13. cikk (1)-(2) bekezdés szerinti információkra is kiterjedően – tájékoztatnia kell a munkavállalót, elkerülve azt, hogy a kamerák titkos megfigyelési eszközzé váljanak. (…)
Az Mt. 11/A. § (1) bekezdésében megfogalmazott általános tájékoztatási kötelezettséget a személyes adatok kezelése tekintetében az általános adatvédelmi rendelet előírásait is figyelembe véve kell teljesíteni, azaz mintegy az általános

adatvédelmi rendelet tölti meg tartalommal, meghatározva azon körülményeket, melyekről e tekin-tetben a munkáltatónak tájékoztatnia kell a munkavállalókat." [321]

Miről kell tájékoztatunk az érintetteket?

- ✓ az adatkezelő kilétéről és az adatkezelés céljáról
- ✓ mind arról ami biztosítja, hogy a személyes adatok kezelése tisztességes és átlátható, illetve arról, hogy
- ✓ az érintetteknek jogukban áll megerősítést és tájékoztatást kapni a róluk kezelt adatokról.

<table>
<tr><th colspan="2">Tájékoztatási kötelezettségünk, ha</th></tr>
<tr><th>az érintettől gyűjtjük az adatokat
[13. cikk]</th><th>nem az érintettől gyűjtjük az adatokat
[14. cikk]</th></tr>
<tr><td colspan="2">az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kiléte és elérhetőségei</td></tr>
<tr><td colspan="2">az adatvédelmi tisztviselő elérhetőségei, ha van ilyen</td></tr>
<tr><td colspan="2">a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja</td></tr>
<tr><td></td><td>az érintett személyes adatok kategóriái</td></tr>
<tr><td colspan="2">ha az adatkezelés a GDPR 6. cikk (1) bekezdésének f) pontján alapul, az adatkezelő vagy harmadik fél jogos érdekeiről</td></tr>
<tr><td colspan="2">a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen</td></tr>
<tr><td colspan="2">adott esetben annak ténye, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat, továbbá a Bizottság megfelelőségi határozatának léte vagy annak hiánya, vagy a GDPR 46. cikkben, a 47. cikkben vagy a 49. cikk (1) bekezdésének második albekezdésében említett adattovábbítás esetén a megfelelő és alkalmas garanciák megjelölése, valamint az azok másolatának megszerzésére szolgáló módokra vagy az azok elérhetőségére való hivatkozás</td></tr>
<tr><td colspan="2">a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai</td></tr>
<tr><td colspan="2">az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való joga</td></tr>
<tr><td colspan="2">a GDPR 6. cikk (1) bekezdésének a) pontján vagy a 9. cikk (2) bekezdésének a) pontján alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét</td></tr>
<tr><td colspan="2">a felügyeleti hatósághoz címzett panasz benyújtásának joga</td></tr>
</table>

[321] NAIH/2020/643/6, Budapest, 2020. július 17., https://www.naih.hu/files/NAIH-2020-643-hatarozat.pdf, utolsó letöltés: 2022. 07. 14.

arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint az érintett köteles-e a személyes adatokat megadni, továbbá, hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása	a személyes adatok forrása és adott esetben az, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e
a GDPR 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír	
Ha az adatkezelő a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő célról és minden releváns kiegészítő információról	
időpont: a személyes adatok megszerzésének időpontjában	időpont: a) a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül b) ha a személyes adatokat az érintettel való kapcsolattartás céljára használjuk, legalább az érintettel való első kapcsolatfelvétel alkalmával; vagy c) ha várhatóan más címzettel is közöljük az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor.
Nincs szükség tájékoztatásra: az érintett már rendelkezik az információkkal	Nincs szükség tájékoztatásra: a) az érintett már rendelkezik az információkkal. b) a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne, különösen a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból végzett

	adatkezelés esetében, vagy amennyiben a tájékoztatási kötelezettség valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezen adatkezelés céljainak elérését. c) az adat megszerzését vagy közlését kifejezetten előírja az adatkezelőre alkalmazandó uniós vagy tagállami jog, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről rendelkezik. d) a személyes adatoknak valamely uniós vagy tagállami jogban előírt szakmai titoktartási kötelezettség alapján, ideértve a jogszabályon alapuló titoktartási kötelezettséget is, bizalmasnak kell maradnia.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„(…) az Ügyfél köteles olyan tömör és érthető módon az adatkezelés megértéséhez minimálisan szükséges információkat nyújtani az érintettek részére, amelyek alapján az érintettek legalább az adatkezelés alapvető mivoltával tisztában vannak. Ezt az Ügyfél sem előzetesen, sem a visszahívások során nem teszi meg, az ügyfélszolgálatát telefonon kereső érintettek pedig semmiből nem sejthetik a hangjuk automatikus elemzését, és nem számíthatnak ésszerűen arra, hogy kérés nélkül visszahívják őket többek között a hangjuk tónusa miatt. Az általános adatvédelmi rendelet 24. cikk (1) bekezdésének megfelelően az adatkezelés újszerű jellege, az érzelmek elemzése és egyéb pszicholingvisztikai elemzések szenzitív jellege, és a többi, fentebb feltárt adatkezelési körülmény alapján az Ügyfél köteles lett volna az adatkezelést akként kialakítani, hogy az maximálisan biztosítsa az érintetti jogokat és szabadságokat, amelyet nyilvánvalóan nem tett meg. Az, hogy erre eddig kevés érintetti panasz érkezett, nem azt erősíti, hogy az érintetteket ez nem zavarta, hanem azt, hogy ésszerűen nem is tudhattak erről, amely önmagában erősen megkérdőjelezi az adatvédelmi megfelelést.”[322]

A belga adatvédelmi hatóság (APD/GBA) gyakorlatából

Az APD/GBA azt vizsgálta, hogy egy autonóm tartományi turisztikai közintézmény megsértette-e a GDPR-t azzal, hogy a Covid19 járvány idején intelligens kamerákat helyezett el a járókelők számlálására meghatározott helyszíneken.
A hatóság arra a megállapításra jutott, hogy a közintézmény nem bizonyította hitelt érdemlően, hogy

[322] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: 2022. 07. 17.

- ✓ *az érintettek megfelelő és átlátható tájékoztatást kapnak (a weboldalon közzétett adatvédelmi tájékoztatás nem volt teljesen pontos és átlátható),*
- ✓ *a személyes adatok kezelése az intelligens kamerákon keresztül konkrét, egyértelmű és jogszerű célokból történik,*
- ✓ *az intelligens kamerák segítségével kezelt személyes adatok megfelelőek, relevánsak és a feldolgozás céljaihoz szükséges mértékre korlátozódnak, illetve*
- ✓ *miért szükséges a személyes adatok intelligens kamerákon keresztül történő kezelése közérdekű feladatának teljesítéséhez.*[323]

Milyennek kell lennie a tájékoztatásunknak?

- ✓ Tömörnek, átláthatónak, érthetőnek és könnyen hozzáférhetőnek;
- ✓ világosnak és közérthetőnek, azaz a célközönség számára érthetően megfogalmazottnak;
- ✓ a világos és közérthető megfogalmazás különösen fontos a gyermekeknek címzett információk esetében;
- ✓ az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadnunk;
- ✓ az érintett kérésére szóbeli tájékoztatást is adhatunk;
- ✓ a tájékoztatást általában díjmentesen kell biztosítanunk (a kivételeket a vonatkozó jogszabály tartalmazza).

Például, ***ha veszünk egy okos tévét, érintettként jó lenne tudnunk****, hogy*

- ✓ *milyen adatokat gyűjt rólunk (kedvenc csatornáink és műsoraink, be- és kikapcsolás időpontja, használat időtartama, internetes böngészési adatok, hangfelvétel, hangasszisztenssel beszélgetéseink stb.);*
- ✓ *az adatainkat a világ melyik pontján ki és mire használja (hol, ki és milyen célból profiloz minket műsorajánlás, marketing és egyéb célból, milyen más adatbázisokkal vezetik össze az adatainkat stb.);*
- ✓ *egyéni tévénézési szokásaink alapján kapjuk-e a reklámokat (személyre szabottan), vagy más módon, például területi alapon válogatják ki nekünk azokat;*
- ✓ *használnak-e mesterséges intelligenciát a profilozásunkra;*
- ✓ *marketing és egyéb, például értékesítési célra használják-e az adatainkat, illetve marketing célból pontosan hány szervezetnek továbbíthatják azokat (adatbrókerek, fejlesztők, tartalomszolgáltatók stb.);*
- ✓ *a tévénk csak a távszabályzó segítségével bevitt adatokat gyűjti, vagy hallgatózik, hangasszisztenssel folytatott társalgásainkat is rögzíti, netalán beszélget-e más okos eszközökkel is, illetve ezektől (okos riasztórendszer, kaputelefon, vízforraló, termosztát, lézeres macskajáték stb.) további információkat gyűjt-e, és ezeket a pluszban begyűjtött információkat kinek és hogyan továbbítja;*
- ✓ *a tévénézés adatait összevezetik-e más forrásból gyűjtött adatokkal és úgy profiloznak-e minket (pl. notebook, PC, tablet, telefon, e-mail, kutyánk*

[323] Numéro de dossier : DOS-2020-02716, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-24-2021.pdf, utolsó letöltés: 2022. 07. 23.

okosnyakörve, akváriumunk hőmérője, más szolgáltatóktól, illetve adatbrókerektől vásárolt adatok stb.);

- ✓ *milyen biztonsági intézkedésekkel védik a tévé által gyűjtött adatainkhoz hozzáférő adatkezelők és adatfeldolgozók az adatainkat és*
- ✓ *hogyan, milyen beállítások segítségével tudjuk megakadályozni a párttalan megfigyelésünket.*

A tévénk természetesen nemcsak rólunk gyűjt adatot, hanem mindenki másról is, aki csak megfordul az eszköz környezetében (családtagjaink, barátaink, szomszédjaink stb.). És természetesen olyan személyekről is, akik nincsenek tudatában annak, hogy a tévénk hangyaszorgalommal figyel „rájuk" (is).

Az adatvédelmi incidensről szóló tájékoztatásunknak ugyanezen követelményeknek kell megfelelnie, különös tekintettel a világos és közérthető nyelvezetre.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A munkahelyi kamerás megfigyeléssel összefüggő adatkezelés esetében lényeges követelmény, hogy a munkavállalók az adatkezelésről megfelelő, átlátható és könnyen értelmezhető tájékoztatást kapjanak. Ezzel kapcsolatban az alábbiakat kell figyelembe venni:
Az Mt. 9. § (2) bekezdése értelmében: „A személyiségi jog korlátozásának módjáról, feltételeiről és várható tartamáról, továbbá szükségességét és arányosságát alátámasztó körülményekről a munkavállalót előzetesen írásban tájékoztatni kell."
Az Mt. 11/A. § (1) bekezdése szerint, ha a munkáltató technikai eszközt is alkalmaz a munkavállalók ellenőrzésére, erről előzetesen írásban köteles tájékoztatni őket.
Az általános adatvédelmi rendelet 13. cikk (1)-(2) bekezdése tartalmazza, hogy az adatkezelés vonatkozásában milyen információkat kell a munkavállalók rendelkezésére bocsátani az adatkezeléssel kapcsolatban.

A kamerás megfigyeléssel összefüggő adatkezelés esetében az általános adatvédelmi rendelet által előírt követelményrendszer szerint a munkavállalókat különösen az alábbi lényeges körülményekről kell tájékoztatni:

- *az elektronikus megfigyelőrendszert üzemeltető személyéről (jogi vagy természetes személy pontos megnevezésével) és elérhetőségeiről,*
- *az adatvédelmi tisztviselő elérhetőségéről, amennyiben az adatkezelő nevezett ki ilyen személyt,*
- *az egyes kamerák elhelyezéséről és a vonatkozásukban fennálló célról, az általuk megfigyelt területről, tárgyról, illetőleg arról, hogy az adott kamerával közvetlen vagy rögzített megfigyelést végez-e a munkáltató,*
- *az adatkezelés jogalapjáról,*
- *az adatkezelő jogos érdekének a meghatározásáról,*
- *a felvétel tárolásának időtartamáról,*
- *az adatok megismerésére jogosult személyek köréről, illetőleg arról, hogy a felvételeket mely személyek, szervek részére, milyen esetben továbbíthatja a munkáltató,*
- *a felvételek visszanézésére vonatkozó szabályokról, illetőleg arról, hogy a felvételeket milyen célból használhatja fel a munkáltató,*

- *arról, hogy a munkavállalókat milyen jogok illetik meg az elektronikus megfigyelőrendszerrel összefüggésben és milyen módon tudják gyakorolni a jogaikat,*
- *arról, hogy az információs önrendelkezési joguk megsértése esetén milyen jogérvényesítési eszközöket vehetnek igénybe, így többek között a Hatósághoz fordulás lehetőségéről.*

A tájékoztatási kötelezettséggel kapcsolatban szükséges továbbá kiemelni, hogy a munkáltatónak minden egyes kamera vonatkozásában pontosan meg kell jelölnie, hogy az adott kamerát milyen célból helyezte el az adott területen és milyen területre, berendezésre irányul a kamera látószöge. A munkáltató ezzel tudja igazolni a munkavállalók számára azt, hogy miért tekinthető szükségesnek az adott terület megfigyelése. Nem fogadható el az a gyakorlat, amikor a munkáltató csupán általánosságban tájékoztatja a munkavállalókat arról, hogy elektronikus megfigyelőrendszert alkalmaz a munkahely területén. (…)"[324]

Amennyiben úgy érezzük, hogy túl sok mondanivalónk van tájékoztatás címén, a kevésbé lényeges, vagy jól elkülöníthető tartalmakat mellékletekbe is rendezhetjük (például sütikezelési szabályzat, adatfeldolgozók felsorolása stb.). Fontos, hogy az érintetteket csak a valós adatkezelésekről tájékoztassuk, mert a felesleges többletinformáció, különösen ha az nem végzett tevékenységekre vonatkozik, az átláthatóság elvébe ütközhet, illetve a tömör, könnyen érthető kommunikációval kapcsolatos követelményeket sem teljesítjük.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Az adatkezelési tájékoztató továbbra is tartalmazza a hírlevélküldéssel kapcsolatos rendelkezéseket. Ezzel ellentétben nem áll rendelkezésre a Kötelezett azon nyilatkozatát cáfoló bizonyíték, miszerint a Hatóság hírlevelekkel kapcsolatos korábbi felhívását teljesítette, és nem küldött hírleveleket. Ez azonban nem lett átvezetve az adatkezelési tájékoztatón, így az érintettek részére megtévesztő tájékoztatást adott erről, mintha jelenleg is folytatna hírlevélküldési célú adatkezelést.

Nem áll rendelkezésre a Kötelezett azon nyilatkozatát cáfoló bizonyíték, miszerint a Hatóság hírlevelekkel kapcsolatos korábbi felhívását teljesítette, és nem tart meg a törlési kérelmek teljesítését követően egyes személyes adatokat. Ez azonban nem lett átvezetve az adatkezelési tájékoztatón, így az érintettek részére megtévesztő tájékoztatást adott az adatok megtartásáról és esetlegesen harmadik személyek részére továbbításáról.

Az adatkezelő arról tájékoztatja az érintetteket, hogy az adatkezelés bejelentésre került az adatvédelmi nyilvántartásba. 2018. május 25-től, az általános adatvédelmi rendelet alapján a Hatóság már nem vezeti az adatvédelmi nyilvántartást, így ezen tájékoztatás valótlan és félrevezető. Az általános adatvédelmi rendelet 30. cikke

[324] NAIH-1006-3/2022, Budapest, 2022. március 29., https://www.naih.hu/hatarozatok-vegzesek?download=521:munkahelyi-kameras-megfigyeles-jogalapjanak-es-arrol-valo-tajekoztatasnak-jogszerusege, utolsó letöltés: 2022. 07. 14.

alapján 2018. május 25-től az adatkezelő köteles az adatkezelési tevékenységekről nyilvántartást vezetni.
A fentiek sértik az általános adatvédelmi rendelet 12. cikk (1) bekezdése szerinti tömör, átlátható, érthető és könnyen hozzáférhető formájú, világosan és közérthetően megfogalmazott tájékoztatás nyújtásának kötelezettségét, valamint az általános adatvédelmi rendelet 5. cikk (1) bekezdés a) pontja szerinti jogszerű és átlátható adatkezelés elvét, mivel a Kötelezett valótlan és ellentmondásos tájékoztatást ad az érintetteknek, úgy, hogy az érintettek ez alapján ésszerűen nem érthetik meg az adatkezelés lényegét."[325]

Az érintettek információba fojtásának elkerülése érdekében folyamodhatunk többszintű tájékoztatáshoz is, az érintettek pedig eldönthetik, mennyi és milyen mélységű részletet igényelnek az adataik kezelésével kapcsolatban.

A többrétegű tájékoztatásra az egyik legjobb példa az elektronikus megfigyelőrendszer üzemeltetése során alkalmazott tájékoztatások lehetnek, melyek a következők:

- ✓ **minimum tartalmú tájékoztatás**: a belépési pontokon piktogramok és figyelemhívó táblák jelzik számunkra a megfigyelés tényét a legalapvetőbb információkat nyújtva; ezen jelzések láttán számíthatunk az adataink kezelésére
- ✓ **kb. egy oldalnyi tájékoztatás**: a portán vagy valahol a bejárat közelében részletesebb tájékoztatóval tudathatják velünk, hogy meddig és ki őrzi a felvételeket, milyen alapvető jogaink vannak és kinél panaszkodhatunk, valamint szükség esetén hol kérhetünk másolatot a felvételekről. Ez a tájékoztató utalhat a „nagy", teljeskörű tájékoztató feltalálási helyére, azaz, ha még több információra van szükségünk, abban az esetben hol,merre találjuk azt
- ✓ **teljeskörű tájékoztatás**: a „nagy" tájékoztató részletes és kimerítő tájékoztatást nyújt az összes érintetti jog tartalmáról és az érintetti jogok érvényesítésének módjáról, valamint minden, az adatkezelésekkel kapcsolatos tényről, amit csak a GDPR megkövetel. Ez a tájékoztatás lehet akár 10-15 oldalnyi terjedelmű vagy még hosszabb is, attól függően, hogy az elektronikus megfigyelésre vonatkozó szabályzatból, illetve a vonatkozó érdekmérlegelési tesztekből mennyit emel át az adatkezelő annak érdekében, hogy minél kevesebb különálló dokumentumot kelljen az érintettnek „összefésülnie" a teljeskörű tájékozódása során.

A spanyol adatvédelmi hatóság (AEPD) gyakorlatából

Miután több panasz érkezett egy energiaipari vállalat (EDP Energía) adatgyűjtésével és -kezelésével kapcsolatban, az AEPD vizsgálatot indított, mely során megállapította, hogy – többek között – nem teljesült a GDPR 13. cikkében foglalt valamennyi követelmény. Például

- ✓ *az egyes szerződéskötési csatornákon keresztül nyújtott tájékoztatás nem adott információt az érintettek jogairól, és nem kínált módot arra, hogy egy második szinten hozzáférjenek azok összességéhez. Ezért a felkínált*

[325] NAIH/2020/2000/5. https://naih.hu/files/NAIH-2020-2000-hatarozat.pdf, 2022. 08. 27.

információk általában (bár az alkalmazott szerződéskötési csatornától függően eltérőek lehettek) töredezettek és szétszórtak voltak,

- ✓ *ha a szerződéskötés telefonon keresztül történt, a legalapvetőbb információk megszerzésének egyetlen lehetősége az volt, hogy vagy átirányították egy másik hívásra, vagy az adatvédelmi nyilatkozatra kellett menni anélkül, hogy a szerződéskötés pillanatában tájékoztatták volna az érintettet megillető jogokról. Az elektronikus úton történő szerződéskötés esetén az érintett nem tudott könnyen hozzájutni ilyen információkhoz, mivel átirányították a szerződéskötési megállapodáshoz, nem pedig egy nem könnyen hozzáférhető információhoz (ez utóbbit meg kellett keresni az adatkezelő weboldalán).*

A GDPR 13. cikke szerint ezeket az információkat az adatkezelőnek közvetlenül az érintettnek kell megadnia, és az a gyakorlat nem megfelelő, amelyben az adatkezelő általános módon kínálja fel ezeket az információkat, az érintettnek pedig aktívan keresgélnie kell azokat. Ez a kívánalom összhangban van az átláthatóság elvével is, azaz a tájékoztatást az adatgyűjtés időpontjában kell felajánlani, nem pedig utólag. Ezeknek a követelményeknek megfelelés általában úgy történik, hogy a tájékoztatást rétegesen nyújtják. Az AEPD a határozatában kifejti, hogy például telefonos szerződéskötés esetén az alapvető információkat (célok, az adatkezelő személye, az érintettek jogai és az adott adatkezeléssel kapcsolatos legfontosabb információk) a hívás során is meg lehet adni, a többi információt pedig később e-mailben vagy az adatvédelmi tájékoztatóra mutató hivatkozáson keresztül lehet elküldeni. A tájékoztatáshoz használt rétegek nem vezethetnek késedelemhez a kevésbé lényeges információk megadásában, amit szintén az adatgyűjtés pillanatában kell megtenni.

Az AEPD álláspontja szerint problematikus az a mód, ahogyan az érintettet tájékoztatták az adatkezelő személyéről. Az adatkezelő, az EDP két különböző vállalatra oszlik: EDP Energy és EDP Marketer. A tájékoztatás szerint „az adatokat az EDP Energy és az EDP Marketer kezeli", akik mindketten adatkezelőnek minősülnek. Nincs azonban konkrét utalás arra, hogy melyik vállalat mely adatokat és milyen célból kezel, ami zavaros és pontatlan tájékoztatást eredményez. Az adatvédelmi tájékoztató, miután tisztázta mindkét adatkezelő létezését, további pontosítás nélkül csak az általános nevet (EDP) használja.

Az AEPD véleménye az volt az esettel kapcsolatban, hogy

- ✓ *a megadott információk alapján nehéz beazonosítani, hogy az adatkezelési tevékenységek hogyan kapcsolódnak az adatkezelő által használt egyes jogalapokhoz és nem egyértelmű, hogy mely folyamatok esetében hivatkozik jogos érdekre. A hivatkozott jogalapokat egyértelműen meg kell adni a tájékoztatásban és az sem tisztázott, hogy az adatkezelő milyen konkrét jogos érdekre vagy érdekekre hivatkozik.*
- ✓ *nem világos, milyen következményekkel jár az ügyfelek kereskedelmi profiljának létrehozása, és hogy ez az adatkezelés a GDPR 21. cikk értelmében kifogásolható-e, és ettől függetlenül a GDPR 22. cikke értelmében profilalkotásnak tekinthető-e.*
- ✓ *nem világos, hogy milyen adatkezelési tevékenységek hivatkoznak hozzájárulásra, mivel a megadott információk nem konkrétak és nem érthetőek egy átlagember számára (pl. a személyre szabott ajánlatok*

nyújtására irányuló adatkezelés, amely a megadott adatok összesített adataiból történik).

- ✓ *a tiltakozási jog (GDPR 21. cikk) létezésének puszta kijelentése – utalva, mint bizonyos adatkezelési tevékenységek elleni tiltakozáshoz való jogra – nem elegendő.*
- ✓ *a jogok gyakorlásának biztosítása érdekében szükséges, hogy az érintett tájékoztatást kapjon arról, hogy az egyes adatkezelésekhez milyen jogalapot használnak, így az érintett egyértelműen tudja, hogy melyik adatkezelési tevékenységhez adott hozzájárulást, így azt vissza is tudja vonni, és hogy mely adatkezelési tevékenységek történnek jogos érdekre hivatkozással, így az érintett tisztában van azzal, hogy az adatkezelés ellen élhet a tiltakozás jogával.*

Ebben az ügyben az AEPD összesen 1,5 millió eurós bírságot szabott ki az energiaipari vállalatra, mivel az érintetteket nem tájékoztatta megfelelően a GDPR 13. cikke alapján (1 millió EUR), illetve nem hajtott végre megfelelő intézkedéseket az adatkezeléssel kapcsolatos kockázatok elkerülése vagy mérséklése érdekében a GDPR 25. cikke alapján (500 ezer EUR).[326]

A GDPR egyéb esetekben is nevesít tájékoztatási kötelezettséget, például:

- ✓ a közös adatkezelésről szóló megállapodásunk lényegét az érintett rendelkezésére kell bocsátanunk;
- ✓ amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, indokolatlan késedelem nélkül tájékoztatnunk kell az érintette(ke)t az adatvédelmi incidensről.

Mikor nem kell tájékoztatnunk az érintetteket?

Akkor nem kell tájékoztatnunk az érintetteket,

- ✓ amennyiben már rendelkeznek a szükséges információkkal;
- ✓ a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne, vagy amennyiben a tájékoztatási kötelezettség valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné adatkezelésünk céljainak elérését. Ilyen esetekben megfelelő intézkedéseket kell hoznunk – az információk nyilvánosan elérhetővé tételét is ideértve – az érintettek jogainak, szabadságainak és jogos érdekeinek védelme érdekében;
- ✓ az adat megszerzését vagy közlését kifejezetten előírja olyan, ránk, mint adatkezelőre alkalmazandó uniós vagy tagállami jog, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről rendelkezik;
- ✓ a személyes adatoknak valamely uniós vagy tagállami jogban előírt szakmai titoktartási kötelezettsége alapján, ideértve a jogszabályon alapuló titoktartási kötelezettséget is, bizalmasnak kell maradnia.

[326] Procedimiento Nº: PS/00236/2020, https://www.aepd.es/es/documento/ps-00236-2020.pdf, utolsó letöltés 2022. 07. 24.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Az adatkezelőnek a GDPR 14. cikke szerinti tájékoztatást kell nyújtania azon esetekben, amikor nem az érintettől szerezte meg a személyes adatait. A GDPR 14. cikk (2) bekezdés f) pontja szerint – ha a személyes adatot az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával – az adatkezelő tájékoztatja az érintettet többek között a személyes adatai forrásáról. Ezen kötelezettség azonban nem áll fenn annyiban, – és abban a mértékben – ha az érintett már rendelkezik azon információkkal, amelyekről őt az adatkezelőnek tájékoztatnia kellene a GDPR 14. cikke alapján.

Amennyiben tehát a [cég] a küldemény kézbesítését megelőzően e-mailben vagy SMS-ben tájékoztatja a címzetteket a kézbesítés várható idejéről, úgy tájékoztatnia kell a címzetteket arról, hogy mi volt a személyes adataik forrása, azaz ki a küldemény feladója. Azokban az esetekben, amikor például a címzett a feladótól megrendelt egy terméket, amelyet a [cég] kézbesít a számára, és a feladó a megrendelés során tájékoztatta a címzettet arról, hogy a kézbesítéshez a [cég] szolgáltatását veszi igénybe, úgy a címzettnek már rendelkeznie kell azzal az információval, hogy a feladó továbbította a nevét és cím adatát a [cég] számára – abból a célból, hogy teljesítse a feladó és a címzett között létrejött szerződést – így a [cég] – választása szerint – mellőzheti a kézbesítésről tájékoztató SMS-ből vagy e-mail üzenetből a feladó személyéről mint a személyes adatok forrásáról való tájékoztatást.

Abban az esetben, ha a kézbesítés várható idejéről a [cég] nem küld külön tájékoztatást a címzettek részére, hanem enélkül kézbesíti a küldeményt vagy annak megkísérléséről értesítést hagy a címzettnek, úgy – mivel a címzett a küldemény vagy értesítés átvételével egyidejűleg értesül a feladó személyéről – a GDPR 14. cikk (5) bekezdése alapján nem szükséges tájékoztatnia az címzetteket a személyes adataik forrásáról."[327]

Személyes adatokhoz hozzáférés joga

Az Alapjogi Charta a személyes adatok védelméhez való alapjog részeként határozza meg azt, hogy az érintettek saját adataikhoz hozzáférjenek.

Az Európai Unió Bíróságának (EUB) gyakorlatából

Az EUB azt állapította meg, hogy az érintett hozzáféréshez való joga szükséges annak lehetővé tételéhez, hogy az érintett gyakorolni tudja azon jogait, hogy kérelmére az adatkezelő helyesbítse, törölje vagy korlátozza az adatait, vagy kérelmére az adatkezelő értesítse az adatokról tudomást szerző harmadik feleket e helyesbítésről, törlésről vagy korlátozásról. Tényleges hozzáférési jog szükséges továbbá azért is, hogy az érintettnek lehetősége legyen az adatkezelés elleni tiltakozáshoz való jogának gyakorlására vagy panasz benyújtásának jogára, illetve azon jogára, hogy kártérítést követeljen. A hozzáférési jognak a bíróság szerint

[327] NAIH/2018/3607/2/V. https://www.naih.hu/files/Adatved_allasfoglalas_NAIH-2018-3607-2.pdf, utolsó letöltés 2022. 08. 27.

nemcsak a jelenre, hanem a múltra is kell vonatkoznia, mivel ennek hiányában az érintett nem gyakorolhatja eredményesen a jogszerűtlennek vagy helytelennek vélt adatok helyesbítéséhez, törléséhez vagy korlátozásához fűződő, valamint jogorvoslati és kártérítéshez való jogát.

A holland bírósági gyakorlatból

A hozzáférési jog gyakorlása során az érintettnek nem kell különösebb érdeket bizonyítania, illetve megadni azt a célt, amelyet a hozzáféréssel el kíván érni, elég az a puszta tény, hogy a rá vonatkozó adatokat kezeli az adatkezelő. Ebben az ügyben a kérelmezők kijelentették, hogy saját adataik helyességét és jogszerűségét kívánják ellenőrizni, és hogy ez előfeltétele más magánélethez fűződő jogok gyakorlásának. Ez elegendő.[328]

A szlovén adatvédelmi hatóság (IP) gyakorlatából

A személyes adatok hozzáférésének joga a GDPR 15. cikke értelmében csak arra a személyre vonatkozik, akinek a személyes adatairól van szó, azaz a kérelmező nem kérhet az adatkezelőtől egy másik személy személyes adataihoz való hozzáférést a GDPR 15. cikkre hivatkozva.[329]

A hozzáférés joga igen fontos az érintettek számára, mivel ezen jog alapján tudnak élni a további érintetti jogaikkal:

- ✓ ha az érintettek nem kapnak hozzáférést az adataikhoz, honnan tudnák, hogy pontatlan vagy hibás személyes adatukat kezeljük adatkezelőként?
- ✓ ha nem tudják, hogy mire hivatkozva kezeljük az adataikat, hogyan tudnának tiltakozni az adatkezelésünk ellen?

A ciprusi adatvédelmi hatóság (Commissioner) gyakorlatából

Az adatvédelmi hatóság úgy ítélte meg, hogy a személyes adatokhoz való hozzáféréshez való jog megsértésének minősül, ha az adatkezelő nem képes megtalálni az érintettel kötött eredeti szerződést és emiatt 15 ezer eurós bírságot szabott ki.
Egy érintett hozzáférési kérelmet nyújtott be a Bank of Cyprushoz és az Eurolife Ltd biztosítótársasághoz, amelyben az eredeti biztosítási szerződés másolatát kérte. A Bank a 2000-ben aláírt eredeti szerződést nem találta meg az irattárában, ezért felajánlotta, hogy felmondja a szerződést és új szerződést köt az érintettel.

A ciprusi adatvédelmi hatóság megállapította, hogy a személyes adatok elérhetetlensége adatvédelmi incidensnek minősül, és hogy ezt be kell jelenteni az adatvédelmi hatóságnak, mivel az valószínűleg kockázatot jelent az érintett jogaira és szabadságaira nézve. Az adatvédelmi hatóság azt is megállapította, hogy a Bank

[328] ECLI:NL:RBAMS:2021:1019, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1019&showbutton=true&keyword=AVG, utolsó letöltés: 2022. 07. 24.
[329] 07121-1/2020/1408, https://www.ip-rs.si/mnenja-gdpr/6048a57a38e8d, utolsó letöltés: 2022. 07. 24.

nem hajtott végre megfelelő technikai és szervezési intézkedéseket a személyes adatok biztonságának (bizalmas jelleg, integritás és rendelkezésre állás) biztosítása érdekében. Ezen kívül mivel a Bank nem találta meg az eredeti megállapodást, nem tett eleget az érintett hozzáférési kérelmének, illetve nem bizonyította az elszámoltathatóság elvének megfelelőségét.[330]

A GDPR alapján az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, akkor jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

- ✓ az adatkezelés céljai;
- ✓ az érintett személyes adatok kategóriái;
- ✓ azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
- ✓ adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- ✓ az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
- ✓ a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
- ✓ ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
- ✓ a GDPR 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár;

Holland bírósági gyakorlatból

Az Oost-Brabant kerületi bíróság megállapította, hogy a T-Mobile megsértette egy ügyfél hozzáférési jogát, mivel nem nyújtott további tájékoztatást az automatizált döntéshozatalról és profilalkotásról.
Az érintettnek telefonelőfizetése volt a T-Mobile-nál. A Központi Statisztikai Hivatal (CBS) statisztikai kutatást végzett a T-Mobile-tól megszerzett nagy adatállományok felhasználásával. A T-Mobile kijelentette, hogy nem osztottak meg személyes adatokat a CBS-szel, mivel minden adatot anonimizáltak.

[330] Commissioner – 11.17.001.008.001, https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/B64595978C98EFCEC2258606003EC47E/$file/%CE%91%CE%9D%CE%A9%CE%9D%CE%A5%CE%9C%20%CE%91%CE%A0%CE%9F%CE%A6%CE%91%CE%A3%CE%97%20%CE%A4%CE%A1%CE%91%CE%A0%CE%95%CE%96%CE%91%20%CE%9A%CE%A5%CE%A0%CE%A1%CE%9F%CE%A5%20%CE%91%CE%A0%CE%A9%CE%9B%CE%95%CE%99%CE%91%20%CE%95%CE%93%CE%93%CE%A1%CE%91%CE%A6%CE%9F%CE%A5.pdf, utolsó letöltés 2022. 07. 18.

Az érintett kétségbe vonta a T-Mobile nyilatkozatát és hozzáférési kérelmet nyújtott be a T-Mobile által a CBS kutatásához kezelt személyes adatokra vonatkozóan, ezt azonban a T-Mobile elutasította azzal az indokkal, hogy nem kezelte az érintett személyes adatait. Az érintett bírósághoz fordult.
A bíróság ideiglenes határozatában úgy rendelkezett, hogy a T-Mobile megsértette a GDPR 15. cikkét, mivel minden anonimizálási folyamat legalább a kezdeti szakaszban személyes adatok kezelésével jár, ezért a T-Mobile-nak meg kell jelölnie a kezelt személyes adatok pontos kategóriáit és eredetüket.

A bíróság – tartva magát az ideiglenes határozatához – megállapította, hogy a T-Mobile nem nyújtott elegendő tájékoztatást az automatizált döntéshozatalról és a profilalkotásról (GDPR 15. cikk (1) bekezdés h) pontja) és kötelezte, hogy két hónapon belül tájékoztassa az érintettet az automatizált döntéshozatal és profilalkotás létezéséről, valamint ismertesse a mögöttes okot, az adatkezelés jelentőségét és várható következményeit az érintett számára.[331]

- ✓ ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a GDPR 46. cikke szerinti megfelelő garanciákról.

A hozzáférés jogát csak úgy tudják az érintettek gyakorolni, ha tudomásuk van arról, hogy az adataikat kezeljük, vagy legalább is kezelhetjük. Ideális esetben a GDPR az érintettek tájékoztatására vonatkozó előírásait teljesítve az adatkezelők adnak információt az adataik kezeléséről, kevésbé ideális esetben „fülesből", pletykák alapján esetleg rossz tapasztalatok vagy kiterjedt magánnyomozás eredményeképpen tudják meg, hogy egy adott adatkezelő kezeli a személyes adataikat.

Például: az érintett vesz egy kütyüt, amely segítségével a macskájának távoli eléréssel piros lézeres pontot tud vetíteni és 360 fokos kamerával nyomon is tudja követni a messzeségből, ennek hogyan örül a kedvence, sőt beszélhet hozzá és jutalomfalatot is dobhat neki. Az ilyen készülék vásárlójának lehetőséget kell adni arra, hogy megtudja:

- ✓ *milyen biztonsági rendszerek védik az eszközt és az alkalmazást (azaz hogyan lehet megakadályozni, hogy más is kukkolja a macskát és vele együtt a lakás és a család kamerával befogott részét);*
- ✓ *ki kezeli az adatokat és mire használja azokat (macska kaja-gyártók, macska-kutatók, marketingesek, nemzetbiztonsági szolgálat, távol-keleti fejlesztők stb.);*
- ✓ *hol és meddig vannak tárolva ezek az adatok;*

[331] ECLI:NL:RBOBR:2022:3257, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBOBR:2022:3257&showbutton=true&keyword=avg, utolsó letöltés: 2022. 08. 18.

- ✓ *milyen garanciák vannak arra, hogy se a macska, se pedig a család tagjai ne váljanak youtube/TikTok (és egyéb video platformok) sztárjaivá úgy, hogy az nem állt szándékukban.*

Adatkezelőként az adatkezelés tárgyát képező személyes adatok másolatát – erre irányuló kérés esetén – az érintett rendelkezésére kell bocsátanunk, azonban a másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A GDPR 12. cikk (2) bekezdése előírja a Kérelmezettnek, hogy segítse elő az érintetti jogok gyakorlását. Ezen rendelkezés szerint az adatkezelő csak akkor tagadhatja meg az érintetti jog gyakorlására irányuló kérelem teljesítését, ha bizonyítja, hogy az érintettet nem áll módjában azonosítani. A GDPR rendelkezései szerint tehát az érintetti kérelem teljesítését – a személyazonosításon kívül – nem lehet különféle feltételek teljesítéséhez kötni, tehát ez alapján nem lehet arra kényszeríteni, hogy az átvétel tényét bizonyító irat aláírásán kívül bármivel kapcsolatos nyilatkozatot tegyen. Az pedig, hogy a személyes adatokat tartalmazó másolat nem használható fel például hatósági eljárás kezdeményezésére, vagy esetlegesen bírósági eljárásban, ellentétes nem csak a GDPR rendelkezéseivel, hanem hatósági és bírósági eljárási szabályokkal, tehát az Ákr.[332] *és a polgári perrendtartásról szóló 2016. évi CXXX. törvény bizonyítással kapcsolatos rendelkezéseivel is.”*[333]

A kérelem teljesítésének határideje a kérelem beérkezésétől számított egy hónap, szükség esetén – figyelembe véve a kérelem összetettségét és a kérelmek számát – ezt a határidőt további két hónappal meghosszabbíthatjuk.[334]

A görög adatvédelmi hatóság (HDPA) gyakorlatából

A HDPA 20 ezer eurós bírságot szabott ki a MZN HELLAS A.E. sportszergyártó vállalatra jogszerűtlen reklámcélú kommunikáció és személyes adatok törlésére irányuló kérelemre adott válasz elmulasztása miatt.

A panaszos kéretlen kommunikáció miatt nyújtott be panaszt az adatvédelmi hatósághoz, ugyanis a vállalat promóciós SMS-t küldött neki annak ellenére, hogy az egyértelműen és kifejezetten kifejezte elutasítását egy e-mailben, és annak ellenére, hogy kérte adatai törlését is. A vállalat azt állította, hogy egyik alkalmazottja hibájából nem törölték a panaszos adatait a szervereikről, illetve az érintettnek nem kellett volna kapcsolatba lépnie a vállalat ügyfélszolgálatával, hogy kérje adatai törlését, hanem ehelyett a kapott SMS-ben szereplő lemondási lehetőséget kellett volna használnia.

[332] az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (Ákr.)
[333] NAIH-55-11/2022. https://naih.hu/hatarozatok-vegzesek/file/540-uzleti-titokra-valo-hivatkozassal-hanganyag-korlatozott-felhasznalhatosaggal-torteno-rendelkezesre-bocsatasa, utolsó letöltés: 2022. 07. 28.
[334] GDPR 12. cikk (3) bekezdés

A HDPA megállapította, hogy a panaszos kifejezetten kérte adatainak törlését. Az a tény, hogy nem használta az opt-out űrlapot (azaz az SMS-ben megadott lemondási lehetőséget), nem befolyásolja a kérelme érvényességét.[335]

Az érintetti kérelmeket mindig a tartalmuk alapján kell elbírálnunk, nem pedig a címük alapján. Azaz, ha az érintett nem a GDPR szakkifejezéseit használja, attól fel kell ismernünk azt, hogy érintetti kérelemmel állunk szemben, arra válaszolnunk kell és nem lepődhetünk meg azon, hogy az esetek többségében az „érintetti kérelem" vagy a „hozzáférési kérelem" szavak egyáltalán nem szerepelnek a megkeresésben. Nekünk, adatkezelőnek az a feladatunk, hogy a kérelem tartalma alapján kitaláljuk, valójában mit szeretne az érintett és azt sem mondhatjuk, hogy egyszerre csak egy érintetti joggal élhet, valamint nem keverheti össze az adatvédelmi és fogyasztóvédelmi igényeit akár egy többszörösen bővített mondaton belül is.

Az érintetti kérelemben előfordulhatnak az alábbi mondatok

- ✓ *„ki és miért mondta meg a feleségemnek, hogy mennyi a fizetésem?"*
- ✓ *„honnan tudták meg, hogy van még egy gyerekem?"*
- ✓ *„miért küldték már megint rossz címre a levelemet? Honnan veszik, hogy ott lakom?"*
- ✓ *„láthatnám azt a felvételt, amin elesek?"*
- ✓ *„megmutatnák nekem azt a felvételt, amin látszik, hogy tízezressel vagy húszezressel fizettem?"*
- ✓ *„hogyan lettem adóstárs, ha nem vettem fel hitelt?"*
- ✓ *„szeretnék kérni egy másolatot a bizonyítványomról másolatáról"!*

Hogyan ismerhetjük fel az érintetti kérelmet és mi a teendőnk?

- ✓ Figyelmes olvasással/értő hallgatással kell kibogoznunk, hogy a kérelem benyújtója valójában mit akar, mert egyáltalán nem biztos, hogy azt, amire elsőre gondolunk.
- ✓ Nem hagyhatunk figyelmen kívül egyetlen érintetti kérelmet sem, bármennyire is furának vagy indokolatlannak, netalán értelmetlennek, abszurdnak vagy durvának tűnik az számunkra.
- ✓ Az érintett jogának érvényesülése nem lehet a mi kegyünk/jószándékunk vagy éppen kedélyállapotunk függvénye, azt a GDPR biztosítja az érintett számára és a figyelmen kívül hagyással olyan alapdokumentumokban foglalt jogokat sértünk, mint az Alapjogi Charta, illetve az Alaptörvényünk.
- ✓ Nem szabad elfelejtkeznünk a panaszhoz való jogáról sem, azaz arról, hogy minden érintettnek, életkorától és társadalmi státuszától függetlenül joga van a felügyeleti hatósághoz benyújtott panaszhoz és bírósági út igénybevételéhez amennyiben úgy érzi, jogait sérelem érte. Erről a jogáról pedig tájékoztatnunk kell az érintettet akkor is, ha egyébként erről mélyen szeretnénk hallgatni.

A spanyol adatvédelmi hatóság (AEDP) gyakorlatából

Az AEDP 170 ezer eurós bírságot szabott ki Spanyolország legnagyobb szupermarketláncára, mert megsértette a GDPR 12. és 15. cikkét, mivel nem

[335] HDPA (Greece) – 13-/2021, https://www.dpa.gr/sites/default/files/2021-04/13_2021anonym.pdf, utolsó letöltés 2022. 07. 23.

válaszolt az érintett hozzáférési kérelmére, valamint a GDPR 6. cikket, mivel jogalap nélkül törölte a videofelvételeket.

Az adatkezelő, a MERCADONA S.A. Spanyolország legnagyobb szupermarketlánca. Az érintett balesetet szenvedett az adatkezelő egyik üzletében, és ezt az adatkezelő videokamerával rögzítette. Az érintett az adatkezelővel szembeni kártérítési igénye érvényesítésének céljából az adatkezelő által biztosított online kapcsolatfelvételi űrlapon keresztül hozzáférést kért a balesetről készült felvételekhez. Az érintett még aznap automatikus választ kapott az adatkezelőtől, hogy üzenetét fogadták. Ezt követően az érintett e-mailben panaszt is tett a baleset miatt. Ez az e-mail tartalmazta a nevét, e-mail címét, telefonszámát, a baleset leírását és az elszenvedett károkat is. Az adatkezelő erre az e-mailre válaszolva megadta az ügy hivatkozási számát.

Miután az adatkezelő több mint egy hónapig nem válaszolt a hozzáférési kérelemre, az érintett ügyvédje e-mailt küldött az adatkezelő adatvédelmi tisztviselőjének, aki azt válaszolta, hogy nem tud semmilyen hozzáférési kérelemről, a videofelvételeket pedig már törölték, mivel a vonatkozó spanyol jogszabály alapján a felvételeket a rögzítés után egy hónappal kötelesek törölni.

Az érintett panaszt nyújtott be az adatvédelmi hatósághoz.
Az AEDP vizsgálata során kiderült, hogy a hozzáférési kérelem emberi hiba miatt nem jutott el az adatvédelmi tisztviselőhöz. Az eljárás során az adatkezelő kártalanította az érintettet, aminek köszönhetően az érintett visszavonta az AEDP előtti panaszát. Az adatvédelmi hatóság azonban úgy döntött, hogy saját hatáskörben (hivatalból) folytatja a vizsgálatot.

Az AEDP álláspontja az ügyben:

- ✓ *a felek egyezsége, illetve az érintett panaszának visszavonása nem köti, illetve az érintett kártalanítása nem mentesíti az adatkezelőt a GDPR megsértéséből eredő felelőssége alól.*
- ✓ *az adatkezelő megsértette a GDPR 12. és a 15. cikket azzal, hogy nem válaszolt a hozzáférési kérelemre. Megállapította, hogy a vonatkozó jogszabály szerinti, a felvételek legkésőbb egy hónap elteltével történő törlésére vonatkozó kötelezettség ellentétes a GDPR-ban foglalt, a hozzáférési kérelem beérkezésétől számított legkésőbb egy hónapon belüli válaszadási kötelezettséggel, illetve a hozzáférési kérelem megválaszolására vonatkozó kötelezettség elsőbbséget élvez, mivel ellenkező esetben az adatkezelő bármikor megkerülhetné az érintett hozzáférési jogát a vonatkozó jogszabály szerinti törlési kötelezettségre való hivatkozással.*
- ✓ *az adatkezelő megsértette a GDPR 6. cikket, mivel jogalap nélkül törölte a videofelvételeket, valamint a GDPR 6. cikk (1) bekezdésében foglalt követelmények egyike sem teljesült. Az AEDP véleménye szerint az érintettnek a videofelvételek bizonyítékként való megszerzéséhez fűződő érdeke, amely a spanyol alkotmány által biztosított hatékony jogorvoslathoz való joga részét képezi, felülmúlta az adatvédelmi megfontolásokat, valamint az adatkezelő azon kötelezettségét, hogy a vonatkozó jogszabály értelmében egy hónapon belül törölje a felvételeket.*

Az AEDP érvelését azzal is alátámasztotta, hogy a GDPR 6. cikk (1) bekezdésének f) pontja alapján jogosult az adatkezelő jogosult a videofelvételeket egy hónapnál hosszabb ideig megőrizni annak érdekében, hogy megvédje magát egy keresettel szemben.

A bírság összegének meghatározásakor az AEDP súlyosbító tényezőként vette figyelembe többek között azt, hogy

- ✓ *az érintett nem tudta felhasználni a videofelvételeket az adatkezelővel szembeni követeléseinek érvényesítésére,*
- ✓ *az adatkezelő csak a törlést követően válaszolt,*
- ✓ *az érintettről készült képek érzékeny adatok voltak (bár nem a különleges kategóriába tartozó adatok).*

Ezen kívül az AEDP azt is megállapította, hogy az adatkezelő korábbi jogsértésének hiánya nem minősül enyhítő körülménynek, míg a korábbi jogsértések súlyosbító körülménynek minősülnek a GDPR 83. cikke (2) bekezdésének e) pontja alapján.[336]

A GDPR alapján[337] az érintettek kérésére az adatkezelés tárgyát képező személyes adataik másolatát a rendelkezésünkre kell bocsátanunk kivéve akkor, ha a másolat igénylésére vonatkozó jog hátrányosan érintheti mások jogait és szabadságait. Természetesen ez nem azt jelenti, hogy ilyen esetekben automatikusan megtagadhatjuk az érintettek hozzáférését a saját személyes adataikhoz, hanem azt, hogy a mások adatait – lehetőség szerint – anonimmá (felismerhetetlenné) kell tennünk és úgy kell teljesítenünk a kérést.

Példák

- ✓ *az érintett olyan kamerafelvételről szeretne másolatot, amelyen nem csak ő látható, abban az esetben a felvételen szereplő egyéb érintettek képmása és cselekedete nem lehet automatikusan rajta a kiadott másolaton. Ebben az esetben ki kell takarni (elhomályosítani, kikockázni stb.) azokat a részeket, amelyek más érintettek érdekeit, jogait és szabadságait sértenék.*
- ✓ *az érintett olyan dokumentumról (például jegyzőkönyvről) szeretne másolatot, amelyben más személyek személyes adatai is szerepelnek. Ebben az esetben a személyes adatokat úgy kell eltávolítani, hogy azok felismerhetetlenné és helyreállíthatatlanná váljanak, például fekete csíkkal történő kitakarással.*

Az anonimizálás lényege, hogy visszafordíthatatlanná teszi az érintett azonosíthatatlanságát, ezért csak olyan technikát alkalmazhatunk a másolat kiadása során, amely tényleges azonosíthatatlanságot eredményez.

A GDPR alapján az érintettnek átadott első másolat általában ingyenes, a további másolatokért az adminisztratív költségeinken alapuló, észszerű mértékű díjat számíthatunk fel. Amennyiben az érintett elektronikus úton nyújtotta be a kérelmet,

[336] Procedimiento Nº: PS/00261/2020, https://www.aepd.es/es/documento/ps-00261-2020.pdf, utolsó letöltés: 2022. 07. 23.
[337] GDPR 12. cikk (3) és (4) bekezdés

abban az esetben az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátanunk, kivéve, ha azt az érintett másként kéri.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„(…) amennyiben a Kérelmező a személyes adataira vonatkozó információkról tájékozódott, úgy a Kötelezettnek – mint adatkezelőnek – akkor is fel kellett volna ismernie, hogy a kérelem a GDPR 15. cikke szerinti kérelem, ha a Kérelmező ezt nem tette volna ennyire egyértelművé, és akkor is a GDPR előírásai szerint kellett volna hozzáférést biztosítania a Kérelmező részére az általa kért információkhoz."[338]

Amennyiben nem teszünk intézkedéseket az érintett kérelme nyomán (azaz nem kívánjuk teljesíteni a kérelmet), késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatnunk kell az érintettet az intézkedésünk elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Amennyiben egy adatkezelő az érintett kérelmének teljesítését megtagadja, azaz annak nyomán semmilyen intézkedést nem hoz, így jelen esetben, amennyiben a Társaság úgy dönt, hogy az Ügyfél erre irányuló kérelme ellenére nem biztosít részére hozzáférést a róla készült kamerafelvételhez, úgy a GDPR 12. cikk (4) bekezdése alapján – a megtagadás indokainak részletezésén túl – köteles tájékoztatni őt arról, hogy az panaszt nyújthat be valamely felügyeleti hatóságnál (azaz jelen esetben a Hatóságnál), és élhet a bírósághoz fordulás jogával.

A jogorvoslathoz való jogról adott tájékoztatás azért különösen fontos az érintetti jogok kezelése során, mivel az adatvédelmi vonatkozású jogszabályokban kevésbé jártas személy nincs feltétlenül tisztában azzal, hogy mely területen ért korlátozás esetén mely hatósághoz fordulhat, így ezen ismeret hiányában az esetlegesen őt ért jogsértés, jogkorlátozás orvosolatlan marad. Ezt támasztja alá, hogy jelen esetben a bejelentő sem volt tisztában azzal, hogy az általa benyújtott kérelem adatvédelmi tárgyú érintetti joggyakorlásnak minősül, amely elutasítása esetén a Hatósághoz fordulhat. Mire a bejelentő a megfelelő jogorvoslati fórumról tudomást szerzett, addigra olyan hosszú idő telt el, hogy a róla készült kamerafelvétellel a Társaság már nem rendelkezett, így a Hatóság sem tudta kötelezni a Társaságot annak kiadására, így az érintett kérelmének megfelelő teljesítésére sem.

Fentiek alapján a Hatóság megállapította, hogy az Ügyfél hozzáférési kérelmének megtagadása során a Társaság nem a GDPR 12. cikk (4) bekezdése alapján járt el, így az Ügyfél hozzáférési kérelmének kezelése nem felelt meg a GDPR előírásainak."[339]

[338] NAIH/2020/4542/4

[339] NAIH/2020/2204/8. https://www.naih.hu/files/NAIH-2020-2204-8-hatarozat.pdf. Utolsó letöltés: 2022. 08. 27.

Mikor tagadhatjuk meg a kérelem teljesítését?

Amennyiben az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre

a) észszerű összegű díjat számíthatunk fel, vagy
b) megtagadhatjuk a kérelem alapján történő intézkedést.

A spanyol adatvédelmi hatóság (AEPD) gyakorlatából

Az AEPD megállapította, hogy az érintett hozzáférési kérelme visszaélésszerű volt, figyelembe véve az érintett és az adatkezelő közötti kapcsolat összefüggéseit és hátterét. Az érintett korábban más jogterületeken különböző követeléseket és pereket nyújtott be az adatkezelővel szemben.

Egy érintett panaszt nyújtott be az AEPD-hez egy olyan egyetem ellen, ahol különböző funkciókat töltött be (alkalmazott, fegyelmi eljárás alá vont alkalmazott, egyetemi hallgató, mesterszakos hallgató, kurzusasszisztens, közigazgatási eljárásokban érdekelt fél, közigazgatási eljárásokban résztvevő, kiválasztási eljárásokban résztvevő, peres fél, ellenérdekű fél stb.).

Az egyetem bizonyos információkat megadott az érintettnek, és kérte, hogy pontosítsa, milyen további információkra van szüksége. Az általános kérelem többi részét a GDPR 12. cikk (5) bekezdésére hivatkozva elutasították. Az egyetem azt állította, hogy igyekeztek időben válaszolni a kérelemre, de nem álltak rendelkezésre a szükséges erőforrások, tekintettel arra, hogy 26 ezer hallgatójuk van, 1122 oktató és kutató, valamint 521 adminisztratív alkalmazottjuk, 269 projekt munkatársuk; az oktatási struktúrájuk 7 kar, 2 iskola, 4 kutatóintézet, 27 tanszék, 33 szolgáltatási és adminisztratív egység, valamint 4 irányítási központ, és az érintettnek ezek közül sokban volt funkciója, mint például öregdiák, alkalmazott és peres fél is.

Az adatkezelő azt is kijelentette, hogy hatékonyabb rendszert vezet be az érintettek kérelmeinek kezelésére, valamint állította, hogy az érintett csak az egyetem működését próbálja megzavarni a különböző kérelmek, követelések és perek útján, az adatvédelemtől eltérő jogterületeken is.

Az érintett a pontosításra kérés után megismételte az eredeti kérelmét ugyanabban a formában, erre válaszul az adatkezelő ismét a GDPR 12. cikkének (5) bekezdésére hivatkozott, és kijelentette, hogy ez joggal való visszaélésnek minősül.
Az AEPD egyetértve az egyetemmel megállapította, hogy az érintett rosszhiszeműen, visszaélésszerűen gyakorolta jogait, valamint idézte a spanyol legfelsőbb bíróság véleményét, miszerint a joggal való visszaélés olyan jog gyakorlását jelenti, amely ugyan megfelel az ilyen jog formai követelményeinek, de a jogok lényegét, szellemiségét és természetét nem tartja tiszteletben.

Az AEPD dokumentumai azt tanúsították, hogy a panaszos rendellenesen gyakorolta jogát, mind mennyiségi (nem ez volt az első alkalom, hogy panaszt tett a válaszadóval szemben), mind minőségi szempontból (tekintettel a számos állítást

tartalmazó kérelmek benyújtására, amelyeket az érintett később nem tisztázott annak érdekében, hogy megkönnyítse azok teljesítését).[340]

Az érintetti kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása minket, adatkezelőt terhel, illetve a másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait – különösen a gyermekekkel kapcsolatos adatkezelések esetén kell fokozott figyelmet fordítanunk a gyermekek jogaira és szabadságaira.

A gyermekeket ugyanúgy megilleti a hozzáférés joga, mint a felnőtteket, éppen ezért az érettségétől és cselekvőképességétől függően szükség lehet a szülői felügyeleti jog gyakorlójának közreműködésére. Azonban az ilyen esetekben a gyermek mindenek felett álló érdekének kell a döntésünk középpontjában állnia, különösen akkor, ha a hozzáférési jogot a gyermek nevében egy felnőtt, például a szülői felügyeleti jog jogosultja gyakorolja.[341]

Adatkezelőként megfelelő intézkedéseket kell megtennünk annak érdekében, hogy elkerüljük a kiskorúak személyes adatainak illetéktelen személy részére történő felfedését.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A gyermekelhelyezési ügyekben, ahol a szülők között nemegyszer szélsőségesen negatív indulatok amúgy is jelentős pszichés megterhelést, lojalitáskonfliktust jelentenek a gyermek számára, a gyermeket is érintő pszichológusi vizsgálat önmagában is jelentős kockázattal, esetlegesen pszichés ártalmakkal, traumatizáló tényezőkkel járó beavatkozás. Optimális esetben ennek a kockázatát csökkenteni, kezelni tudja az igazságügyi szakértő. Ez azonban csak akkor biztosítható, ha a szakértői vizsgálat biztonságos légkörét meg tudja védeni a szakértő.

A pszichológiai vizsgálat anyagainak átadása azt jelentené, hogy a pszichológus olyan személynek adja át a gyermek biztonságát, pszichés integritását érintő adatokat, akinek se kompetenciája, se tapasztalata nincs, hogy felmérje az így előálló, a gyermeket további negatív hatásokkal károsító körülményeket.
A vizsgálati adatoknak a szakvéleménybe történő felhasználásakor a szakértő ügyel arra is, hogy pl. a gyermek explorációjából csak a kirendelés szempontjából lényeges azon elemek kerüljenek, melyek nem váltják ki az ellenérdekű szülő esetleges retorzióját a gyermekkel szemben."[342]

A másolat kiadásának korlátja lehet például az, ha a kért dokumentum üzleti titkot tartalmaz.

---

[340] Procedimiento Nº: E/00739/2021. https://www.aepd.es/es/documento/e-00739-2021.pdf, utolsó letöltés 2022. 08. 27.
[341] Guidelines 01/2022 on data subject rights – Right of access, https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf, utolsó letöltés: 2022. 08. 27.
[342] NAIH/2018/426/3/V. https://www.naih.hu/files/Adatved_allasfoglalas_NAIH-2018-426-szakertoi_kamara.pdf, utolsó letöltés: 2022. 08. 27.

Amennyiben megalapozott kétségeink vannak az érintetti kérelmet benyújtó természetes személy kilétével kapcsolatban, további, az érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérhetjük. Ezen észszerű intézkedéseket különösen az online szolgáltatásokkal és az online azonosítókkal összefüggésben szükséges megtennünk, azonban nem őrizhetjük meg a személyes adatokat kizárólag abból a célból, hogy a lehetséges kérelmeket meg tudjuk válaszolni.

A holland bírósági gyakorlatból

A holland Államtanács (Raad van State) úgy ítélte meg, hogy egy önkormányzat jogosan kérhette az érintettet, hogy a hozzáférési kérelem céljából azonosítsa magát érvényes személyazonosító igazolvány bemutatásával, vagy a kérelemnek egy online kormányzati személyazonosságkezelő portálon (DIGI-D) keresztül történő újbóli benyújtásával.

Egy érintett hozzáférési kérelmet nyújtott be egy önkormányzathoz olyan személyes adatokkal kapcsolatban, amelyek a lakcímén lévő hulladékgyűjtő konténerhez csatlakoztatott chipkártyaleolvasó által történő gyűjtésére, kezelésére és tárolására vonatkozó információkkal voltak kapcsolatban.

Válaszában az Önkormányzat arra kérte az érintettet, hogy 14 napon belül online és a DIGI-D segítségével aláírva nyújtsa be a kérelmét, vagy igazolja magát a városházán személyesen egy érvényes személyazonosító okmánnyal. Az Önkormányzat kifejtette, hogy a kérelem személyes adatokra vonatkozik, amelyeket nem adhat át nem megfelelő személynek, ezért fontos az érintett személyazonosságának megfelelő megállapítása. Amikor az érintett nem azonosította magát a kért módon, az Önkormányzat határozatban közölte, nem veszi figyelembe a kérelmet. Az érintett kifogást nyújtott be e határozat ellen, amelyet az Önkormányzat megalapozatlannak nyilvánított.

Az elsőfokú bíróság elutasította ezen határozat elleni fellebbezést, ezek után az érintett az Államtanácshoz fordult. Az Államtanács a fellebbezést megalapozatlannak nyilvánította:

- ✓ *az elsőfokú bíróság helyesen döntött úgy, hogy az Önkormányzatnak a GDPR 12. cikkének (6) bekezdése alapján oka volt kételkedni a fellebbező személyazonosságában.*
- ✓ *az a tény, hogy az Önkormányzat levelet küldött az érintett lakcímére, nem változtatott azon a tényen, hogy észszerűen kétségek merülhettek fel a személyazonosságával kapcsolatban. Igaz, hogy a szóban forgó címen csak az érintett lakik, de ez nem feltétlenül jelenti azt, hogy ő az a személy, aki a kérelmet benyújtotta. Más személyek is lakhatnak ezen a címen, akik nincsenek oda bejelentve, és akik az érintett nevében leveleket küldhetnek, azaz a lakcím nem ad automatikusan végleges választ a kérelmező személyazonosságára.*
- ✓ *az a tény, hogy az önkormányzat más eljárásokban nem kifogásolta azt, ahogyan az érintett kérelmeit intézte, nem befolyásolja azt a tényt, hogy ebben az esetben az Önkormányzatnak észszerű kétségei lehettek a személyazonosságát illetően. Az Önkormányzat helyesen állapította meg*

azt, hogy a GDPR értelmében fontos, hogy meggyőződjön a kérelmet benyújtó személyazonosságáról.

✓ *az érintett nem állította azt, hogy objektív akadálya lenne annak, hogy kérelmét a DIGI-D -n keresztül nyújtsa be, vagy hogy a városházán személyesen azonosítsa magát. Az elsőfokú bíróság ezért helyesen ítélte meg, hogy az Önkormányzat által kért információk arányosak voltak.*[343]

Helyesbítéshez való jog

A pontosság elvével szoros összefüggésben az érintett jogosult arra, hogy kérésére adatkezelőként indokolatlan késedelem nélkül helyesbítsük a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.[344]

A kiegészítés korlátja lehet az adattakarékosság elve, hiszen kiegészítés keretében sem kezelhetünk több adatot, mint amennyi az adatkezelési célunk eléréséhez szükséges.

A belga bírósági gyakorlatból

A brüsszeli fellebbviteli bíróság megállapította, hogy az érintetteknek a GDPR 16. cikke értelmében joguk van ahhoz, hogy nevüket helyesen írják le, amikor egy bank számítógépes rendszere kezeli azokat.

Egy bank ügyfele a GDPR 16. cikke alapján kérte a bankot, hogy nevének leírásakor a megfelelő írásjeleket használja. A bank azzal érvelt, hogy ez a jelenlegi számítógépes rendszerükben nem lehetséges, ezért nem tudják teljesíteni a kérést. Válaszul az ügyfél panaszt nyújtott be a belga adatvédelmi hatósághoz.
A DPA peres kamarája (Geschillenkamer) úgy döntött, hogy a bank érvelése a technikai lehetetlenséggel kapcsolatban nem elegendő és a banknak teljesítenie kell az ügyfél kérelmét.

A bank fellebbezett a határozat ellen és a fellebbezésében azzal érvelt, hogy a nagybetűk helyes írásjeleinek használatára nincs kötelezettség, és hogy az nem „személyes adat". Az adatvédelmi hatóság ezzel nem értett egyet, és azzal érvelt, hogy a GDPR 16. cikke fenntartás nélkül biztosítja az érintett számára azt a jogot, hogy késedelem nélkül kérje a helytelen személyes adatok helyesbítését, illetve a név helyes írásmódja a GDPR 4. cikkének (1) bekezdése szerint személyes adatnak minősül.

A brüsszeli fellebbviteli bíróság megállapította, hogy az érintettnek joga van ahhoz, hogy nevét helyesen írják, amikor azt a bank számítógépes rendszereiben kezelik. Az az állítás, hogy 2019-ben egy számítógépes rendszer kiigazítása a diakritikus betűk helyes kezelése érdekében több hónapos munkába kerülne és/vagy

[343] ECLI:NL:RVS:2021:1744, https://uitspraken.rechtspraak.nl/InzienDocument/GetPdf?ecli=ECLI%3ANL%3ARVS%3A2021%3A1744, utolsó letöltés: 2022. 08. 27.
[344] GDPR 16. cikk

többletköltséget jelentene a bank számára, még nem teszi lehetővé a bank számára, hogy figyelmen kívül hagyja az érintett jogait. Egy megfelelően működő pénzintézettől elvárható, hogy a számítástechnikai rendszerek megfeleljenek a jelenlegi szabványoknak, beleértve az emberek nevének helyesen leírásához való jogot is.[345]

Adatkezelőként minden olyan címzettet tájékoztatnunk kell valamennyi helyesbítésről, akivel, illetve amellyel a személyes adatot közöltük, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére adatkezelőként tájékoztatnunk kell e címzettekről.[346]

A holland bírósági gyakorlatból

A Midden-Nederlandi Kerületi Bíróság (Rb. Midden-Nederland) úgy határozott, hogy az orvosi szakvéleményben szereplő pontatlanságok kijavításához való jog nem teljesíthető úgy, hogy kiegészítő szakvéleményt állítanak ki anélkül, hogy azokat az eredeti dokumentumban ténylegesen kijavítanák.
A felperes az egészségügyi helyzetéről és a munkavégzés lehetőségeiről szóló szakvéleményekben szereplő ténybeli pontatlanságok miatt panaszkodott a foglalkoztatási támogatás odaítélésével összefüggésben. Kérte az e jelentésekben szereplő adatok helyesbítését. Az alperes azt állította, hogy a pontatlanságokat egy új szakvélemény kibocsátásával javította ki, de a felperes ezt nem találta elegendőnek, mivel a pontatlanságok az eredeti szakvéleményben maradtak, és a helyesbítéshez való jogának megsértésére hivatkozott.

A Bíróságnak azt kellett értékelnie, hogy az alperesnek milyen módon kellett volna elvégeznie a helyesbítést, figyelembe véve a műszaki lehetőségeit is.
A kerületi bíróság a GDPR 24. cikkére és a (78) preambulumbekezdésére hivatkozott, és arra a következtetésre jutott, hogy az adatkezelőknek meg kell tenniük a GDPR követelményeinek teljesítéséhez szükséges megfelelő technikai és szervezési intézkedéseket. Megállapította, hogy egy kiegészítő szakvélemény nem tekinthető elegendőnek a helyesbítéshez való jog teljesítéséhez. Az adatkezelőnek minden tőle telhetőt meg kell tennie annak biztosítása érdekében, hogy a szabályzatok és rendszerek összhangban legyenek a GDPR-ral, beleértve a pontatlanságok átlátható és egyértelműen felismerhető helyesbítését, amely nem csupán egy dokumentumnak az orvosi aktába történő egyszerű beillesztését jelenti.[347]

A helyesbítéshez való jog gyakorlását gyakran a hozzáférési joggal élés előzi meg, mivel ezen jog segítségével tudják meg az érintettek, hogy ami adatot kezelünk rólunk az hibás.

---

[345] Court of Appeal of Brussels – 2019/AR/1006, https://www.gegevensbeschermingsautoriteit.be/publications/arrest-van-9-oktober-2019-van-het-marktenhof.pdf, utolsó letöltés: 2022. 07. 23.
[346] GDPR 19. cikk
[347] ECLI:NL:RBMNE:2020:2226, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2020:2226&showbutton=true&keyword=AVG, utolsó letöltés 2022. 07. 23.

Például

- ✓ *téves lakcímet tartunk nyilván az érintettel kapcsolatban (hatodjára is átszámozta az önkormányzat az utcájában a házakat);*
- ✓ *megváltozott az érintett telefonszáma;*
- ✓ *aki felvette az érintett adatait az félreírta az adóazonosító jelét;*
- ✓ *az iskolai végzettségek és képesítések közül pont az maradt ki az adatbázisba bevitelből, ami az adott munkakör betöltéséhez szükséges.*

Egyes adatkezelések esetében – az adatkezelés sajátosságaira tekintettel – a helyesbítés-hez való jog kizárt (pl. kamerás adatkezelések, nyers egészségügyi adatok, biometrikus adatok stb.).

Előfordulhat, hogy az érintett helyesbítés iránti kérelme önmagában nem elegendő és megköveteljük az érintettől az állítólagos valótlanság bizonyítását. Ez az igényünk azonban nem róhat aránytalanul nagy bizonyítási terhet az érintettre és nem akadályozhatja meg abban, hogy az adatai helyesbítését kérje. Különösen igaz ez arra az esetre, amikor olyan adatbázisból szeretnénk bizonyítékot szereztetni az érintettel, amely az átlagos polgárok számára elérhetetlen.

Például

- ✓ *az érintett egy adatbázisból megtudja, hogy állítólag tagja egy titkos társaságnak. Vajon hogyan szerezhet igazolást ettől a szervezettől arról, hogy mégsem a tagjai?*
- ✓ *az érintett megtudja, hogy egykori titkos ügynökként/besúgóként tartják nyilván. Hogyan tudja hitelt érdemlően bebizonyítani, hogy soha nem volt titkos ügynök/besúgó?*

Az említett két példában az érintett szempontjából az adatkezelés hibás adatot tartalmaz, a helyesbítés pedig alapvető érdeke és joga, a helytelen adat pedig akár komoly következményekkel is járhat számára (hátrány a szociális életében, jó hírnevének sérelme, privát vagy szakmai életének válsága stb.).

A nem helyes / nem pontos személyes adat is személyes adat és ugyanúgy vonatkoznak rá az adatvédelemmel kapcsolatos jogszabályok, mintha az helyes /pontos személyes adat lenne.

A törléshez való jog – avagy az elfeledtetés joga

Az érintett jogosult arra, hogy kérésére indokolatlan késedelem nélkül töröljük a rá vonatkozó személyes adatokat, illetve adatkezelőként kötelesek vagyunk arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül töröljük, ha az alábbi indokok valamelyike fennáll:[348]

a) a személyes adatokra már nincs szükségünk abból a célból, amelyből azokat gyűjtöttük vagy más módon kezeltük
b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja

[348] GDPR 17. cikk

c) az érintett a GDPR 21. cikk (1) bekezdése alapján tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a 21. cikk (2) bekezdése alapján tiltakozik az adatkezelés ellen
d) a személyes adatokat jogellenesen kezeltük
e) a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölnünk kell
f) a személyes adatok gyűjtésére információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Tekintettel arra, hogy a törölni kért adat kezelését a Kötelezett számára törvény nem írja elő, továbbá az (…) megfelelő érdekmérlegelés hiányában az általános adatvédelmi rendelet 6. cikk (1) bekezdés f) pontja alapján sem kezelhető, a Kötelezett azzal, hogy a Kérelmező kérelmének nem tett eleget, megsértette az általános adatvédelmi rendelet 17. cikk (1) bekezdését, nem biztosította a Kérelmező törléshez való jogának érvényesülését.”[349]

Amennyiben nyilvánosságra hoztuk a személyes adatot és azt törölni vagyunk kötelesek, az elérhető technológia és a megvalósítás költségeinek figyelembevételével meg kell tennünk az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassuk az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

Személyes adatok keresőmotorok találati listájából történő eltávolíttatása

Az EUB 2014. május 13-ai ítéletében tisztázta a keresőmotorok és az adatvédelmi jog kapcsolatát és megállapította, hogy a felhasználók bizonyos feltételek mellett kérhetik a keresőmotorokat, hogy a nevükre történő keresések eredménylistájából töröljenek bizonyos, a magánéletüket érintő információkra mutató linkeket. Amennyiben egy keresőmotor elutasítja az ilyen törlési kérelmet, az érintett az adatvédelmi hatóságokhoz vagy az illetékes igazságügyi hatósághoz fordulhatnak.
Az EUB azt is kimondta, hogy a találati listáról eltávolításának joga *„főszabály szerint nemcsak a keresőmotor működtetőjének gazdasági érdekét előzik meg, hanem a nyilvánosság ahhoz fűződő érdekét is, hogy az e személy nevére vonatkozó keresés során meg lehessen találni az említett információt”*.[350] Van azonban kivétel ezen általános szabály alól, például „*ha valamilyen sajátos okból kifolyólag, például az érintett közéletben játszott szerepe folytán […] az [érintett] alapvető jogaiba való beavatkozást igazolja az említett nyilvánosság ahhoz fűződő nyomós érdeke, hogy [a kérdéses információhoz] hozzá lehessen férni azáltal, hogy az szerepel a találati listán”*.[351]

[349] NAIH/2019/2526/2, Budapest, 2019. március 4. https://www.naih.hu/files/NAIH-2019-2526-2-H-hatarozat.pdf, utolsó letöltés 2022. 07. 23.
[350] C-131/12. sz. ügy, „Google Spain-ügy”, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:62012CJ0131&from=HU, utolsó letöltés: 2022.08.27
[351] C-131/12. sz. ügy, „Google Spain-ügy”, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:62012CJ0131&from=HU, utolsó letöltés: 2022.08.27

A 29. cikk szerinti adatvédelmi munkacsoport összeállította azon kritériumok listáját,[352] amelyeket a hatóságok értékelni tudják az elutasított törlési kérelmek miatti hatóságokhoz benyújtott panaszokat.

A 29. cikk szerinti adatvédelmi munkacsoport szempontjai:

1. A keresés találatok természetes személyhez, azaz egyénhez kapcsolódnak? A keresési találatok az érintett nevére történő keresés eredményeként jelentek meg?
2. Az érintettnek van közéleti szerepe? Az érintett közéleti személyiség?
3. Az érintett kiskorú?
4. Az adatok pontosak?
5. Az adatok lényegesek és nem túlzott mértékűek?
a. Az adatok az érintett munkával kapcsolatos életére vonatkoznak?
b. A keresési találat olyan információra mutat, ami állítólag a panaszossal szembeni gyűlöletbeszédnek/rágalmazásnak/becsületsértésnek vagy hasonló bűncselekménynek minősül a véleménynyilvánítás területén?
c. Egyértelmű, hogy az adatok az egyén személyes véleményét tükrözik, vagy ellenőrzött ténynek tűnnek?
6. Az információ különleges adatnak minősül?
7. Az adat naprakész? Az adat az adatkezelés céljához szükségesnél hosszabb ideig érhető el?
8. Az adatkezelés okoz kárt az érintettnek? Az adatnak aránytalanul hátrányos hatása van az érintett magánéletére?
9. A keresési találat olyan információra mutat, hogy az kockázatot jelent az érintettre?
10. Milyen összefüggésben tették közzé az információt?
a. A tartalmat az érintett önkéntesen hozta nyilvánosságra?
b. A tartalmat a nyilvánosságnak szánta? Az érintett észszerűen tudhatta, hogy a tartalom nyilvánosságra kerül?
11. Az eredeti tartalmat újságírási célokkal összefüggésben tették közzé?
12. Az adatok kiadójának van jogi lehetősége – vagy jogi kötelezettsége – arra, hogy a személyes adatokat nyilvánosságra hozza?
13. Az adatok bűncselekményre vonatkoznak?

Az Európai Adatvédelmi Testület (EDPB) gyakorlatából

„Az Európai Unió Bíróságának (a továbbiakban: Bíróság) 2014. május 13-i Costeja ítéletét[353] követően az érintett kérheti az online keresőprogram szolgáltatójától (a továbbiakban: keresőmotor-szolgáltató)[354], hogy töröljön egy

[352] Az Európai Unió Bíróságának a C-131/12 SZ., GOOGLE SPAIN AND INC KONTRA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) ÉS MARIO COSTEJA GONZÁLEZ ügyben hozott ítéletének végrehajtására vonatkozó iránymutatás, https://ec.europa.eu/newsroom/article29/items/667236, utolsó letöltés 2022. 08. 27. Elfogadás időpontja: 2014. november 26.
[353] A Bíróság 2014. május 13-i Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González ítélete, C-131/12.
[354] Beleértve az olyan internetes archívumokat, mint az archívum.org

vagy több internetes oldalra mutató linket a neve alapján végzett keresést követően megjelenített találati listáról. (...)

Ha az érintett eléri, hogy egy bizonyos tartalmat töröljenek a találati listáról, az azt eredményezi, hogy az adott tartalmat törlik az érintettre vonatkozó keresési találatok listájáról, amennyiben a keresés főszabály szerint az érintett nevén alapul. Ez a tartalom azonban más keresési feltételek mellett továbbra is elérhető lesz.

A találati listáról való törlés iránti kérelmek nem eredményezik a személyes adatok teljes törlését. A személyes adatokat ugyanis nem törlik sem a forrásweboldalról, sem a keresőmotor-szolgáltató indexéből és gyorsítótárából. Az érintett például kérheti, hogy a keresőmotor indexéből töröljék azon személyes adatait, amelyek valamely médiaorgánumtól – például újságcikkből – származnak. Ebben az esetben a személyes adatokra mutató link törölhető a keresőmotor indexéből; a szóban forgó cikk azonban továbbra is a médiaorgánum ellenőrzése alatt marad, valamint a nyilvánosság számára rendelkezésre áll és hozzáférhető marad, még akkor is, ha az alapvetően az érintett nevét tartalmazó lekérdezéseken alapuló keresési eredményekben már nem jelenik meg.

Mindazonáltal a keresőmotor-szolgáltatók általában véve nem mentesülnek a teljes törlés kötelezettsége alól. Néhány kivételes esetben tényleges és teljes törlést kell végrehajtaniuk indexeikben vagy gyorsítótáraikban. Abban az esetben például, ha a keresőmotor-szolgáltatók nem tartják tiszteletben az eredeti kiadó által teljesített robotok.txt kéréseket, teljes mértékben törölniük kell a tartalom URL-címét, szemben az elsősorban az érintett nevén alapuló, találati listáról való törléssel."[355]

Nem alkalmazandó a törléshez való jog, amennyiben az adatkezelés szükséges:

a) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából

A német bírósági gyakorlatból

A felperes fogorvos, és azt követelte, hogy az alperes, amely egy orvosok számára havi több mint hatmillió felhasználóval rendelkező értékelő portált üzemeltet, törölje az e portálon az ő hozzájárulása nélkül közzétett adatait. Az elsőfokú bíróság megállapította, hogy a felperes kérheti a személyes adatainak törlését, mivel az adatokat jogellenesen kezelték. Az alperes azt állította, hogy tevékenysége a [(153) preambulumbekezdéssel együttesen értelmezett GDPR 85. cikk] kivétel hatálya alá tartozik, valamint a véleménynyilvánítás és a tájékozódás szabadságához való jog, mint kivétel érvényes rá, mivel újságírói célú adatkezelési tevékenységet végez.

[355] Európai Adatvédelmi Testület 5/2019 iránymutatás az elfeledtetéshez való jog kritériumairól az általános adatvédelmi rendelet hatálya alá eső, keresőmotorokkal kapcsolatos ügyekben (1. rész), 2.0. változat, Elfogadás időpontja: 2020. július 7., 1. és 8-10. pont https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_hu.pdf, utolsó letöltés 2022. 07. 23.

A fellebbezés során a legfőbb kérdés az volt, hogy újságírói platformnak minősül-e egy olyan platform, amely bizonyos előnyöket biztosít a „prémium" listák számára?

A másodfokú bíróság különösen arra összpontosított, hogy az értékelő oldal „semleges információközvetítőnek" minősül-e azáltal, hogy „rejtett előnyöket" nyújt az ügyfeleknek, illetve a GDPR 17. cikkének (3) bekezdésében foglalt kivétel alkalmazható-e. A bíróság megvizsgálta az oldal különböző funkcióit és megállapította, hogy az oldal négy, általa működtetett funkció révén elhagyta a semleges információközvetítő szerepét, ezért nem tekinthető újságírói platformnak, azaz az orvost megilleti a törlés joga.[356]

b) a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából
c) a népegészségügy területét érintő közérdek alapján
d) közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben a törléshez való jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést
e) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Egy korábbi valóságshow szereplő a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (Hatóság) fordult adatvédelmi hatósági eljárás megindításának igényével, sérelmezve, hogy az egyik nagy internetes hírportál egy 2014. évben közzétett, az ő személyes adatait tartalmazó cikket a kérelme ellenére nem távolít el az oldaláról (a cikk arról ad számot, hogy a Kérelmező szerepelt legrosszabbul a szereplők saját maguk között tartott menetrendszerű szimpátia szavazásán.) A Kérelmező kijelentette, hogy a cikk negatív hatással van az életére, kifejezetten hátrányosan hat a szakmai karrierjére, amiatt már több állásajánlat kapcsán is elutasították.

A Hatóság megállapította, hogy a kifogásolt cikk az RTL Klub televízió csatornáján a 2014. évben futó Való Világ valóságshow 6. szériájának egyik történéséről szóló tájékoztató híradás, amely megfelel(t) a sajtószabadságról és a médiatartalmak alapvető szabályairól szóló 2010. évi CIV. törvény (Smtv.) szerinti tájékoztatási jogok teljesülését biztosító sajtótevékenységre vonatkozó előírásoknak. A sajtótartalom mellett megjelenített fénykép a csatornát üzemeltető Magyar RTL Televízió Zrt. által kiadott hivatalos sajtófotó, amelyet a televíziós társaság kifejezetten azzal a céllal adott közre és biztosított valamennyi sajtótermék részére, hogy a műsorral kapcsolatos híradásokban megfelelő képi illusztrációként szolgáljon.

[356] Oberlandesgericht Köln, 15 U 126/19. https://www.justiz.nrw.de/nrwe/olgs/koeln/j2019/15_U_126_19_Urteil_20191114.html, utolsó letöltés 2022. 07. 29.

A Hatóság megállapította azt is, hogy a cikk a panaszos nevét nem, csak a RTL Klub valóságshowjában használt „becenevét" (VV6 XY) tartalmazza, amely azonban közvetlen módon nem kapcsolható a panaszos jelenlegi szakmai karrierjéhez, illetve munkaerő-piaci helyzetéhez. A panaszos teljes nevére az érintett internetes hírportál nem ad ki keresési találatot. Ezzel ellentétben, a Google kereső motorja a VV6 XY kifejezés megadásának különféle módozataira több tízezer találatot jelez.

A panaszos a Hatósághoz érkezett kérelmében a cikk eltávolítását indítványozta. Az érintett személyes adatai törléshez való jogának érvényesíthetősége kivételeit az általános adatvédelmi rendelet 17. cikk (3) bekezdése rendezi. Ennek a) pontja értelmében a véleménynyilvánítás szabadsága és a tájékozódáshoz való jog a személyes adatokra vonatkozó törlési kérelem megtagadásának jogszerű eszközét jelentheti, tehát a személyes adatok további megőrzése jogszerűnek tekinthető, ha – többek között – az a véleménynyilvánítás és a tájékozódás szabadságához való jog gyakorlása céljából szükséges. Tehát az általános adatvédelmi rendelet 17. cikk (3) bekezdés a) pontja hivatott egyensúlyt teremteni az érintett törléshez való joga, a véleménynyilvánítás szabadsága és a tájékozódáshoz való jog gyakorlása között, ezzel biztosítva – többek között – a sajtószabadságot, valamint az internet szabadságát.

A Hatóság a fentiekre tekintettel elutasította a panaszos azon kérelmét is, amelyben a cikkben található személyes adatainak törlését kezdeményezte, ugyanis ezen információk eltávolítása a Hatóság álláspontja szerint csorbítaná a véleménynyilvánítás szabadságát és a tájékozódáshoz való jogot."[357]

Az azzal kapcsolatos bizonyítási teher, hogy az adatkezelésünk jogszerű, minket terhel, mivel adatkezelőként mi vagyunk a felelősek az adatkezelés jogszerűségéért. Ezen kívül az elszámoltathatóság elve alapján bármikor tudnunk kell bizonyítanunk, hogy az általunk végzett adatkezelésnek a jogalapja jogszerű. Amennyiben erre nem vagyunk képesek, meg kell szüntetnünk az adatkezelést.

Kutatásunk során a kérdőívek alapján a megkérdezett személyek saját adataik törlésével kapcsolatos álláspontjuk a következő:

- ✓ a megkérdezettek szerint jelenleg a gyakorlatban nem rendelkeznek kontrollal a személyes adataik tekintetében, mivel az adatok törlését fizikailag nem tudják ellenőrizni;
- ✓ jelenleg nincs olyan technológiai megoldás, ami lehetővé tenné a felhasználók számára azt, hogy saját adataikat személyesen töröljék egy harmadik fél informatikai rendszerében elhelyezett tárolón;
- ✓ a felhasználók gyakorlatilag nem hisznek abban, hogy a szolgáltatók a gyakorlatban ténylegesen törlik személyes adataikat. Jellemzően abban bíznak, hogy a jogszabályok és a bírságok elrettentő erővel bírnak az adatkezelés területén.

[357] Tájékoztató a NAIH/2020/842 sz. ügyben hozott határozatának tartalmáról, Budapest, 2020. március 30, https://naih.hu/hatarozatok-vegzesek?download=208:valosagshow-szereplojerol-szolo-internetes-cikk-torlesere-vonatkozo-kerelem-tajekoztato-a-naih-2020-842-sz-ugyben-hozott-hatarozatanak-tartalmarol, utolsó letöltés: 2022. 07. 23.

A holland bírósági gyakorlatból

Az amszterdami elsőfokú bíróság elutasította egy fogorvosnak (felperesnek) a Google-hoz intézett azon kérelmét, hogy távolítsa el azokat a keresési találatokat, amelyek a nevére való kereséskor az ő nevére mutattak. A bíróság úgy ítélte meg, hogy ebben az esetben a felperes magánélethez való jogába való beavatkozást az információhoz való hozzáféréshez fűződő nyomós közérdek igazolja.

A németországi felperes korábban Hollandiában praktizált, ahol be volt jegyezve az egészségügyi szakemberek nyilvántartásába. Az amszterdami és zwollei regionális egészségügyi fegyelmi tanács a kezelésekkel kapcsolatos panaszok után fegyelmi intézkedéseket rendelt el vele szemben. A felperes arra kérte a Google-t, hogy távolítson el minden olyan keresési eredményt, amely a nevére vagy a neve és a „fegyelmi" keresőszó kombinációjára való kereséskor az ő nevére hivatkozik. A Google néhányat eltávolított, a többit azonban megtagadta arra hivatkozva, hogy a GDPR 6. cikk (1) bekezdésének f) pontja szerint, a véleménynyilvánítás szabadságára és a nyilvánosság online információkereséshez fűződő érdekére hivatkozva jogos érdeke fűződik az adatkezeléshez. A felperes ezzel szemben azzal érvelt, hogy joga van az elfeledtetés jogához és az ő esetében az egymással ellentétes jogok és érdekek mérlegelése során az ő jogainak és érdekeinek kell előnyben részesülniük.

A bíróság megállapította, hogy bár az ítélkezési gyakorlatból következik, hogy a magánélethez és a személyes adatok védelméhez való jog az érdekek mérlegelése során elsőbbséget élvez az információszabadsághoz való joggal szemben, ebben az esetben a felperes magánélethez való jogába való beavatkozást az információhoz való hozzáféréshez fűződő nyomós közérdek igazolja. A bíróság rámutatott, hogy

- ✓ *a Google nem tehető felelőssé a szóban forgó weboldalak tartalmának pontosságáért, másrészt azonban az érdekmérlegelés során nem hagyhatja teljesen figyelmen kívül ezt a tartalmat.*
- ✓ *a felperes nem tudta bizonyítani, hogy ez a tartalom helytelen, irreleváns, túlzott vagy elavult lenne.*
- ✓ *a felperes közszereplőnek tekinthető, mivel megjelent a televízióban és bekapcsolódott az esztétikai fogászatról szóló nyilvános vitákba.*[358]

Az adatkezelés korlátozásához való jog

Az érintett jogosult arra, hogy kérésére korlátozzuk az adatkezelést, ha az alábbiak valamelyike teljesül:[359]

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy ellenőrizzük a személyes adatok pontosságát

b) az adatkezelés jogellenes és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását

[358] ECLI:NL:RBAMS:2019:9887, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:9887&showbutton=true&keyword=AV, utolsó letöltés: 2022. 07. 30.
[359] GDPR 18. cikk

c) adatkezelőként már nincs szükségünk a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy
d) az érintett a GDPR 21. cikk (1) bekezdése szerint tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Amennyiben az adatkezelés korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből kezelhetjük.

A német bírósági gyakorlatból

Egy vasúttársaság egyes vonatjaiba olyan videokamerákat telepített, amelyek a vonatok közlekedése során aktívak. A felvételeket 48 óra elteltével automatikusan törlik. Az érintett 2021. április 27-én felszállt az egyik ilyen vonatra, majd ugyanazon a napon e-mailben kérte az adatkezelőt, hogy adja át a videofelvételeket, és ennek érdekében ne törölje azokat. Az adatkezelő azonban a 48 órás törlési határidőn belül törölte az adatokat, ezért megtagadta a kért információk átadását az érintettnek.
A bíróság megállapította, hogy az automatikus törlés megakadályozása és az érintettről készült felvételek kiszűrése jelentős időt, költséget és munkaerőt igényelt volna az adatkezelőtől, különösen mivel az adatkezelő nem rendelkezik arcfelismerő szoftverrel. A bíróság indoklása szerint a GDPR 18. cikk (1) bekezdésének c) pontja a felek érdekeinek mérlegelését is megköveteli, és különösen a peres eljárás valószínűségét, az érintett követelések súlyát, valamint az érintett érdekeit is figyelembe kell venni.[360]

Adatkezelőként az érintettet, akinek a kérésére korlátoztuk az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatnunk kell. Ezen kívül minden olyan címzettet tájékoztatnunk kell az adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közöltük, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére tájékoztatnunk kell e címzettekről.

Példa

- ✓ *az érintett esetében téves TAJ szám van a rendszerünkben, ő ezt jelzi nekünk, mi pedig akkor helyesbítjük az adatot, amikor az érintett bemutatja nekünk a TAJ kártyáját bizonyítva, hogy mi a helyes szám.*
- ✓ *az érintett jelzi, hogy megváltozott a lakcíme, ám azt nem bizonyítja semmivel sem. A titkárságunk kéri, hogy mutassa be az új lakcímkártyáját és amíg ezt nem történik meg, addig nem írja át az adatot, csak megjelöli azt, hogy a régi címre még véletlenül se küldjenek ki semmit.*

[360] AG Pankow, Urteil vom 27.03.2022, Az. 4 C 199/21, https://rewis.io/service/pdf/urteile/prn-28-03-2022-4-c-19921.pdf, utolsó letöltés: 2022. 07. 23.

- ✓ *a kamerafelvételek tárolási időtartama lejár (azaz törölnünk kellene a felvételeket), de az érintett szeretné, ha nem törölnénk azokat a felvételeket, amelyekkel bizonyítani tudja, hogy ki, mikor, mivel és hogyan ment neki a kocsijának a cég belső, elektronikus megfigyelőrendszerrel megfigyelt parkolójában.*
- ✓ *az általunk üzemeltetett beléptető rendszer adatait már törölni szeretnénk, azonban az érintett kéri bizonyos személyes adatai megtartását, mivel ezekkel kívánja bizonyítani a rendőrségen, hogy az adott időpontban nem bankot rabolt, hanem éppen az irodájában tartózkodott és dolgozott.*
- ✓ *Az érintett szeretne töröltetni egy felvételt, ami szerinte előnytelen oldalról mutatja őt (a nyakába fújta a szoknyáját egy hirtelen széllökés), ám a felvétel olyan egyéb adatokat tartalmaz, ami miatt mindenképpen meg akarjuk azt tartani (két munkavállalónk éppen veri egymást ugyanezen a felvételen).*

Milyen módszerekkel korlátozhatjuk az adatkezelést? Például:

- ✓ a kiválasztott és korlátozott személyes adatokat egy másik rendszerbe ideiglenesen áthelyezzük;
- ✓ megszüntetjük a felhasználók (az adott rendszerhez felhatalmazottak) számára a hozzáférhetőségét a korlátozott személyes adatokhoz;
- ✓ a honlapról az ott közzétett adatokat ideiglenesen eltávolítjuk stb.

A tiltakozáshoz való jog

A GDPR alapján az érintettek jogosultak arra, hogy a saját helyzetükkel kapcsolatos okokból bármikor tiltakozzanak a személyes adataik jogos érdekre vagy közérdekre hivatkozó kezelése ellen, ideértve az ezen alapuló profilalkotást is. Ebben az esetben a tiltakozással érintett személyes adatokat nem kezelhetjük tovább kivéve, ha bizonyítjuk, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

A jogos érdeken alapuló adatkezelés esetén érdekmérlegelési tesztet kell készítenünk, ennek pedig részletesen tartalmaznia kell a kényszerítő erejű jogos okokat.
Ezen kívül az érintettek jogosultak arra is, hogy bármikor és térítésmentesen tiltakozzanak személyes adataik közvetlen üzletszerzés érdekében történő kezelése ellen. Erről a jogukról egyértelműen és minden más információtól elkülönítve kell tájékoztatnunk az érintetteket.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A jogos érdeken alapuló, továbbá az automatizált adatkezeléssel szembeni tiltakozás joga nem az adatkezelő döntésétől függ, annak biztosítására az Ügyfél köteles az általános adatvédelmi rendelet 21. cikke alapján is. A tiltakozási jog teljes hiánya miatt alapvetően a jelen ügyben mindenképpen fennáll az általános adatvédelmi rendelet 21. cikkének sérelme, de elvi szinten a Hatóság rögzíti, hogy az ügyfélmegtartási célú telefonos agitáció az ügyfélszerzéshez hasonlóan marketing célnak minősül, így ezzel kapcsolatban az általános adatvédelmi rendelet

21. cikk (2) bekezdése szerinti objektív tiltakozási jogot kell biztosítani az érintetteknek, az egyéb célok – minőségellenőrzés, belső hatékonyság növelés – tekintetében az általános adatvédelmi rendelet 21. cikk (1) bekezdése szerinti feltételes tiltakozási jog biztosítandó. (…)

(…) alapvetően hibás és elfogadhatatlan az Ügyfél azon érvelése, hogy eddig érintetti panasz nem érkezett a vizsgált adatkezeléssel kapcsolatban, ha arról az érintettek érdemben nem is szerezhettek tudomást."[361]

Kinek az érdeke az erősebb?

Az Európai Unió Bíróság álláspontja szerint az érintett jogai főszabályként megelőzik az adatkezelő gazdasági érdekeit a kérdéses információ jellegétől, valamint attól is függően, hogy az információ mennyire érzékeny az érintett személy privát szférája szempontjából, illetve, hogy a nyilvánosságnak milyen érdeke fűződik ezen információ megismeréséhez.

A belga adatvédelmi hatóság (APD/GBA) gyakorlatából

Az APD/GBA 7 500 eurós bírságot szabott ki egy vállalat ellen, amiért az felmondás után visszaállította az adatokat egy volt alkalmazott munkahelyi laptopján, és ezt követően megsértette az érintett hozzáférési, törlési, korlátozási és tiltakozási jogát. Az érintett az adatkezelő korábbi ügyvezető igazgatója volt, aki, amikor elbocsátották, mielőtt azt leadta volna törölte a munkahelyi laptopján lévő adatokat. Az érintett szerint csak a magánjellegű adatokat, például a magán e-mail postafiókját törölte, az adatkezelő azonban azt állította, hogy az összes adatot törölte. Ezért az adatkezelő visszaállította a laptopon korábban tárolt összes adatot (adatfeldolgozó igénybevételével), beleértve az érintett személyes adatait is. Miután az érintett tudomást szerzett a visszaállításról, megpróbált élni a tájékoztatáshoz, a törléshez és az adatkezelés korlátozásához, valamint a tiltakozáshoz való jogával, kéréseit azonban az adatkezelő nem teljesítette.

A belga adatvédelmi hatóság megállapította a GDPR rendelkezéseinek megsértését az adatkezelés jogalapjának részleges hiánya miatt és az érdekmérlegelési teszttel kapcsolatban is hiányosságokat talált. A hatóság szerint elbocsátás esetén – miután tájékoztatta az e-mail fiókok birtokosát és harmadik feleket az e-mail fiók lezárásának időpontjáról – a munkáltatónak törölnie kell az e-mail címet, amennyiben az személyes adatnak minősül (a munkavállaló nevét tartalmazza). Az e-mail fiók birtokosának lehetővé kell tennie a magánüzeneteinek szortírozását és személyes átvitelét. Ha a tartalom egy részét a vállalkozás zavartalan működésének biztosítása érdekében vissza kell állítani, ezt az elbocsátás előtt és a munkavállaló közreműködésével kell megtenni.

Az adatvédelmi hatóság megállapította a hozzáféréshez való jog, a törléshez való jog, az adatkezelés korlátozásához való jog és a tiltakozáshoz való jog sérelmét is.

[361] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: 2022. 07. 17.

Ezen kívül az adatkezelő megsértette a GDPR 28. cikkét is, mivel nem kötött adatfeldolgozási megállapodást az adatfeldolgozóval.[362]

A GDPR alapján a bizonyítási teher az adatkezelőt, azaz minket terhel, nekünk kell tudnunk felmutatni és igazolni az adatkezelés folytatását indokoló kényszerítő okokat.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Az Ügyfél döntése alapján a munkavállalóinak a hangja is elemzésre és értékelésre kerül, amelyet az Ügyfél (...) nyilatkozata alapján többek között teljesítménybérezésre is használnak. A munkavállaló érintettek esetén szintén kérdéses, hogy mennyi tényleges tiltakozási lehetőségük lenne a függelmi viszony miatt. Ezen körülményt szintén nem mérlegelte az Ügyfél. A munkavállalók tekintetében a szerződés teljesítésének ellenőrzése, a minőségbiztosítás – a munkajogi szabályokból is adódóan – adott körülmények között megalapozhat bizonyos jogos érdeket. Azonban ezen esetben is kiemelten fontos az alkalmasság és arányosság kérdése, amit többek között az Ügyfél saját (...) nyilatkozata is megkérdőjelez, valamint a garanciák megfelelő rendszere sem biztosított a függelmi viszonyban lévő, így egy harmadik személy érintettnél is kiszolgáltatottabb munkavállalók részére. A nem bizonyíthatóan hatékony és az önrendelkezési jogot mélyen és súlyosan korlátozó érzelem-elemzés a munkavállalók esetén sem támasztható alá észszerű módon. Mivel a munkavállalók esetén kifejezetten (...) munkahelyi teljesítményhez kötődő profilalkotás is történik, az erre vonatkozó szabályok és garanciák alapos elemzése is szükséges egy új technológiával történő adatkezelés előtt, amelyet az Ügyfél szintén nem tett meg az érdekmérlegelése során.”[363]

Hogyan tiltakozhatnak az érintettek?

Nincs formai megkötöttség, írásban, szóban, bárhogy.

Például

- ✓ *az érintett kérheti, hogy a számára kellemetlen kamerafelvételt töröljük le (saját lábában hasra esett a kamera látószögében, nyakába fújta a szél a szoknyáját és kilátszott a fehérneműje stb.);*
- ✓ *az érintett le akarja szedetni azt a faliújságra kiragasztott csapatépítős bulin készült csoportképet, amelyen véleménye szerint úgy néz ki, mint aki éppen begombázott, netalán úgy értékeli, túl nagy a feneke/hasa;*
- ✓ *az érintett felháborodik, amiért távollétében a személyes használatra kiadott szekrényét a főnöke kinyitatta;*
- ✓ *az érintett rosszallását fejezi ki amiatt, hogy megszondáztatta a főnöke.*

Az érintett tiltakozását törlési kérelemnek kell tekinteni.

[362] Numéro de dossier : DOS-2020-02892, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-46-2022.pdf, utolsó letöltés: 2022. 07. 24.
[363] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: 2022. 07. 17.

A tiltakozás azonban nem jelenti azt, hogy nekünk, mint adatkezelőnek azt feltétlen el kell fogadnunk. Bizonyíthatjuk, hogy a Munka törvénykönyve és egyéb vonatkozó jogszabályok alapján jogszerűen kértük meg a munkavállalót, hogy fújja meg a szondát (erőteljesen kacsázva, szemmel láthatóan ittas állapotban érkezett a hajnali munkakezdésre, veszélyeztetve ezzel saját és munkatársai biztonságát). A jogszerűségnek ebben az esetben alapvető feltétele, hogy

- ✓ *legyen az alkoholszonda használatára jogszerű, érvényes belső szabályzatunk (azaz a szabályzatunk megfelel a szükségesség-arányosság és a fokozatosság követelményének) és*
- ✓ *azt ismerjék a beosztottak, illetve*
- ✓ *az intézkedés megkezdése előtt tájékoztassuk – többek között – az ellenőrzés menetéről, a panasztételi lehetőségekről, valamint az adatkezeléssel kapcsolatos kérdésekről.*

Az adathordozhatósághoz való jog

Az adathordozhatósághoz való jogot a GDPR vezette be. Ez a jog támogatja az érintettek választását, rendelkezését, valamint tudatos magatartását és a célja az, hogy biztosítsa számukra a személyes adataik feletti ellenőrzést. Az érintettek ezt a jogot hívhatják segítségül például akkor, amikor az egyik banktól a másikhoz szeretnék migrál(tat)ni a személyes adataikat.

Mire jogosultak az érintettek az adathordozhatósághoz való joguk alapján?

Jogosultak arra, hogy a rájuk vonatkozó, saját maguk által az adatkezelő rendelkezésére bocsátott személyes adataikat tagolt, széles körben használt, géppel olvasható formátumban megkapják, továbbá jogosultak arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsák anélkül, hogy ezt akadályozná az adatkezelő, amennyiben

- ✓ az adatkezelés a hozzájárulásukon vagy szerződésen alapul és
- ✓ az adatkezelés automatizált módon történik.

A holland bíróság gyakorlatából

A PDF-fájlok nem minősülnek a GDRP 20. cikk alkalmazásában megfelelő formátumnak, mivel nem eléggé strukturáltak és leíró jellegűek az adatok újra felhasználásához.[364]

Az adathordozhatósághoz való jog alapján az érintetteknek joguk van arra, hogy

- ✓ a rájuk vonatkozó, az adatkezelő által kezelt személyes adataikat tagolt, széles körben használt, géppel olvasható és interoperábilis formátumban megkapják, valamint
- ✓ – amennyiben ez technikailag megvalósítható – a személyes adataikat az adatkezelők egymás között, akadályoztatás nélkül – közvetlenül továbbítsák.

[364] ECLI:NL:RBAMS:2021:1020, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1020, utolsó letöltés: 2022. 07. 24.

Amennyiben érdemben válaszolunk az érintett adathordozhatósági kérelmére, akkor az érintett utasításai szerint kell eljárnunk, azaz nem vagyunk felelősek a címzett adatvédelmi szabályoknak való megfelelőségéért, hiszen maga az érintett döntötte el, hogy kinek továbbítsuk a kérelmében megjelölt, adathordozhatóságban érintett adatokat, nem pedig mi.

Az adathordozhatósághoz való jog korlátja, hogy az nem érintheti hátrányosan mások jogait és szabadságait.

A holland bírósági gyakorlatból

Az Ola platform sofőrök a rájuk vonatkozó személyes adatok meghatározott formátumban történő továbbítását azért kérték, hogy ezeket az adatokat közvetlenül a WHO adatbázisába vigyék be elemzés céljából, a platformokon dolgozók tárgyalási pozíciójának javítása céljából.
A GDPR (68) preambulumbekezdése kimondja, hogy az adathordozhatósághoz való jog az érintettek saját adataik feletti ellenőrzésének megerősítését szolgálja. A bíróság szerint az Ola helyesen érvel azzal, hogy e jog fontos célja a másik szolgáltatóhoz való váltás megkönnyítése és az eredeti adatkezelőnél az úgynevezett „user lock-in"[365] megakadályozása. Ez azonban nem jelenti azt, hogy a kérelmezők tervezett célja – saját személyes adataik elemzése vagy saját céljaikra történő felhasználása – kizárható az adathordozhatósághoz való jogból.

A bíróság továbbá kimondta, hogy az adatkezelő (az Ola) megtagadhatja a hozzáférést, ha ez mások jogainak és szabadságainak védelme érdekében szükséges, ebben az összefüggésben maga az adatkezelő is „mások" alatt értendő. Ez a rendelkezés kivételt tartalmaz az átruházott jogok alól, ezért megszorítóan kell értelmezni. Azt, hogy egy konkrét esetben fennáll-e olyan ok, amely a kérelem korlátozásához vagy elutasításához vezethet, a bíróságnak kell eldöntenie az összes érintett érdek mérlegelését követően. E kivételes rendelkezés alkalmazásakor a tájékoztatási kötelezettség elvileg az adatkezelőt (jelen esetben az Ola-t) terheli.

Az adathordozhatóságra vonatkozó joggal kapcsolatban a bíróság arra a következtetésre jutott, hogy a GDPR 20. cikke nem vonja automatikusan maga után a személyes adatok CSV-fájlban vagy API segítségével történő átadásának kötelezettségét.[366]

[365] a felhasználók (érintettek) „foglyul ejtése", azaz a szolgáltatóváltás megnehezítése
[366] ECLI:NL:RBAMS:2021:1019, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1019&showbutton=true&keyword=AVG, utolsó letöltés: 2022. 07. 24.

AUTOMATIZÁLT DÖNTÉSHOZATAL ÉS PROFILALKOTÁS

Az automatizált döntéshozatal és a profilalkotás egyénekre gyakorolt hatása már az 1970-es évektől, az automatizálás és a számítógépek megjelenésétől kezdve a jogalkotók egyik fő problémája. Az aggályokat úgy kezelték, hogy a használatot jelentősen korlátozták és az érintettek számára jogokat biztosítottak. Az 1978-as francia adatvédelmi törvény például kifejezetten megtiltotta az automata döntéshozatal igénybevételét az emberi viselkedés értékelésével kapcsolatos olyan bírósági, közigazgatási vagy magánjellegű döntésekkel összefüggésben, amelyek az egyén személyiségének profilját vagy személyiségének meghatározását tartalmazzák, ezzel párhuzamosan az egyének számára biztosította a megismeréshez való jogot és az őket érintő automatizált adatkezelés által használt információk és érvelés megtámadásához való jogot.

Az 1995. évi adatvédelmi irányelv a francia törvényhez hasonló rendelkezést tartalmazott az automata döntéshozatallal kapcsolatban, a GDPR pedig ezt a rendelkezést egészítette ki, engedélyezve például a hozzájáruláson alapuló automata döntéshozatalt.

Az olasz adatvédelmi hatóság (Garante per la protezione dei dati personali, „Garante") gyakorlatából

A Garante megállapította –az adatvédelmi irányelv rendelkezéseit átültető olasz törvény alapján –, hogy egy adatkezelő, aki személyre szabott díjszabást kínált autómegosztó szolgáltatását használók számára az összegyűjtött szokásaik és jellemzőik alapján, az érintettek profilozását végezte. Az adatkezelő az eljárás során azzal érvelt, hogy nem történt a szolgáltatás felhasználóinak „kategorizálása", mivel a díjszámításhoz használt adatok nem kapcsolódtak állandó jelleggel az érintettekhez.

A Garante elutasította ezt az álláspontot és kijelentette, hogy ebben az esetben kétséget kizáróan
a) személyes adatok kezeléséről volt szó,
b) az adatkezelés kizárólag automatizált feldolgozáson alapult és
c) az egyének profiljának vagy személyiségének meghatározására, szokásainak, illetve fogyasztási választásának elemzésére irányult.

A 60 ezer eurós bírságot kiszabó döntést az adatkezelő megtámadta, ám azt az olasz legfelsőbb bíróság (Corte Suprema di Cassazione) helybenhagyta és úgy ítélte meg, hogy a személyes adatok algoritmuson keresztül történő feldolgozása egy személyre szabott díjszabás kiszámítása érdekében profilalkotásnak minősül még akkor is, ha az adatok nem az érintetthez köthetők, és nem is az adatkezelő tárolja azokat.[367]

[367] Ancora sul tema della profilazione dei dati personali [Cass. civ. Sez. VI – 2 Ord., 08 novembre 2021, n. 32411], https://dirittodiinternet.it/ancora-sul-tema-della-profilazione-dei-dati-personali-cass-civ-sez-vi-2-ord-08-novembre-2021-n-32411/, utolsó letöltés: 2022. 07. 24.

A GDPR alapján az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené. A profilalkotás a személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen ha

- ✓ a munkahelyi teljesítményhez,
- ✓ gazdasági helyzethez,
- ✓ egészségi állapothoz,
- ✓ személyes preferenciákhoz,
- ✓ érdeklődéshez,
- ✓ megbízhatósághoz,
- ✓ viselkedéshez,
- ✓ tartózkodási helyhez vagy
- ✓ mozgáshoz kapcsolódó jellemzők

elemzésére vagy előrejelzésére használjuk.[368]

Az olasz adatvédelmi hatóság (Garante per la protezione dei dati personali, „Garante") gyakorlatából

A hatóság a Foodinho (a GlovoApp23 leányvállalatának) vizsgálatakor több súlyos jogsértést is talált, különös tekintettel a munkavállalók adatainak kezelésére használt algoritmusokra. A vállalat – többek között – nem tájékoztatta megfelelően a munkavállalóit a rendszer működéséről és nem hajtott végre megfelelő biztosítékokat a futárok teljesítményének értékelésére használt algoritmikus eredmények pontosságának és igazságosságának biztosítására. Ezenfelül a vállalat nem rendelkezett olyan eljárásokkal, amelyekkel az érintettek érvényesíthették volna az emberi beavatkozáshoz, az álláspontjuk kifejezéséhez és az algoritmusok által hozott döntések megtámadására vonatkozó jogait ami – egyes esetekben – a futárok kizárását vonta maga után a munkára vonatkozó megbízásokból.

A Foodinho-t kötelezték a rendszer által használt adatok – a futárok és az ügyfélszolgálat közötti csevegések, e-mailek és telefonhívások, a 15 másodperces időközönkénti geolokáció, az útvonalak feltérképezése, a becsült és tényleges szállítási idő, a jelenlegi és korábbi megrendelések kezelésének részletei, az ügyfelektől és partnerektől érkező visszajelzések, a készülék akkumulátorának töltöttsége stb. – relevanciájának és pontosságának ellenőrzésére. Ennek célja többek között az volt, hogy minimálisra csökkentsék a hibák és torzítások kockázatát, amelyek – többek között – azt eredményezhetik, hogy bizonyos futárok esetében csökken a szállítási megbízások száma, vagy akár ki is zárnak egyes futárokat a platformról. A szóban forgó kockázat azon minősítési rendszerhez is kapcsolódik, amely egy matematikai képlet alkalmazásán alapul, amely büntetést ró ki azokra a futárokra, akik nem fogadják el azonnal a megrendeléseket, vagy elutasítják azokat, míg a megrendeléseket határidőre elfogadó vagy a legtöbb megrendelést kézbesítő futárokat előnyben részesíti. A minősítés figyelembe veszi például a teljesített megrendeléseket, és a kiadott megrendelés 30 másodpercen belüli elfogadását.

[368] GDPR 4. cikk 4. pont

A vállalatnak az ügyfelek és üzleti partnerek visszajelzései alapján intézkedéseket kell megállapítania a hírnév-mechanizmusok nem megfelelő és/vagy diszkriminatív alkalmazásának megakadályozására is.[369]

Ez nem alkalmazandó abban az esetben, ha a döntés:

a) az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges
b) meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít, vagy
c) az érintett kifejezett hozzájárulásán alapul.

Az a) és c) pontokban említett esetekben adatkezelőként kötelesek vagyunk megfelelő intézkedéseket tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek legalább azt a jogát, hogy az adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

Az a)–c) pontokban említett döntések nem alapulhatnak a személyes adatoknak a különleges kategóriáin, kivéve akkor, ha az adatkezelés kifejezett hozzájáruláson vagy az adatkezelés jelentős közérdek miatt szükséges és az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében megfelelő intézkedések megtételére került sor.[370]

Az olasz bírósági gyakorlatból

A Corte di Cassazione úgy ítélte meg, hogy a hozzájárulás nem érvényes, ha az algoritmus nem átlátható, mivel az érintett nem lehet valóban tudatában a személyes adatok kezeléséhez való hozzájárulás következményeinek anélkül, hogy pontosan tudná, hogyan fogják felhasználni azokat egy bizonyos döntés meghozatalához.

A bíróság arra a következtetésre jutott, hogy a hozzájárulás csak akkor érvényes, ha azt szabadon, kifejezetten és egyértelműen meghatározott kezelésre vonatkozóan fejezik ki. Egy olyan esetben, amikor egy rendszer személyes adatokat kezel az egyének hírnévprofiljának létrehozása és a megbízhatóság pontozása céljából, a „tájékozott beleegyezés" követelménye nem tekinthető teljesítettnek, ha az algoritmus végrehajtási sémája és azok az elemek, amelyekből az algoritmus áll, ismeretlenek, vagy nem ismerik az érintettek.[371]

[369] Ordinanza ingiunzione nei confronti di Foodinho s.r.l. – 10 giugno 2021 [9675440], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9675440 utolsó letöltés 2022. 07. 18.
[370] GDPR 22. cikk, 9. cikk (2) bekezdés a) és g) pont
[371] Civile Ord. Sez. 1 Num. 14381 Anno 2021, http://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snciv&id=./20210525/snciv@s10@a2021@n14381@tO.clean.pdf, utolsó letöltés: 2022. 07. 24.

Mi az a profilalkotás?

A profilalkotás olyan eljárás, amely egy sor statisztikai következtetést foglalhat magában és gyakran használjuk arra, hogy különböző forrásokból származó adatok felhasználásával előrejelzéseket készítsünk természetes személyekről oly módon, hogy az egyénről más, statisztikai szempontból hasonlónak tűnő személyek tulajdonságai alapján vonunk le következtetéseket.[372]

A mindennapjaik során számtalan olyan helyzetbe kerülünk, amikor profiloznak minket – szinte minden mobil applikáció ezt csinálja a tőlünk/rólunk szerzett adatok alapján-, de a wifis elektromos vízforralónk is sokkal többet tud rólunk, mint amennyit szeretnénk. Sőt, az általunk használt böngésző azt is tudja, hogy mit fogunk holnap csinálni és a preferenciáinkat (kereséseinket, kattintásainkat) felhasználva információs buborékban tart minket, azaz csak olyan „hírekkel" és reklámokkal traktál bennünket, amelyek az adott platform szerint érdekesek számunkra.

A profilalkotás három elemből áll:

- ✓ az adatkezelésünknek valamilyen formájú automatizált adatkezelésnek kell lennie
- ✓ személyes adatok tekintetében kell végeznünk és
- ✓ a profilalkotásunk célja egy természetes személy vagy személyek személyes jellemzőinek vagy viselkedési mintáik értékelése annak érdekében, hogy bizonyos kategóriába vagy csoportba soroljuk őket, elemezve vagy előrejelzéseket alkotva érdeklődési körről, képességről egy feladat végrehajtásáról vagy várható magatartásról.

A profilozás folyamatában három szakaszt különíthetünk el:

- ✓ adatgyűjtés,
- ✓ automatizált elemzés az összefüggések felismerésére és
- ✓ az összefüggések alkalmazása adott természetes személyre a jelenlegi vagy jövőbeli viselkedés jellemzőinek azonosítására.

Mi az az automatizált döntéshozatal?

Az automatizált döntéshozatal az a képességünk, hogy adatkezelőként technológiai eszközök segítségével, emberi beavatkozás nélkül hozzunk döntéseket.

Az automatizált döntéshozatal hatóköre eltérő a profilalkotástól, azonban részben át is fedheti a profilalkotást vagy eredhet magából a profilalkotásból is, a döntések pedig alapulhatnak bármilyen „származású" személyes adatokon, például:

- ✓ *közvetlenül az érintett természetes személyektől szerzett adatokon (például kérdőívre adott válaszok)*
- ✓ *természetes személyekről megfigyelés révén nyert adatokon (például alkalmazásban gyűjtött helymeghatározási adatok, gépjárművek*

[372] GDPR (71) preambulumbekezdés

sebességének mérése gyorshajtás detektálása és szankcionálása érdekében)

- ✓ *származtatott vagy kikövetkeztetett adatokon, például a természetes személy már korábban létrehozott profilján (pl. hitelminősítési pontszám alapján hitelfolyósítás engedélyezése vagy megtagadása), illetve*
- ✓ *a különböző módon beszerzett adatok összevetésével (különféle adatbrókerektől és saját adatgyűjtésekből szerzett adatok összevegyítésével összeállított profil).*

Az automatizált döntéseket meghozhatjuk profilalkotással vagy anélkül, és a profilalkotás is történhet automatizált döntéshozatal nélkül, a két eljárás azonban keveredhet is.

Az olasz adatvédelmi hatóság (Garante per la protezione dei dati personali, „Garante") gyakorlatából

A Garante 2,5 millió eurós bírságot szabott ki a Deliveroo Italy-ra, mert a futároknak szánt alkalmazás nem nyújtott átlátható tájékoztatást a munkaidő-beosztások kezeléséhez használt algoritmusokról. Ezenkívül az alkalmazás aránytalanul nagy mennyiségű adatot gyűjtött a futárokról, megsértve ezzel a jogszerűség, az átláthatóság, az adattakarékosság és a korlátozott tárolhatóság elvét.

A Deliveroo Italy tulajdonosa a Roofoods LTD brit vállalat, amelynek adatközpontja Írországban található, a két cég a futárok adatainak tekintetében közös adatkezelők. A vizsgálat indításának időpontjában a Deliveroo Italy-nak nyolcezer olyan futárja van, akik a Deliveroo futár alkalmazást használták, és a Roofoods gyűjtötte a velük kapcsolatos személyes és szerződéses adatokat, a fizetési adatokat, a kiszállításhoz használt járműre vonatkozó adatokat, valamint meghatározta, hogyan kezeli a futárok adatait. A Roofoods állítása alapján az olaszországi futárfoglalási rendszer a kritikus idősávokban való rendelkezésre álláson és a futár megbízhatóságán (azaz a lefoglalt műszakokban való tényleges részvételen vagy a műszak kezdete előtti lemondáson) alapul és az alkalmazás nyomon követi a futár megrendelésének kezelését is (a megrendelés elfogadásától a kiszállításig), valamint tizenkét másodpercenként nyomon követi a futár tartózkodási helyét.

A Roofoods azt állította, hogy a Deliveroo ügyfelei megfelelő tájékoztatást kaptak a róluk gyűjtött adatokról, és hogy az érintettekről gyűjtött adatok (például a földrajzi helyzet) szükségesek a szolgáltatáshoz. Azzal is érvelt, hogy a foglalási rendszer mögött álló algoritmusokra vonatkozó statisztikák az alkalmazás egy erre a célra szolgáló oldalán elérhetőek a futárok számára, és vasárnaponként minden egyes futár tájékoztatást kap a következő heti foglalási időpontokról.

A Garante megállapította, hogy

- ✓ *a Deliveroo nem nyújtott megfelelő tájékoztatást a futárok számára az algoritmusokról, és nem tartotta be az átláthatóság elvét.*
  A futárok számára biztosított adatkezelési tájékoztató nem tüntette fel a futárok földrajzi helyzetére vonatkozó adatok kezelésének konkrét

módszereit. A Garante kifejtette, hogy a helymegosztás különleges invazivitása szükségessé teszi, hogy az adatkezelő tájékoztatást adjon a földrajzi helyzet meghatározásának konkrét módszereiről és időzítéséről, illetve a földrajzi helyzet automatizált feldolgozása a GDPR 22. cikk szerinti profilalkotásnak minősül, ami fokozott tájékoztatási kötelezettséget tesz szükségessé. A Deliveroo nem nyújtott tájékoztatást az alkalmazott logikáról, valamint az ilyen profilalkotás jelentőségéről és várható következményeiről.

A társaság által e téren végzett profilalkotás valószínűleg jelentős hatást gyakorolt az érintett futárokra, amely abból állt, hogy bizonyos előre meghatározott idősávokban lehetővé tette vagy megtagadta a munkalehetőségekhez való hozzáférést, lehetőséget nyújtva a használatra vagy megtagadva azt. A rendszer úgy volt kialakítva, hogy a magasabb pontszámot elért futárokat előnyben részesítse a munkabeosztás kiválasztásában, illetve az alacsonyabb pontszámmal rendelkező futárokat büntette, bár a pontszámot lehetett csökkenteni azzal is, ha egyszerűen nem a megfelelő időben jelentkezett be a futár az alkalmazásba. Alapvetően nem voltak átláthatóak ezek a beosztási algoritmusok, amelyekről az adatkezelő az információkat nem tette nyilvánosan hozzáférhetővé.

- ✓ *a Deliveroo nem adott tájékoztatást az adatmegőrzési időtartamok meghatározásához használt kritériumokról, ami sérti a GDPR 13. cikkét. A társaság előírta, hogy a munkaviszony megszűnését követően 6 évig meg kell őrizni a különböző célokra gyűjtött, különböző típusú adatokat. Tekintettel arra, hogy a különböző típusú személyes adatok kezelésével kapcsolatos tényleges célok mindegyikéhez képest megfelelőnek ítélt megőrzési időt kell meghatározni, a társaság nem őrizheti meg egyszerűen az összes adatot homogén időtartamokra osztott blokkokban.*

  A Deliveroo az adattárolási gyakorlatával megsértette a GDPR azon rendelkezését, miszerint az adattárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. Az adatkezelőnek kötelessége, hogy biztosítsa, hogy a személyes adatok megőrzési ideje a szükséges minimumra korlátozódjon.
- ✓ *a Deliveroo félrevezető tájékoztatást nyújtott a futároknak az érintettként őket megillető jogokról, például azt sugallva, hogy Olaszországban tartózkodásuk ellenére az Egyesült Királyság adatvédelmi hatóságánál (ICO) tehetnek panaszt. Ily módon nem könnyítette meg a futárok számára a jogaik gyakorlását.*
- ✓ *a Deliveroo eleve és alapértelmezetten megsértette az adattakarékosság, integritás és bizalmas jelleg elvét. Az alkalmazás rendszerei úgy voltak konfigurálva, hogy a rendelés kezelésével kapcsolatos valamennyi adatot összegyűjtsenek és tároljanak, valamint lehetővé tegyék az arra felhatalmazott üzemeltetők számára, hogy egyszerű funkciókat adjanak át egyik rendszerből a másikba, ezáltal megosztva a különböző rendszerek között az összegyűjtött adatokat. A Deliveroo nem indokolta meg konkrétan, hogy miért van szükség mindezen adatgyűjtésre és adatmegosztásra a szolgáltatásai nyújtásához.*

A Deliveroo továbbá nem hozott megfelelő technikai és szervezési intézkedéseket az adatkezelés megfelelő biztonságának garantálása érdekében, megsértve ezzel a GDPR 32. cikkét, valamint nem végzett adatvédelmi hatásvizsgálatot, megsértve ezzel a 35. cikket. [373]

Adatkezelőként mikor célszerű automatizált döntéshozatalt és profilalkotást alkalmaznunk?

Akkor, amikor az ilyen típusú eljárások használata

- ✓ nagyobb következetességet/méltányosságot eredményezhet a döntéshozatali folyamatunkban, például ezzel a módszerrel csökkenthetjük az esetleges emberi hibák arányát, a diszkriminációt, a hatalommal való visszaélést, valamint a korrupciót,
- ✓ segítséget nyújthat nagy mennyiségű adat korrekt feldolgozásában és a döntés figyelembevételében („Big Data")
- ✓ csökkentheti annak kockázatát, hogy az ügyfeleink nem fizetnek (például hitelképességi referencia alkalmazása esetén)
- ✓ lehetővé teheti, hogy rövidebb idő alatt/hatékonyabban hozzunk döntéseket.

Példa:
egy bank dönthet úgy, hogy

- ✓ *az ember (ügyintéző, vezető stb.) dönt bizonyos típusú hitelek nyújtásáról, kizárólag automatizált eszközökkel létrehozott profil alapján*
- ✓ *az algoritmus dönt a hitelnyújtásról és ezt a döntést automatikusan, bármilyen előzetes és érdemi emberi értékelés (beavatkozás) nélkül megküldi az ügyfélnek.*

A profilalkotási és automatizált döntési folyamatnak azonban vannak árnyoldalai is:

- ✓ gyakran láthatatlan és túlságosan komplex az érintettek számára, hiszen adatkezelőként származtatott vagy következtetett adatokat hozunk létre a természetes személyekről, olyanokat, amelyeket nem az érintettek bocsátottak a rendelkezésünkre;
- ✓ a profilalkotás akár tisztességtelen is lehet (például a rendszerben található torzítások miatt);
- ✓ hátrányos megkülönböztetést eredményezhet, amelynek eredményeképpen például egyes fogyasztóknak kevésbé vonzó ajánlatokat kínálhatunk, mint másoknak;
- ✓ a felhasznált adatok minősége (pontossága) is befolyásolhatja a profilalkotást, illetve a döntést, további problémákat okozva az adatvédelemre vonatkozó jogszabályoknak megfelelősége terén.

A norvég adatvédelmi hatóság (Datatilsynet) gyakorlatából

Az adatvédelmi hatóság 2020 augusztusában közzétett közleményében a Nemzetközi Érettségi Irodát (IB) a diákok érdemjegyeinek korrekciójára szólította fel

[373] Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l. – 22 luglio 2021 [9685994], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994, utolsó letöltés 2022. 07. 24.

tisztességtelen profilalkotás miatt. Tekintettel a vizsgák törlésére a Covid19 járvány idején, az IB úgy döntött, hogy a diákok „iskolai kontextusát" és „korábbi adatait" figyelembe veszi az osztályozás során. Az adatvédelmi hatóság megállapította, hogy ez az eljárás sértette a tisztességesség elvét, és pontatlan osztályozáshoz vezetett, megsértve a pontossági elvét is.

A hatóság véleménye szerint az ilyen osztályozás nem tükrözi a tanulók egyéni tanulmányi szintjét és potenciálisan az általuk látogatott iskola alapján történő megkülönböztetéshez vezetett. Az adatvédelmi hatóság rámutatott az EDPB beépített és alapértelmezett adatvédelemre vonatkozó iránymutatásában meghatározott méltányossági kritériumokra is, amelyek szerint az adatok bármilyen kezelésének – beleértve a szóban forgóhoz hasonló profilalkotási eseteket is – megkülönböztetésmentesnek, etikusnak és átláthatónak kell lennie, és figyelembe kell vennie a hatalmi és információs egyensúlyt. Az adatvédelmi hatóság szerint az IB az osztályozási rendszere nem felelt meg a diákok azon észszerű elvárásainak, miszerint a jegyeik tükrözzék a tanulmányi eredményeiket, a befektetett munkájukat, valamint az elsajátított ismereteiket és készségeiket. Ezen túlmenően az IB osztályozási (profilalkotási) algoritmus logikája nem volt nyilvánosan ismert, és a szervezet nem volt hajlandó a modellről további magyarázatot adni sem az adatvédelmi hatóságnak, sem a diákoknak, megsértve ezzel az átláthatóság elvét is.[374]

Amennyiben adatkezelőként a saját vagy harmadik fél jogos érdekre hivatkozva kívánunk profilalkotásba vagy automatikus döntéshozatalba bocsátkozni, az érdekmérlegelési teszt végzése során figyelembe kell vennünk a releváns feltételeket a vonatkozó ajánlás alapján[375]:

- ✓ a profil részletességi szintje (tágan leírt csoportban profilozott érintett vagy szegmentált és szemcsés szinten célzott)
- ✓ a profil átfogó jellege (a profil az érintettnek csak egy kisebb jellemzőjét írja le vagy átfogóbb képet fest róla)
- ✓ a profilalkotás hatása (az érintettre gyakorolt hatás)
- ✓ a profilalkotási eljárás tisztességességét, megkülönböztetésmentességét és pontosságát biztosító garanciák (különös tekintettel a mesterséges intelligencia alkalmazására)
- ✓ profilok jövőbeli felhasználása vagy összekapcsolása
- ✓ a profilalkotás eredményezi-e a „sima" személyes adatok különleges személyes adattá válását (például egy lakcím alapján nemzetiségi hovatartozásra következtetés).

[374] Advance notification of order to rectify unfairly processed and incorrect personal data – International Baccalaureate Organization, https://www.datatilsynet.no/contentassets/04df776f85f64562945f1d261b4add1b/advance-notification-of-order-to-rectify-unfairly-processed-and-incorrect-personal-data.pdf, utolsó letöltés: 2022. 07. 24.

[375] WP251rev.01. 15. oldal

Egy tanulmányban[376] a szerzők arra a következtetésre jutottak, hogy a könnyen hozzáférhető digitális viselkedési nyilvántartások, így például a Facebook like-ok felhasználhatók arra, hogy automatikusan és pontosan megjósoljanak rendkívül érzékeny személyes tulajdonságokat, így többek között szexuális irányultság, etnikai hovatartozás, vallási és politikai nézetek, személyiségjegyek, intelligencia, boldogság, függőséget okozó szerek használata, szülői különélés, életkor és nem terén. Az elemzés során 58 ezer önkéntes Facebookon közzétett kedveléseit, részletes demográfiai profiljait, valamint számos pszichometriai teszt eredményét vizsgálták és a szerzők által javasolt modell

- ✓ *az esetek 88%-ában helyesen különböztette meg a homoszexuális és heteroszexuális férfiakat,*
- ✓ *az esetek 95%-ában az afroamerikaiakat és a kaukázusi származású amerikaiakat,*
- ✓ *az esetek 85%-ában a demokratákat és a republikánusokat,*
- ✓ *a „nyitottság" személyiségjegy esetében az előrejelzés pontossága megközelítette egy standard személyiségteszt pontosságát.*

A fokozott kockázatra tekintettel a GDPR alapján az érintett jogosult arra, hogy ne terjedjen ki rá olyan, kizárólag automatizált adatkezelésen alapuló – akár intézkedést is magában foglaló – döntés hatálya, amely a rá vonatkozó egyes személyes jellemzők kiértékelésén alapul, és amely rá nézve joghatással jár vagy őt hasonlóan jelentős mértékben érinti, mint például egy online hitelkérelem automatikus elutasítása vagy emberi beavatkozás nélkül folytatott online munkaerő-toborzás, és ilyen adatkezelésnek minősül a „profilalkotás" is.

Mikor érinti az adatkezelésünk jelentős mértékben az érintettet?
Akkor, ha az adatkezelésünk hatása kellően nagy vagy fontos ahhoz, hogy

- ✓ jelentősen befolyásolja az érintett természetes személyek körülményeit, viselkedését vagy választásait,
- ✓ hosszan tartó vagy tartós hatást gyakoroljon az érintettre vagy
- ✓ a legszélsőségesebb esetben természetes személyek kirekesztéséhez vagy hátrányos megkülönböztetéséhez vezessen.

Jelentős hatású döntés lehet például:

- ✓ *az érintett anyagi körülményeit befolyásoló döntések (pl. hitelre/ösztöndíjra jogosultság megállapítása, megkülönböztető árazás);*
- ✓ *olyan döntések, amelyek befolyásolják az egyén egészségügyi szolgáltatásokhoz való hozzáférését (pl. műtéti várólista);*
- ✓ *olyan döntések, amelyek megtagadnak valakitől egy foglalkoztatási lehetőséget (pl. pályázatok automatizált szűrése toborzás során), vagy valakit súlyos hátránynak tesznek ki (pl. nem kap segélyt);*

[376] Michael Kosinski, David Stilwell és Thore Graepel: A személyes vonások és jellemzők előrejelezhetők az
emberi viselkedésre vonatkozó digitális adatokból. A National Academy of Sciences of the United States of
America eljárásai, http://www.pnas.org/content/110/15/5802.full.pdf

- ✓ *olyan döntések, amely befolyásolják valakinek az oktatáshoz való hozzáférését (középiskolai vagy egyetemi felvételi).*[377]

A GDPR alapján tehát főszabályként általános tilalom vonatkozik a joghatással vagy hasonlóképpen jelentős hatással járó kizárólag automatizált egyedi döntéshozatalra, kivéve az ilyen típusú adatkezeléseken – ideértve profilalkotást is – alapuló döntéshozatalt, amennyiben

- ✓ azt olyan uniós vagy tagállami jog engedélyezi kifejezetten, amelynek hatálya alá az adatkezelő tartozik, például a csalások és az adócsalás nyomon követése, valamint megelőzése céljából, feltéve, hogy erre az uniós intézmények vagy a tagállami felügyeleti hatóságok szabályaival, előírásaival és ajánlásaival összhangban kerül sor, vagy
- ✓ az adatkezelő által nyújtott szolgáltatás biztonságának és megbízhatóságának a biztosítása érdekében, vagy
- ✓ ha arra valamely, az érintett és egy adatkezelő közötti szerződés megkötése vagy teljesítése érdekében van szükség, vagy
- ✓ ha az érintett ahhoz kifejezett hozzájárulását adta.

Különleges adatok esetében az előbbiekben felsorolt lehetőségek mellett[378] még meg kell felelnünk a különleges adatok kategóriájába tartozó adatok kezelésének feltételeinek is. Ebben az esetben két lehetőségünk van:

- ✓ az érintett kifejezett hozzájárulása[379]
- ✓ az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes
  adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.[380]

Az ilyen típusú adatkezelést csakis megfelelő garanciák mellett végezhetjük, amelybe beletartozik az érintett külön tájékoztatása és az ahhoz való joga, hogy emberi beavatkozást kérjen és kapjon, különösen, hogy

- ✓ kifejtse álláspontját,
- ✓ magyarázatot kapjon az ilyen értékelés alapján hozott döntésről és
- ✓ megtámadja a döntést.

Az ilyen intézkedés gyermekre nem vonatkozhat.
Az érintett szempontjából tekintve tisztességes és átlátható adatkezelés biztosítása érdekében – az adatkezelés konkrét körülményeinek figyelembevételével – ha adatkezelőként a profilalkotáshoz megfelelő matematikai és statisztikai eljárásokat alkalmazunk, olyan technikai és szervezési intézkedéseket kell bevezetnünk, amelyek

- ✓ biztosítják különösen az adatok pontatlanságát előidéző tényezők korrekcióját és a hibalehetőségek minimálisra csökkentését, továbbá

[377] WP251rev.01. 23. oldal
[378] GDPR 22. cikk (2) bekezdés
[379] GDPR 9. cikk (2) bekezdés a) pont
[380] GDPR 9. cikk (2) bekezdés g) pont

- ✓ a személyes adatok biztonságáról oly módon gondoskodik, amely az érintett érdekeit és jogait potenciálisan veszélyeztető tényezőket figyelembe veszi, és
- ✓ amely megakadályozza egyebek között az olyan hatások érvényesülését, amelyek a természetes személyek közötti hátrányos megkülönböztetést eredményeznek faji vagy etnikai származás, politikai vélemény, vallási vagy világnézeti meggyőződés, szakszervezeti tagság, genetikai vagy egészségi állapot, szexuális irányultság vagy nemi identitás alapján, illetve amelyek ilyen hatást kiváltó intézkedésekhez vezetnek.

Az érintettek jogai

A GDPR garantálja, hogy az érintettek jogosultak legyenek megtámadni az automatizált döntéshozatal, illetve a profilalkotás során hozott döntéseket és képesek legyenek vitatni az adatkezelő által használt adatok pontosságát, valamint a rájuk alkalmazott profil relevanciáját.

Adatkezelőként tájékoztatnunk kell az érintetteket az automatizált döntéshozatal tényéről, ideértve a profilalkotást is. A tájékoztatásunk nem szorítkozhat csak a tény közlésére, hanem érthető információkat kell biztosítanunk az érintettek számára az alkalmazott logikára és arra vonatkozóan is, hogy az ilyen adatkezelés az érintettre nézve milyen várható következményekkel jár.

Példa:

- ✓ *egy automatizált döntéshozatalt alkalmazó biztosítónak általános tájékoztatást kell adnia az algoritmus működésére, továbbá arra vonatkozóan, hogy az algoritmus mely tényezőit használja a biztosítási díj kiszámításához.*

Az érintettek hozzáférési jogának biztosítása keretében az adatkezelésre vonatkozó általános tájékoztatáson felül kötelesek vagyunk az érintett rendelkezésre bocsátani a profil kialakításához bemenetként felhasznált adatokat, továbbá hozzáférést kell biztosítanunk a profilra vonatkozó információhoz és arra vonatkozó részleteket is meg kell adnunk, hogy az érintettet mely szegmensekbe soroltuk.

A GDPR védelmet ad[381] számunkra az üzleti titkunk vagy szellemi tulajdonunk feltárása tekintetében, így a hozzáférés joga nem érintheti hátrányosan mások jogait és szabadságait, beleértve az üzleti titkokat vagy a szellemi tulajdont, és különösen a szoftverek védelmét biztosító szerzői jogokat. Azonban nem hivatkozhatunk az üzleti titkunk védelmére ürügyként csak azért, hogy megtagadjuk a hozzáférést vagy visszautasítsuk az érintett tájékoztatását.

A svéd adatvédelmi hatóság (IMY) gyakorlatából

Az IMY mintegy 750 ezer eurós bírságot szabott ki a Klarna Bank AB-re a GDPR átláthatósági követelményeinek többszörös megsértése miatt.

Az IMY megállapította – többek között –, hogy

[381] GDPR (63) preambulumbekezdés

- ✓ *2020 márciusa és júniusa közötti időszakban a bank nem nyújtott érdemi tájékoztatást a hitelkérelmekről való döntés, valamint a csalás vagy pénzmosás potenciális eseteinek felderítése céljából végzett minősített automata döntéshozatal indoklásáról, mibenlétéről és előrelátható következményeiről.*
- ✓ *a bank adatvédelmi tájékoztatója csak azt jelezte, hogy bizonyos típusú információkat felhasználnak az automatizált döntéshozatallal kapcsolatban (például kapcsolattartási, azonosító és pénzügyi információkat), de nem magyarázta el az ügyfeleknek, hogy mely körülmények lehetnek döntőek egy negatív hitelengedélyezési döntés meghozatalakor.*
- ✓ *nem volt egyértelmű, hogy a bank a saját belső pontozási modelljét használta-e, amely többek között belső és külső pénzügyi információkon alapult, illetve az sem, hogy a pénzügyi információk milyen típusú adatokat tartalmaznak, például más hitelezőkkel szembeni kötelezettségekre vonatkozó információkat.*

Az IMY véleménye szerint az automatizált hitelbírálati döntés mögött meghúzódó logikára vonatkozó érdemi tájékoztatás követelménye magában foglalja a belső pontozási modellel kapcsolatban döntő fontosságú adatkategóriák megjelölését, valamint az elutasító döntéshez – rendszerint – vezető körülmények lehetséges meglétét.[382]

Adatkezelőként ezen kívül kötelesek vagyunk megfelelő intézkedéseket tenni az érintettek jogainak, szabadságainak és jogos érdekeinek védelmére. Ez magában foglalja legalább az érintetteknek azt a jogát, hogy

- ✓ tőlünk (az adatkezelőtől) emberi beavatkozást kérjenek,
- ✓ álláspontjukat kifejezhessék és
- ✓ a személyes adataik automatizált kezelésén alapuló döntéssel szemben kifogást nyújtsanak be.

Ezen kívül minden intézkedést meg kell tennünk a profilalkotással járó adatpontatlansági tényezők kijavítására, a kockázatok, illetve hibák korlátozására és időszakosan értékelnünk illik az adatok és az alkalmazott algoritmusok minőségét is.

A spanyol adatvédelmi hatóság (AEPD) gyakorlatából

A hatóság az EDP Comercializadora S.A.U. energiaipari társasággal kapcsolatban megállapította, hogy a társaság – többek között – nem tájékoztatta megfelelően az érintetteket a marketingcélú profilalkotásról:

- ✓ *az ügyfelek nem kaptak megfelelő tájékoztatást személyes adataik kezeléséről az adatgyűjtéssel egyidejűleg (pl. telefonos vagy elektronikus szerződéskötéskor) többek között arról, hogy a társaság hogyan hozta létre a kereskedelmi profiljaikat, és hogy ennek (azaz a profil alapján hozott döntéseknek) milyen gyakorlati következményei vannak a számukra.*

[382] DI-2019-4062, https://www.imy.se/globalassets/dokument/beslut/2022/beslut-tillsyn-klarna.pdf, utolsó letöltés: 2022. 07. 24.

- ✓ *bár a társaság esetében a személyre szabott marketingkommunikáció küldése céljából végzett ügyfélprofilok létrehozása nem minősült a GDPR 22. cikk hatálya alá tartozó automata döntéshozatalnak, a profilalkotási tevékenységet végző adatkezelőknek ettől függetlenül átláthatónak kell lenniük az érintettek felé és tájékoztatniuk kell az érintetteket a profilalkotási gyakorlatukról, valamint arról, hogy hogyan élhetnek a profilalkotás elleni tiltakozáshoz való jogukkal.*

Az AEDP nem fogadta el a társaság azon érvelését, miszerint a profilalkotás valójában a személyre szabott marketingkommunikáció céljával függött össze és megállapította, hogy a hatósághoz benyújtott általános szerződési feltételekben a profilalkotás szerepel a személyes adatok felhasználásának céljai között.

Az AEDP 1,5 millió eurós bírságot szabott ki az adatkezelőre, ebből 1 millió eurót a tájékoztatáshoz való jog megsértése miatt.[383]

Tiltakozás joga

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a GDPR 6. cikk (1) bekezdésének e) vagy f) pontján alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben a személyes adatokat nem kezelhetjük tovább, kivéve, ha bizonyítjuk, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

Az érintett tiltakozása esetén mindig el kell végeznünk a mérlegelést az adatkezelő érdekei és az érintett tiltakozásának (személyes, szociális vagy szakmai okkal kapcsolatos) alapja között és

- ✓ *meg kell vizsgálnunk a profilalkotásunk jelentőségét a saját különös célkitűzéseink tekintetében*
- ✓ *meg kell vizsgálnunk a profilalkotás hatását az érintett érdekeire, jogaira és szabadságaira nézve (ezt a cél eléréséhez szükséges legkisebb mértékre kell korlátoznunk) valamint*
- ✓ *el kell végeznünk az érdekmérlegelést.*

A „szokásos" érdekmérlegelési teszthez képest ebben az esetben nem elegendő, ha egyszerűen csak azt bizonyítjuk, hogy a jogos érdekre vonatkozó korábbi elemzésünk helyes volt, hanem követelmény az is, hogy a jogos érdek kényszerítő legyen, azaz a jogszabály magasabb küszöböt határoz meg a tiltakozással szembeni elsőbbségre vonatkozóan.

Ha a személyes adatokat közvetlen üzletszerzés érdekében kezeljük,

[383] Procedimiento Nº: PS/00037/2020, https://www.aepd.es/es/documento/ps-00037-2020.pdfm utolsó letöltés: 2022. 07. 24.

- ✓ az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik
- ✓ ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatokat a továbbiakban e célból nem kezelhetjük.

Az érintett tiltakozással kapcsolatos jogaira legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívnunk a figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjelenítenünk.

Amennyiben a személyes adatokat tudományos, történelmi kutatási vagy statisztikai célból kezeljük, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozhasson a rá vonatkozó személyes adatok kezelése ellen, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükségünk.

KORLÁTOZÁSOK

A személyes adataink kezelésével kapcsolatos védelem alapvető jogunk, a GDPR pedig védi természetes személyként a jogainkat és szabadságainkat, különösen az adatvédelemhez való jogunkat. Az adatvédelem nem biztosítható a GDPR-ban meghatározott jogok és elvek betartása nélkül. Ezen jogok és kötelezettségek az adatvédelemhez való alapvető jog középpontjában állnak, az adatvédelemhez való alapvető jog bármilyen korlátozásának pedig figyelembe kell vennie az Európai Unió Alapjogi Chartájának 52. cikkét, mely szerint a Chartában elismert jogok és szabadságok gyakorlása csak a törvény által, és e jogok lényeges tartalmának tiszteletben tartásával korlátozható. Az arányosság elvére figyelemmel, korlátozásukra csak akkor és annyiban kerülhet sor, ha és amennyiben az elengedhetetlen és ténylegesen az Európai Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálja.

A GDPR „korlátozások" szakaszát (23. cikkét) a Charta 52. cikkében foglaltak szerint kell értelmeznünk. Ezen cikk alapján az uniós vagy tagállami jog alapján a GDPR egyes, az érintettek jogaira és az adatkezelők kötelezettségeire vonatkozó rendelkezéseinek alkalmazása az ott felsorolt helyzetekben korlátozható. A korlátozásokat úgy kell tekinteni, mint az általános szabály alóli kivételeket. A korlátozásokat minden esetben szűken kell értelmezni, csakis a kifejezetten meghatározott körülmények között és csak bizonyos feltételek teljesülése esetén alkalmazhatók. A jogalkotó szándékát az EDPB iránymutatása[384] segít értelmezni.

Az Európai Adatvédelmi Testület (EDPB) gyakorlatából

„A személyes adatok védelme még kivételes helyzetekben sem korlátozható teljes mértékben. Az általános adatvédelmi rendelet 23. cikke szerint minden rendkívüli intézkedés során fenn kell tartani, így hozzájárulva a demokrácia, a jogállamiság és az alapvető jogok átfogó értékeinek tiszteletben tartásához, amelyekre az Unió épül: a tagállamok által hozott minden intézkedésnek tiszteletben kell tartania a jog általános elveit, az alapvető jogok és szabadságok lényegét, és nem lehet visszafordíthatatlan, az adatkezelőknek és adatfeldolgozóknak pedig továbbra is meg kell felelniük az adatvédelmi szabályoknak.

Minden olyan esetben, amikor az uniós vagy tagállami jog lehetővé teszi az érintettek jogainak vagy az adatkezelők (ideértve a közös adatkezelőket is) és az adatfeldolgozók kötelezettségeinek korlátozását, meg kell jegyezni, hogy az általános adatvédelmi rendelet 5. cikkének (2) bekezdésében meghatározott elszámoltathatóság elve továbbra is alkalmazandó. Ez azt jelenti, hogy az adatkezelő felelős azért, és képesnek kell lennie arra, hogy bizonyítsa az érintettek felé, hogy megfelel az uniós adatvédelmi keretnek, beleértve az adataik feldolgozására vonatkozó elveket is."[385]

[384] EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 2.0 Adopted on 13 October 2021, https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf, utolsó letöltés 2022. 07. 25.

[385] EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 2.0

A GDPR 23. cikke alapján az adatkezelőre vagy az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel korlátozhatja a GDPR 12–22. cikkben és a 34. cikkben foglalt, valamint a 12–22. cikkben meghatározott jogokkal és kötelezettségekkel összhangban lévő rendelkezései tekintetében az 5. cikkben foglalt jogok és kötelezettségek hatályát, ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát, valamint az alábbiak védelméhez szükséges és arányos intézkedést egy demokratikus társadalomban:

a) nemzetbiztonság;
b) honvédelem;
c) közbiztonság;
d) bűncselekmények megelőzése, nyomozása, felderítése vagy a vádeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása, beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését;
e) az Unió vagy valamely tagállam egyéb fontos, általános közérdekű célkitűzései, különösen az Unió vagy valamely tagállam fontos gazdasági vagy pénzügyi érdeke, beleértve a monetáris, a költségvetési és az adózási kérdéseket, a népegészségügyet és a szociális biztonságot;
f) a bírói függetlenség és a bírósági eljárások védelme;
g) a szabályozott foglalkozások esetében az etikai vétségek megelőzése, kivizsgálása, felderítése és az ezekkel kapcsolatos eljárások lefolytatása;
h) az a)–e) és a g) pontban említett esetekben – akár alkalmanként – a közhatalmi feladatok ellátásához kapcsolódó ellenőrzési, vizsgálati vagy szabályozási tevékenység;
i) az érintett védelme vagy mások jogainak és szabadságainak védelme;
j) polgári jogi követelések érvényesítése.

A holland bírósági gyakorlatból

A holland Államtanács úgy ítélte meg, hogy az Oktatási Felügyelet jogosult volt megtagadni az érintettől a hozzáférést az iskolában történt állítólagos szexuális visszaélésekről szóló összes dokumentum másolatához. A Felügyelet jogszerűen korlátozhatta a hozzáférési jogot, mivel ebben az összefüggésben az érintett tájékoztatáshoz való jogát ellensúlyozta a szexuális visszaélések megelőzéséhez fűződő általános közérdek tekintettel arra, hogy a szexuális visszaélések bejelentésére irányuló hajlandóság csökkenhet, ha a Felügyelettel folytatott kommunikáció nem marad bizalmas.

A holland Államtanács a hozzáférési jog korlátozását a GDPR 23. cikk (1) bekezdésének h) pontja alapján jogszerűnek ítélte, miután észszerű mérlegelést végzett a közérdek és az érintett egyéni érdeke között. Ebben a konkrét esetben a

Adopted on 13 October 2021, https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf, utolsó letöltés 2022. 07. 25.

nemzeti jog által a Felügylelet számára előírt titoktartás fontosabb volt, mint az érintett egyedi érdeke.[386]

Ezen korlátozó jogalkotási intézkedések adott esetben részletes rendelkezéseket tartalmaznak legalább:

a) az adatkezelés céljaira vagy az adatkezelés kategóriáira,
b) a személyes adatok kategóriáira,
c) a bevezetett korlátozások hatályára,
d) a visszaélésre, illetve a jogosulatlan hozzáférésre vagy továbbítás megakadályozását célzó garanciákra,
e) az adatkezelő meghatározására vagy az adatkezelők kategóriáinak meghatározására,
f) az adattárolás időtartamára, valamint az alkalmazandó garanciákra, figyelembe véve az adatkezelés vagy az adatkezelési kategóriák jellegét, hatályát és céljait,
g) az érintettek jogait és szabadságait érintő kockázatokra, és
h) az érintettek arra vonatkozó jogára, hogy tájékoztatást kapjanak a korlátozásról, kivéve, ha ez hátrányosan befolyásolhatja a korlátozás célját.

[386] ECLI:NL:RVS:2021:1613, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RVS:2021:1613, utolsó letöltés: 2022. 07. 24.

A SZEMÉLYES ADATOKKAL ÖSSZEFÜGGŐ JOGOK ÉRVÉNYESÍTÉSE AZ ÉRINTETT HALÁLÁT KÖVETŐEN

A GDPR csak természetes személyek jogairól rendelkezik, azonban a tagállamok dönthetnek úgy, hogy az elhunyt személyek hozzátartozóinak biztosítanak bizonyos jogokat annak érdekében, hogy rendelkezhessenek az elhunyt személy adataival. Magyarországon az Infotv.[387] 25. §-a rendelkezik az ilyen esetekről.

> A jogi értelemben vett jogképesség a személyeknek a jogok és kötelezettségek gyakorlására való képességét jelenti. A jogi rendszerek általában csak természetes személyeket (egyének) ismernek el jogképesnek, akik önállóan cselekedhetnek, jogokat gyakorolhatnak és kötelezettségeket vállalhatnak.
>
> A természetes személyekre jellemző, hogy rendelkeznek az emberi tulajdonságokkal, mint például az értelem, az akarat, az önálló gondolkodás és a döntéshozatal képessége. Ezek a tulajdonságok teszik lehetővé számukra, hogy jogokat gyakoroljanak és kötelezettségeket vállaljanak. Az ember halálával a jogképessége megszűnik.
>
> Az elhunyt személyek nem képesek jogi cselekményeket végrehajtani, szerződéseket kötni, vagy más jogi aktusokat végrehajtani. Jogilag az elhunyt személyek nem tekinthetők jogalanyoknak, akik jogokkal és kötelezettségekkel rendelkezhetnek.
>
> Azonban vannak olyan jogi mechanizmusok és eljárások, amelyek az elhunyt személyek vagyonára és jogi helyzetére vonatkoznak. Ezek a mechanizmusok lehetővé teszik például a hagyaték kezelését, azaz az elhunyt személy által hátrahagyott vagyon elosztását a jogosultak között, vagy épp az elhunyt személy emlékét, jóhírét sértő cselekmények elleni fellépést (kegyeleti jog), mely szintén az élő hozzátartozók joga, illetve bizonyos jogok gyakorlását az adatvédelem területén.

Az érintett halálát követő öt éven belül az Infotv. 14. § b)-e) pontjában, illetve – a GDPR hatálya alá tartozó adatkezelési műveletek esetén – a GDPR 15-18. és 21. cikkében meghatározott, az elhaltat életében megillető jogokat az érintett által arra ügyintézési rendelkezéssel, illetve közokiratban vagy teljes bizonyító erejű magánokiratban foglalt, az adatkezelőnél tett nyilatkozattal – ha az érintett egy adatkezelőnél több nyilatkozatot tett, a későbbi időpontban tett nyilatkozattal – meghatalmazott személy jogosult érvényesíteni.

Amennyiben egy személy rendelkezik ilyen meghatalmazással, az élhet

- ✓ a hozzáférés jogával,
- ✓ a helyesbítés jogával
- ✓ a törléshez való joggal (az elfeledtetéshez való joggal)
- ✓ az adatkezelés korlátozásához való joggal, illetve

[387] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.)

- ✓ a tiltakozáshoz való joggal.

Ha az érintett nem tett az ilyen meghatalmazó jognyilatkozatot, akkor a Polgári Törvénykönyv szerinti közeli hozzátartozó ilyen meghatalmazás hiányában is jogosult a GDPR hatálya alá tartozó adatkezelési műveletek esetén

- ✓ a helyesbítéshez és a tiltakozáshoz való jogot, valamint
- ✓ ha az adatkezelés már az érintett életében is jogellenes volt vagy az adatkezelés célja az érintett halálával megszűnt – akkor az elhaltat életében megillető a helyesbítéshez, illetve törléshez való jogokat érvényesíteni az érintett halálát követő öt éven belül lehet.

Az érintett jogainak ily módon történő érvényesítésére az a közeli hozzátartozó jogosult, aki ezen jogosultságát elsőként gyakorolja.

Az érintett jogait a fentiek alapján érvényesítő személyt e jogok érvényesítése – így különösen az adatkezelővel szembeni, valamint a Hatóság (NAIH), illetve bíróság előtti eljárás – során az Infotv. által az érintett részére megállapított jogok illetik meg és kötelezettségek terhelik.

Amennyiben valaki az elhunyt személy érintett jogait szeretné érvényesíteni, akkor az érintett halálának tényét és idejét halotti anyakönyvi kivonattal vagy bírósági határozattal, valamint saját személyazonosságát – és amennyiben nem meghatalmazás alapján jár el, abban az esetben a közeli hozzátartozói minőségét – közokirattal kell igazolnia.

Adatkezelőként a kérelemre tájékoztatnunk kell az érintett Polgári Törvénykönyv szerinti közeli hozzátartozóját a fentiek szerint eljárva megtett intézkedésekről, kivéve, ha azt az érintett nyilatkozatában megtiltotta.

JOGORVOSLATHOZ VALÓ JOG

„Mindenkinek, akinek az Unió joga által biztosított jogait és szabadságait megsértették, az e cikkben megállapított feltételek mellett joga van a bíróság előtti hatékony jogorvoslathoz.

Mindenkinek joga van arra, hogy ügyét a törvény által megelőzően létrehozott független és pártatlan bíróság tisztességesen, nyilvánosan és ésszerű időn belül tárgyalja. Mindenkinek biztosítani kell a lehetőséget tanácsadás, védelem és képviselet igénybevételéhez.

Azoknak, akik nem rendelkeznek elégséges pénzeszközökkel, költségmentességet kell biztosítani, amennyiben az igazságszolgáltatás hatékony igénybevételéhez erre szükség van.”

> *A hatékony jogorvoslathoz és a tisztességes eljáráshoz való jog, Európa Unió Alapjogi Charta, 47. cikk*

„Mindenkinek joga van ahhoz, hogy jogorvoslattal éljen az olyan bírósági, hatósági és más közigazgatási döntés ellen, amely a jogát vagy jogos érdekét sérti.”

> *Magyarország Alaptörvénye, XXVIII. Cikk (7) bekezdés*

Mindenkinek joga van a hatékony jogorvoslathoz az adatvédelmi jog területén is. A GDPR alapján az érintetteknek vannak olyan jogaik, amelyek egyfajta jogorvoslatként is működnek, ilyen például a helyesbítés, kiegészítés, a tiltakozáshoz és törléshez való jog – ezen eszközökben rejlő lehetőségekkel az esetek nagy százalékában a sérelmesnek tartott intézkedések gyorsan orvosolhatóak. Éppen ezért célszerű minden esetben javasolnunk az érintetteknek, mielőtt a felügyeleti hatósághoz vagy bírósághoz fordulnának vélt vagy jogos sérelmük orvoslása érdekében, feltétlen vegyék fel velünk a kapcsolatot.

Természetesen számos olyan eset van, amit nem lehet „házon belül" megoldani, a GDPR pedig több lehetőséget is biztosít a panaszok orvoslására:

- az érintett panaszt tehet a felügyeleti hatóságnál
- az érintett bírósághoz fordulhat jogorvoslatért.

Adatkezelőként velünk is előfordulhat, hogy nem értünk egyet a hatóság ránk vonatkozó döntésével, ez esetben mi is bírósághoz fordulhatunk hatékony jogorvoslat érdekében.

A felügyeleti hatóságnál történő panasztételhez való jog

Az egyéb közigazgatási vagy bírósági jogorvoslatok sérelme nélkül, minden érintett jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál – különösen a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban –, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti a GDPR-ban foglaltakat („közigazgatási jogorvoslat").[388]

A felügyeleti hatóságok illetékességét, feladatait és hatásköreit a GDPR 55-58. cikkei tartalmazzák.

Az a felügyeleti hatóság, amelyhez a panaszt benyújtották, köteles tájékoztatni az ügyfelet a panasszal kapcsolatos eljárási fejleményekről és annak eredményéről, ideértve azt is, hogy az ügyfél jogosult bírósági jogorvoslattal élni.

[388] GDPR 77. cikk

Az osztrák bírósági gyakorlatból

A GDPR 77. cikke („a felügyeleti hatóságnál történő panasztételhez való jog") lehetővé teszi az érintettek számára, hogy közvetlenül az adatvédelmi hatósághoz forduljanak, és panaszt tegyenek a felügyeleti hatóságnál. Ez egy független panaszjog, amely nem kapcsolódik a nemzeti jog formai vagy tartalmi követelményeihez vagy bizonyítékok szolgáltatásához. E tekintetben már az olyan alapelvek megsértése, mint a GDPR 5. cikk (1) bekezdésének f) pontja („integritás és bizalmas jelleg") is érintheti a panaszos személyes adatainak a kezelését, és biztosíthatja számukra ezt a konkrét jogot. A kifogásolt jogsértéseknek az adatvédelmi hatóság által más feltételezésen alapuló elutasítása ezért érvénytelennek tekinthető, és azt helyesbíteni kell.

A panaszjog érvényesítésének szükséges előfeltétele, hogy
- ✓ *a panaszos maga is érintett legyen az adatkezelésben,*
- ✓ *az adatkezelés sértse a GDPR rendelkezéseit, valamint*
- ✓ *a hatóság, amelyhez fordul, illetékes hatóság legyen.*

A GDPR 77. cikke nem határozza meg a panaszos bizonyítási kötelezettségét, így a GDPR rendelkezéseinek valamennyi megsértése panasztételre alkalmas, ideértve például a GDPR 5. cikkében foglalt alapelvek és az érintetti jog valamennyi olyan megsértését, amely a panaszos személyes adatainak kezelését érintheti.[389]

A felügyeleti hatósággal szembeni hatékony bírósági jogorvoslathoz való jog

Az egyéb közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben.[390]

Az egyéb közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden érintett jogosult a hatékony bírósági jogorvoslatra, ha
- ✓ az illetékes felügyeleti hatóság nem foglalkozik a panasszal, vagy
- ✓ három hónapon belül nem tájékoztatja az érintettet a benyújtott panaszával kapcsolatos eljárási fejleményekről vagy annak eredményéről.

A felügyeleti hatósággal szembeni eljárást a felügyeleti hatóság székhelye szerinti tagállam bírósága előtt kell megindítani.

[389] ENTSCHEIDUNGSDATUM 09. 08. 2021 GESCHÄFTSZAHL 2112222613-2/11E, https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20210809_W211_2222613_2_00_01/BVWGT_20210809_W211_2222613_2_00_01.pdf, utolsó letöltés: 2022. 07. 24.
[390] GDPR 78. cikk

A holland bírósági gyakorlatból

Az Amszterdami Kerületi Bíróság kimondta, hogy az Adatvédelmi Alapítvány (hollandiai nonprofit szervezet) a holland bíróság előtt perelheti a Facebookot a holland Facebook-felhasználók nevében abban a kérdésben, hogy a Facebooknak van-e érvényes jogalapja az adatkezelési tevékenységeire.[391]

A belga bírósági gyakorlatból

A belga adóhivatal fellebbezett a belga adatvédelmi hatóság ideiglenesen végrehajtható határozatával szemben, és a bíróság érdemi döntésének meghozásáig kérte a már meghozott végrehajtási intézkedések azonnali felfüggesztését.

A brüsszeli fellebbviteli bíróság elutasította a határozat végrehajtásának felfüggesztését, mivel a fellebbező (a belga adóhivatal) nem terjesztett elő konkrét bizonyítékot a felfüggesztés iránti kérelmének alátámasztására. A fellebbezőnek kell bizonyítania, hogy az adatvédelmi hatóság határozatának végrehajtása sértené az Alapjogi Charta 47. cikkében meghatározott hatékony jogorvoslathoz való jogot.[392]

Az adatkezelővel vagy az adatfeldolgozóval szembeni hatékony bírósági jogorvoslathoz való jog

A rendelkezésre álló közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak GDPR-nak nem megfelelő kezelése következtében megsértették az érintetti jogait („bírósági jogorvoslat").[393]

Az érintett az adatkezelő, illetve – az adatfeldolgozó tevékenységi körébe tartozó adatkezelési műveletekkel összefüggésben – az adatfeldolgozó ellen bírósághoz fordulhat, ha megítélése szerint az adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a személyes adatait a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírások megsértésével kezeli.[394]

Az adatkezelővel vagy az adatfeldolgozóval szembeni eljárást az adatkezelő vagy az adatfeldolgozó tevékenységi helye szerinti tagállam bírósága előtt kell megindítani. Az ilyen eljárás megindítható az érintett szokásos tartózkodási helye szerinti tagállam bírósága előtt is, kivéve, ha az adatkezelő vagy az adatfeldolgozó valamely tagállamnak a közhatalmi jogkörében eljáró közhatalmi szerve.

---

[391] ECLI:NL:RBAMS:2021:3307, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:3307&showbutton=true&keyword=AVG, utolsó letöltés: 2022. 07. 24.
[392] 2021/AR/1044, https://www.gegevensbeschermingsautoriteit.be/publications/tussenarrest-van-16-juli-2021-van-het-marktenhof-ar-1044.pdf utolsó letöltés: 2022. 07. 24.
[393] GDPR 79. cikk
[394] Infotv. 23.§ Az Infotv. 2.§ (2) bekezdése alapján a GDRP rendelkezéseit az Infotv. 23.§-ban foglalt kiegészítésekkel kell alkalmazni

Az Európa Unió Bíróságának (EUB) gyakorlatából

A Fővárosi Törvényszék annak eldöntése érdekében, hogy a közigazgatási és a bírósági jogorvoslat hogyan viszonyul egymáshoz, az alábbi kérdéseket tette fel előzetes döntéshozatalra a Budapesti Elektromos Művek Zrt.-vel és a Nemzeti Adatvédelmi és Információszabadság Hatósággal kapcsolatos ügyben:

A GDPR 77. cikkének (1) bekezdését és 79. cikkének (1) bekezdését úgy kell-e értelmezni, hogy a 77. cikkben foglalt közigazgatási jogorvoslat a közjogi jogérvényesítés, míg a 79. cikkben foglalt bírósági jogorvoslat a magánjogi jogérvényesítés eszköze? Amennyiben igen, ebből következik-e, hogy a közigazgatási jogorvoslatra hatáskörrel rendelkező felügyeleti hatóság a jogsértés tényének megállapítására elsődleges hatáskörrel rendelkezik?

Amennyiben az érintett – akinek megítélése szerint a rá vonatkozó személyes adatok kezelése megsértette a GDPR-t – mind az általános adatvédelmi rendelet 77. cikkének (1) bekezdése szerinti panasztétel jogával, mind a 79. cikkének (1) bekezdése szerinti bírósági jogorvoslat jogával egyszerre él, melyik értelmezés áll az Alapjogi Charta 47. cikkével összhangban:

a.) a felügyeleti hatóság és a bíróság egymástól függetlenül köteles a jogsértés tényét vizsgálni, és ezáltal akár eltérő eredményre juthatnak; vagy
b.) a felügyeleti hatóság döntése – a jogsértés elkövetésének ténye megítélésében – elsőbbséget élvez a GDPR 51. cikkének (1) bekezdésében foglalt felhatalmazásra és az 58. cikk (2) bekezdésének b) és d) pontjaiban biztosított hatáskörökre tekintettel?

A GDPR 51. cikkének (1) bekezdése és 52. cikkének (1) bekezdése által a felügyeleti hatóság számára biztosított független jogállást úgy kell-e értelmezni, hogy a felügyeleti hatóság a GDPR 77. cikk szerinti panasz elbírálása iránti eljárásában és döntésében független a 79. cikk szerinti hatáskörrel rendelkező bíróság jogerős ítéletében foglaltaktól, és ezáltal az ugyanazon vélt jogsértés vonatkozásában akár eltérő döntésre juthat?[395]

A kártérítéshez való jog és a felelősség

Minden olyan személy, aki a GDPR szabályainak megsértésének eredményeként vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért az adatkezelőtől vagy az adatfeldolgozótól kártérítésre jogosult.[396]

[395] A Fővárosi Törvényszék (Magyarország) által 2021. március 3-án benyújtott előzetes döntéshozatal iránti kérelem – BE kontra Nemzeti Adatvédelmi és Információszabadság Hatóság (C-132/21. sz. ügy), https://curia.europa.eu/juris/document/document.jsf?text=&docid=241822&pageIndex=0&doclang=HU&mode=lst&dir=&occ=first&part=1&cid=3910462, utolsó letöltés: 2022. 07. 24.
[396] GDPR 82. cikk

A holland bírósági gyakorlatból

A GDPR megsértése nem vonja automatikusan maga után a személy integritásának olyan sérelmét, amely kártérítéshez vezetne. Az a tény, hogy a GDPR megsértése nem vagyoni kárt is eredményezhet, és hogy az érintettnek a GDPR értelmében teljes és tényleges kártérítést kell kapnia, nem jelenti azt, hogy a rendelet megsértése mindig kártérítést eredményez. Az okozott kárnak valósnak és biztosnak kell lennie.[397]

A holland bírósági gyakorlatból

A s-Hertogenbosch-i fellebbviteli bíróság elutasította egy érintett édesanyjának törlési kérelmét, mivel az ő érdekei nem voltak fontosabbak az adatkezelő érdekeinél. Ugyanakkor úgy ítélte meg, hogy az anyának nem kell megfizetnie az eljárás költségeit, mivel ez ellentétes lenne a hatékony jogorvoslathoz való, a GDPR 79. cikke szerinti jogával.[398]

Az adatkezelésben érintett valamennyi adatkezelő felelősséggel tartozik minden olyan kárért, amelyet a GDPR rendelkezéseit sértő adatkezelés okozott. Az adatfeldolgozó csak abban az esetben tartozik felelősséggel az adatkezelés által okozott károkért,

- ✓ ha nem tartotta be az GDPR-ban meghatározott, kifejezetten az adatfeldolgozókat terhelő kötelezettségeket, vagy
- ✓ ha az adatkezelő jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el.

Az adatkezelésben érintett valamennyi adatkezelő felelősséggel tartozik minden olyan kárért, amelyet a GDPR előírásait sértő adatkezelés okozott. Az adatfeldolgozó csak abban az esetben tartozik felelősséggel az adatkezelés által okozott károkért, ha nem tartotta be a GDPR-ban meghatározott, kifejezetten az adatfeldolgozókat terhelő kötelezettségeket, vagy ha az adatkezelő jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el.

Érintettként hol nyújthatjuk be a panaszunkat az általunk jogszerűtlennek vélt adatkezelés miatt?

A tartózkodási helyünk, a munkahelyünk vagy a feltételezett jogsértés helye szerinti tagállam felügyeleti hatóságánál – azaz, ha például a spanyolországi nyaralásunk alatt a helyi szálloda adatkezelése tűnt számunkra jogszerűtlennek, akkor a hazai, azaz a magyar felügyeleti hatóságnál anyanyelvükön is panaszkodhatunk, azaz nem kell a spanyol adatvédelmi hatóságot megkeresnünk.

Az adatkezelő, illetve az adatfeldolgozó mentesül ezen felelősség alól, ha bizonyítja, hogy a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség.

[397] ECLI:NL:RVS:2020:900, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RVS:2020:900&showbutton=true&keyword=avg, utolsó letöltés: 2022. 07. 24.
[398] ECLI:NL:GHSHE:2022:80, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHSHE:2022:80&showbutton=true&keyword=AVG utolsó letöltés: 2022. 07. 24.

Nem kell megtéríteni a kárt és nem követelhető a sérelemdíj annyiban, amennyiben a kár a károsult vagy a személyiségi jog megsértésével okozott jogsérelem a személyiségi jogi jogsérelmet szenvedő személy szándékos vagy súlyosan gondatlan magatartásából származott.[399]

A kártérítésnek „teljesnek és ténylegesnek" kell lennie az elszenvedett károkozás vonatkozásában. Ha egy adatkezelésben több adatkezelő, illetve adatfeldolgozó okozott kárt az érintettnek, akkor minden egyes adatkezelő vagy adatfeldolgozó egyetemleges felelősséggel tartozik a teljes kárért annak érdekében, hogy biztosítva legyen a tényleges kártérítés.

Az osztrák bírósági gyakorlatból

Az osztrák legfelsőbb bíróság úgy döntött, hogy – többek között – nem vagyoni kártérítésként 500 euró kártérítést ítélt meg a felperesnek a hozzáférési jog megsértése miatt, amely „jelentős mértékben bosszantotta".

A bíróság megállapította, hogy

- ✓ *a felperest a Facebook adatkezelése „jelentős mértékben bosszantotta", de pszichésen nem károsította.*
- ✓ *a jogsérelemből eredő érzelmi károsodások, mint például a kitettség, diszkrimináció vagy hasonlók miatt bekövetkezett, vagy csak fenyegető félelem, stressz vagy szenvedési állapotok nem vagyoni kárként kártérítési igényt eredményezhetnek.*
- ✓ *nem szükséges az érzelmi világ különösen súlyos károsodása, a GDPR (146) preambulumbekezdésének 3. mondata alapján a kár fogalmát tágan kell értelmezni.*
- ✓ *a GDPR (146) preambulumbekezdése szerint a kártérítés nem lehet túlságosan korlátozott („érintetteket az őket ért kárért teljes és tényleges kártérítés illeti meg"), ellenkező esetben nem lenne biztosított az uniós jog gyakorlati hatékonysága. A kártérítésnek érzékelhetőnek kell lennie ahhoz, hogy megelőző és elrettentő hatása legyen.*
- ✓ *a hatékonysági kritériumnak csak korlátozott jelentősége van, mivel a GDPR egyébként is magas szankciókat ír elő, így magas kártérítést nem lehet könnyen követelni, ellenkező esetben fennállna a „hatékonysági spirál" veszélye.*
- ✓ *a „jelentős mértékben bosszantott", pszichés károsodás nélkül is elegendő a nem vagyoni kár feltételezéséhez. Az okozatiság már abból is következett, hogy a felperes azzal érvelt, hogy zavarta, hogy nem tudott a személyes adatai felett rendelkezni, mert azok nem jelentek meg az eszközökben. Ebben az esetben a „mert" szó használata megteremtette a szükséges kapcsolatot.*
- ✓ *a kár összegénél a bíróság figyelembe vette, hogy a felperes hosszú időn keresztül nem rendelkezett a személyes adatai felett.* [400]

[399] Infotv. 24.§ Az Infotv. 2.§ (2) bekezdése alapján a GDRP rendelkezéseit az Infotv. 24.§-ban foglalt kiegészítésekkel kell alkalmazni

[400] 6Ob56/21k, https://www.ris.bka.gv.at/Dokumente/Justiz/JJT_20210623_OGH0002_0060OB00056_21K00

A GDPR lehetővé teszi azt is az érintettek számára, hogy felügyeleti hatósághoz panaszt benyújtóként vagy bíróság előtt keresetet indító személyként képviseletükkel nonprofit jellegű szervet, szervezetet vagy egyesületet bízzanak meg. Ezen nonprofit szervezetekkel szemben követelmény, hogy alapszabályukban rögzített céljaik a közérdeket szolgálják és az adatvédelem területén tevékenykedjenek. Amennyiben az érintettek találnak és megbíznak ilyen szervezetet az érdekeik védelmével és jogaik érvényesítésével, akkor ez a szervezet benyújthatja a panaszukat vagy gyakorolhatja a bírósági jogorvoslathoz való jogot az érintettek nevében.

Az Európai Unió Bírósága (EUB) gyakorlatából

A Bíróság (harmadik tanács) 2022. április 28-i ítélete (a Bundesgerichtshof [Németország] előzetes döntéshozatal iránti kérelme) – Meta Platforms Ireland Limited, korábban Facebook Ireland Limited kontra Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.
(C-319/20. sz. ügy)

„A GDPR 80. cikkének (2) bekezdését úgy kell értelmezni, hogy azzal nem ellentétes az olyan nemzeti szabályozás, amely lehetővé teszi a fogyasztói érdekvédelmi egyesületek számára, hogy a személyes adatok védelmét állítólagosan megsértő személlyel szemben a tisztességtelen kereskedelmi gyakorlatok tilalmára, valamely fogyasztóvédelmi törvény megsértésére vagy az érvénytelen általános szerződési feltételek alkalmazásának tilalmára hivatkozva bírósághoz forduljanak e célból számukra adott megbízás nélkül és az érintett személyek konkrét jogainak megsértésétől függetlenül, amennyiben az érintett adatkezelés érintheti az azonosított vagy azonosítható természetes személyeket e rendelet alapján megillető jogokat.”[401]

Az ítélet alapján a képviseleti kereset indításának csupán az a feltétele, hogy az adott szervezet „megítélése szerint” az érintett személyes adatainak kezelése következtében megsértették az érintett a GDPR szerinti jogait, és e szervezet a GDPR rendelkezéseivel ellentétes adatkezelés fennállására hivatkozik. Az EUB megállapította, hogy az ilyen szervezetnek az említett rendelkezés értelmében vett kereshetőségi jogának elismerése érdekében elegendő arra hivatkozni, hogy az érintett adatkezelés érintheti azokat a jogokat, amelyek azonosított vagy azonosítható természetes személyeket az említett rendelet alapján megilletnek, anélkül, hogy az érintett személyt valamely konkrét helyzetben a jogainak megsértéséből eredően ért tényleges kárt bizonyítani kellene.

Ez az értelmezés megfelel az EUMSZ 16. cikkből és az Európai Unió Alapjogi Chartájának 8. cikkéből eredő követelményeknek, és így a GDPR azon céljának is, amely a természetes személyek alapvető jogai és szabadságai hatékony védelmének,

00_000/JJT_20210623_OGH0002_0060OB00056_21K0000_000.pdf, utolsó letöltés: 2022. 07. 24.

[401] C-319/20. sz. ügy, https://curia.europa.eu/juris/document/document.jsf?text=&docid=261210&pageIndex=0&doclang=HU&mode=req&dir=&occ=first&part=1&cid=3931809, utolsó letöltés: 2022. 07. 24.

valamint többek között a bármely személyt megillető, a rá vonatkozó személyes adatok védelméhez való jog magas szintű védelmének biztosítására irányul.

GDPR

- ✓ Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések [12. cikk, (58)-(59) preambulumbekezés]
- ✓ Rendelkezésre bocsátandó információk, ha a személyes adatokat az érintettől gyűjtik [13. cikk, (60)-(62) preambulumbekezés]
- ✓ Rendelkezésre bocsátandó információk, ha a személyes adatokat nem az érintettől szerezték meg [14. cikk]
- ✓ Az érintett hozzáférési joga [15. cikk, (63)-(64) preambulumbekezés]
- ✓ A helyesbítéshez való jog [16. cikk, (65) preambulumbekezés]
- ✓ A törléshez való jog („az elfeledtetéshez való jog") [17. cikk, (65)-(66) preambulumbekezés]
- ✓ Az adatkezelés korlátozásához való jog [18. cikk, (67) preambulumbekezés]
- ✓ A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség [19. cikk]
- ✓ Az adathordozhatósághoz való jog [20. cikk, (68) preambulumbekezés]
- ✓ A tiltakozáshoz való jog [21. cikk, (69)-(70) preambulumbekezés]
- ✓ Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást [22. cikk, (71)-(72) preambulumbekezés]
- ✓ Korlátozások [23. cikk, (73) preambulumbekezés]
- ✓ A felügyeleti hatóságnál történő panasztételhez való jog [77. cikk, (141) preambulumbekezés]
- ✓ A felügyeleti hatósággal szembeni hatékony bírósági jogorvoslathoz való jog [78. cikk, (143) preambulumbekezés, (143) preambulumbekezés]
- ✓ Az adatkezelővel vagy az adatfeldolgozóval szembeni hatékony bírósági jogorvoslathoz való jog [79. cikk, (145) preambulumbekezés]
- ✓ Az érintettek képviselete [80. cikk, (142) preambulumbekezés]
- ✓ A kártérítéshez való jog és a felelősség [82. cikk, (146)-(147) preambulumbekezés]

Infotv.

- ✓ Az érintett jogai érvényesülésének biztosítása [23.§]
  A személyes adatokkal összefüggő jogok érvényesítése az érintett halálát követően [25.§]

ÚJ, INNOVATÍV TECHNOLÓGIÁK – A MESTERSÉGES INTELLIGENCIA

„Az innováció csak akkor szolgálja az emberek javát, ha az megfelelő, hatékony, és erős garanciákkal párosul.”[402]

Mi az a Big Data („Nagy Adat”)?

A „Big Data” technológia (és elnevezés) az információk hozzáférhetőségének és automatizált felhasználásának exponenciális növekedésének eredménye. A különféle szervezetek (vállalatok, kormányzati szervek és egyéb szervezetek) gigantikus méretű digitális adatbázisokat építenek, amelyeket aztán számítógépes algoritmusok segítségével különféle célokra elemeznek és felhasználnak.

A Big Data technológiának számos felhasználási területe van, alkalmazzák – többek között – az egészségügyben, a kommunikációban, a marketingben, az összekapcsolt rendszerekben és az intelligens hálózatokban, a bűnüldözésben és a különböző internetes platformokon is. A Big Data felhasználható az általános trendek és összefüggések azonosítására, az érintettek személyes preferenciáinak, viselkedésének és attitűdjeinek elemzésére vagy előrejelzésére (profilozására), és támaszkodhat rá az automatikus döntéshozatalnál is (például személyre szabott ajánlatok, célzott reklámok stb.).

Milyen kockázatokat hordoz a Big Data az információs önrendelkezési jog szempontjából?

A technológia számos aggályt vet fel, többek között:

- az adatgyűjtés, a nyomon követés, a megfigyelés és a profilalkotás mértéke és általánossá válása, különös tekintettel az összegyűjtött adatok sokféleségére és részletességére, valamint arra, hogy gyakran számos különböző forrásból származó adatokat kombinálnak (például különféle adatbrókerektől vásárolt adatokat gyűjtenek össze egyetlen Nagy Adatba),
- az adatok biztonsága egyre fontosabb, mivel a védelem szintje általában elmarad a volumen növekedésétől, illetve az adatmennyiség a kiberbűnözők számára csalogató célponttá válhat,
- az érintettek nem kapnak elegendő információt az adatkezelésekről (sérül az átláthatóság elve), ha pedig nem kapnak megfelelő tájékoztatást, abban az esetben olyan döntéseknek lehetnek kitéve, amelyeket nem értenek, és amelyek felett nem gyakorolhatnak ellenőrzést,
- fokozott a veszélye a pontatlanságnak, a megkülönböztetésnek, a kirekesztésnek és a gazdasági egyensúlyhiánynak, ez pedig jogszerűtlen eredményt okozhat, állandósítva, vagy akár fokozva is az előítéleteket,
- jelentősen megnőnek a kormányzati felügyelet lehetőségei.

[402] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: 2022. 07. 17.

Az, hogy a Big Data következménye a „megfigyelési kapitalizmus”[403], vagy a „megfigyelési kapitalizmus” terméke a Big Data nem igazán egyértelmű. Shoshana Zuboff A megfigyelési kapitalizmus kora című könyvében részletesen elemzi az új, innovatív technológiák korát:

„A megfigyelési kapitalizmus a tudás és a tudásból fakadó hatalom soha nem látott aszimmetriáján keresztül működik. A megfigyelő kapitalisták mindent tudnak rólunk, miközben működésüket úgy alakították ki, hogy számunkra kiismerhetetlenek legyenek. A tőlünk származó tudásból új tudás hatalmas birodalmát halmozzák fel, de nem a mi számunkra. A jövőnket mások haszna érdekében jósolják meg, nem a miénkért.”[404]

Mi az a mesterséges intelligencia?

„A mesterséges intelligencia intelligens viselkedésre utaló rendszereket takar, amelyek konkrét célok eléréséhez elemzik a környezetüket és – bizonyos mértékű autonómiával – intézkedéseket hajtanak végre.

A mesterséges intelligencián alapuló rendszerek lehetnek kizárólag szoftver-alapú rendszerek, amelyek a virtuális világban működnek (pl. hangasszisztensek, képelemző szoftverek, keresőprogramok, hang- és arcfelismerő rendszerek), illetve a mesterséges intelligencia beépíthető hardvereszközökbe is (pl. fejlett robotok, autonóm járművek, drónok és a tárgyak internetéhez kapcsolódó alkalmazások).

A mesterséges intelligenciát napi szinten használjuk, például nyelvek fordításához, videók feliratozásához és kéretlen elektronikus levelek kiszűréséhez.

Életünk megkönnyítésén túl a mesterséges intelligencia segít a világ legnagyobb kihívásainak megoldásában: a krónikus betegségek kezelésében, a halálos kimenetelű közlekedési balesetek csökkentésében,[405] az éghajlatváltozás leküzdésében és a kiberbiztonsági fenyegetések előrejelzésében.”[406]

A mesterségesintelligencia-rendszer (MI-rendszer) olyan gépi alapú rendszer[407], amelyet úgy terveztek, hogy különböző szintű autonómiával működjön, és amely

[403] Megfigyelési kapitalizmus („Surveillance capitalism”) definíciója: 1. Egy új gazdasági rend, amely az emberi tapasztalatot ingyenes nyersanyagként követeli a kiaknázás, előrejelzés és értékesítés rejtett kereskedelmi gyakorlataihoz; 2. Egy parazita gazdasági logika, amelyben az áruk és szolgáltatások előállítása a viselkedésmódosítás új globális architektúrájának van alárendelve (…) Shoshana Zuboff: The Age of Surveillance Capitalism, PublicAffairs New York 2019)

[404] Shoshana Zuboff: The Age of Surveillance Capitalism, PublicAffairs New York 2019,

[405] Becslések szerint a közúti balesetek mintegy 90 %-át emberi hiba okozza. Lásd a Bizottság jelentését: A halálos kimenetelű közúti balesetek csökkentése: a gépjárműbiztonság javítása az Európai Unióban (COM(2016) 0787 final)

[406] A Bizottság közleménye A közös európai adattér kialakítása felé {SWD(2018) 137 final}, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52018DC0237&from=EN, utolsó letöltés: 2022. 07. 17.

[407] DRAFT Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence

kifejezett (explicit) vagy közvetett (implicit) célok érdekében képes olyan kimeneteket, például előrejelzéseket, ajánlásokat vagy döntéseket létrehozni, amelyek befolyásolják a fizikai vagy virtuális környezetet.[408]

„A mesterséges intelligencia (MI) olyan gyorsan fejlődő technológiacsalád, amely széles körű gazdasági és társadalmi előnyökhöz vezethet az iparágak és a társadalmi tevékenységek teljes spektrumában. Az előrejelzések javításával, a műveletek és az erőforrások elosztásának optimalizálásával, valamint a szolgáltatásnyújtás személyre szabásával a mesterséges intelligencia használata elősegítheti a társadalmi és környezeti szempontból előnyös eredményeket, és kulcsfontosságú versenyelőnyt biztosíthat a vállalkozások és az európai gazdaság számára. Ilyen intézkedésekre különösen a nagy hatású ágazatokban van szükség, beleértve az éghajlatváltozást, a környezetvédelmet, az egészségügyet, a közszférát, a pénzügyet, a mobilitást, a belügyet és a mezőgazdaságot. Ugyanakkor ugyanazok az elemek és technikák, amelyek elősegítik a mesterséges intelligencia társadalmi-gazdasági előnyeit, új kockázatokkal vagy negatív következményekkel is járhatnak az egyének vagy a társadalom számára. A technológiai változás sebességére és a lehetséges kihívásokra való tekintettel az EU kiegyensúlyozott megközelítés mellett kötelezte el magát. Az Unió érdeke, hogy megőrizze az EU technológiai vezető szerepét, és biztosítsa, hogy az európaiak élvezhessék az uniós értékeknek, az alapvető jogoknak és az alapelveknek megfelelően kifejlesztett és működő új technológiák előnyeit.

(…) a Bizottság előterjeszti a mesterséges intelligenciára vonatkozóan javasolt szabályozási keretet az alábbi konkrét célkitűzésekkel:

- *annak biztosítása, hogy az Unióban forgalomba hozott és használt MI-rendszerek biztonságosak legyenek, és tiszteletben tartsák az alapvető jogokra és az uniós értékekre vonatkozó hatályos jogszabályokat;*
- *a jogbiztonság biztosítása a mesterséges intelligenciába történő beruházások és a mesterséges intelligenciát érintő innováció elősegítése érdekében;*
- *az irányításnak és az MI-rendszerek tekintetében az alapvető jogokra és biztonsági követelményekre vonatkozó hatályos jogszabályok hatékony érvényesítésének a javítása;*
- *a jogszerű, biztonságos és megbízható MI-alkalmazások tekintetében az egységes piac kialakításának elősegítése és a piac széttöredezettségének megelőzése.”*[409]

(Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9 0146/2021 – 2021/0106(COD)). 16/5/2023 Version: 1.1

[408] a mesterséges intelligencia rendszerek jelen meghatározása ideiglenes, a mesterséges intelligencia használatáról szóló rendelet tervezetének 2023. május 16-i állapota alapján

[409] Javaslat Az Európai Parlament és a Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról, Brüsszel, 2021.4.21. COM(2021) 206 final 2021/0106(COD), https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52021PC0206&from=FR, utolsó letöltés: 2022. 07. 17.

Mesterséges intelligenciát ma már szinte mindenki mindennap használ (bár nem biztos, hogy tudatában van annak, hogy mesterséges intelligenciával működő alkalmazással áll szemben), gondoljunk például a fordító programokra, az online keresőmotorokra, a chatbotokra, a különböző képgeneráló szoftverekre, illetve az egyre szélesebb körben használt és rohamosan fejlődő ChatGPT-re.

Miért jelenthet nagy kockázatot az érintettek jogaira és szabadságaira nézve a mesterséges intelligencia alkalmazása?

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Az általános adatvédelmi rendelet 25. cikk (1) és (2) bekezdése alapján az Ügyfél köteles lett volna a mesterséges intelligenciát alkalmazó automata hangelemzés megkezdése előtt felmérni, hogy az adatkezelés a jelenlegi technikai és társadalmi körülmények között kivitelezhető-e az adatvédelmi szabályok maximális betartása mellett. Az Ügyfél érdekmérlegelése (...) nyilatkozataival ellentétes, és a feltárt tényállás is a jogszerűtlen állapotot támasztja alá. Az Ügyfél tudta, vagy a jogilag elvárható körültekintés mellett tudhatta volna az adatkezelés megkezdése előtt, hogy milyen módon lehetséges vagy nem lehetséges az érintettek tájékoztatása, valamint a tiltakozási és egyéb érintetti jogok érvényesítése. A fentiek és az általános adatvédelmi rendelet 24. és 25. cikkei alapján az Ügyfél eleve nem dönthetett volna úgy, hogy a hangelemzéses adatkezelést megkezdi ebben a formában."[410]

A mesterséges intelligencia olyan sajátos jellemzőkkel rendelkezhet (az alkalmazott eljárástól függően), mint például az átláthatatlanság,[411] az összetettség, az adatoktól való függés, illetve az autonóm magatartás és a használata hátrányosan érinthet számos olyan alapvető jogot, amely az Európai Unió Alapjogi Chartájában rögzítve van. Ilyen – a mesterséges intelligencia által érintett – alapvető jog lehet például

- az emberi méltósághoz való jog (1. cikk),
- a magánélet tiszteletben tartása és a személyes adatok védelme (7. és 8. cikk),
- a megkülönböztetésmentesség (21. cikk),
- a nők és férfiak közötti egyenlőség (23. cikk).
- a véleménynyilvánítás szabadsága (11. cikk) és a gyülekezés szabadsága (12. cikk)
- a hatékony jogorvoslathoz és a tisztességes eljáráshoz való jog (47. cikk)
- Az ártatlanság vélelme és a védelemhez való jog (48. cikk),
- a megfelelő ügyintézés általános elve
- a munkavállalók tisztességes és igazságos munkafeltételekhez való joga (31. cikk)
- a magas szintű fogyasztóvédelem (28. cikk),

[410] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: 2022. 07. 17.

[411] Az átláthatatlan mesterséges intelligencia alkalmazások olyan rendszerek, amelyek működése és döntéshozatala nem könnyen érthető vagy magyarázható az ember számára. Ilyen rendszerek például a mesterséges intelligenciát használó hitelminősítési rendszerek a bankokban és a pénzintézetekben. Az átláthatatlan rendszerek esetében az embereknek nincs pontos betekintése abba, hogy milyen adatokat és algoritmusokat használ a rendszer a döntéshozatalhoz. Ez a hiányosság kiszolgáltathatja az ügyfeleket, akik nem értik, mi alapján döntenek róluk.

- a gyermekek jogai (24. cikk)
- a fogyatékossággal élő személyek integrációja (26. cikk)
- a magas szintű környezetvédelemhez és a környezet minőségének javításához való jog (37. cikk)
- a vállalkozás szabadsága (16. cikk),
- a művészet és a tudomány szabadsága (13. cikk)
- a szellemi tulajdon védelméhez való jog (17. cikk (2) bekezdés).

„A mesterséges intelligencia egyik nagy kihívása az átláthatóság biztosításának kérdése”[412]

A mesterséges intelligencia rendszerekkel kapcsolatos alapelvek

Amennyiben mesterséges intelligencia rendszert használunk, minden tőlünk telhetőt meg kell tennünk annak érdekében, hogy bizonyos alapelveknek megfeleljünk:

a) a mesterséges intelligencia rendszereket olyan eszközként kell kifejlesztenünk és használnunk, amely az embereket szolgálja, tiszteletben tartja az emberi méltóságot és a személyes autonómiát, és amely úgy működik, hogy az általunk megfelelően ellenőrizhető és felügyelhető legyen (emberi irányítás és felügyelet)

b) a mesterséges intelligencia rendszereket úgy kell kifejlesztenünk és használnunk, hogy
- minimalizáljuk a nem szándékos, illetve váratlan károkat,
- robusztusak legyenek a nem szándékos problémák esetén,
- ellenállóak legyenek a mesterséges intelligencia rendszer használatának vagy teljesítményének megváltoztatására irányuló kísérletekkel szemben, valamint
- ne tegyék lehetővé a jogellenes használatot rosszindulatú harmadik felek számára (műszaki robusztusság és biztonság)

c) a mesterséges intelligencia rendszereket a hatályos magánélet- és adatvédelmi szabályoknak megfelelően kell kifejlesztenünk és használnunk, miközben a minőség és az integritás tekintetében magas szintű követelményeknek megfelelő adatokat kell feldolgoznunk (magánélet és az adatok védelme)

d) a mesterséges intelligencia rendszereket úgy kell kifejlesztenünk és használnunk, hogy azok megfelelően nyomon követhetők és megmagyarázhatóak legyenek, miközben az emberek tudatában vannak annak, hogy egy mesterséges intelligencia rendszerrel kommunikálnak vagy lépnek kölcsönhatásba, valamint megfelelően tájékoztatnunk kell a felhasználókat a mesterséges intelligencia rendszer képességeiről és korlátairól, illetve az érintett személyeket a jogaikról (átláthatóság)

e) a mesterséges intelligencia rendszereket úgy kell kifejlesztenünk és használnunk, hogy a különböző szereplőket bevonjuk, valamint elősegítjük az egyenlő hozzáférést, a nemek közötti egyenlőséget és a kulturális sokszínűséget, ugyanakkor elkerüljük az

[412] NAIH-85-3/2022, https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei, utolsó letöltés: 2022. 07. 17.

uniós vagy nemzeti jog által tiltott diszkriminációt és a tisztességtelen előítéleteket (sokszínűség, megkülönböztetésmentesség és méltányosság)

f) a mesterséges intelligencia rendszereket fenntartható és környezetbarát módon, valamint minden ember javát szolgáló módon kell fejlesztenünk és használnunk, miközben figyelemmel kísérjük és értékeljük az egyénre, a társadalomra és a demokráciára gyakorolt hosszú távú hatásokat (társadalmi és környezeti jólét)

A mesterséges intelligencia rendszerek kockázatalapú megközelítése

A mesterséges intelligencia használatával kapcsolatos rendelet javaslata – a GDPR-hoz hasonlóan – alapvetően kockázatalapú megközelítést alkalmaz.

Tiltott mesterséges intelligencia rendszerek

A tervezet alapján elfogadhatatlan kockázatúak az olyan mesterséges intelligencia rendszerek (MI-rendszerek), amelyek egyértelműen veszélyeztetik az emberek egészségét, biztonságát és alapvető jogait. Ezek tiltva lesznek. Ilyenek például az olyan MI-rendszerek vagy -alkalmazások, amelyek a felhasználók szabad akaratának megkerülése érdekében manipulálják az emberi viselkedést, valamint az olyan rendszerek is, amelyek lehetővé teszik a kormányok általi „társadalmi pontozást”.

A rendelet tervezete alapján[413] *tilos*[414]*:*

- *olyan mesterséges intelligenciával működő rendszer forgalomba hozatala, üzembe helyezése vagy használata, amely a személy tudatán kívül szubliminális technikákat vagy célzottan manipulatív vagy megtévesztő technikákat alkalmaz azzal a céllal vagy azzal a hatással, hogy egy személy vagy személyek egy csoportja magatartását jelentősen torzítsa azáltal, hogy érzékelhetően rontja a személy tájékozott döntéshozatalra való képességét, és ezáltal a személyt olyan döntés meghozatalára készteti, amelyet egyébként nem hozott volna meg, oly módon, amely jelentős kárt okoz vagy valószínűleg jelentős kárt okoz az adott személynek, más személynek vagy személyek csoportjának. Ez a tilalom nem vonatkozik azokra a mesterséges intelligencia rendszerekre, amelyeket jóváhagyott terápiás célokra kívánnak használni, a velük kapcsolatba kerülő személyek vagy adott esetben a törvényes képviselőjük külön tájékoztatáson alapuló hozzájárulása alapján.*
- *az olyan mesterséges intelligencia rendszer forgalomba hozatala, üzembe helyezése vagy használata, amely kihasználja egy személy vagy személyek egy meghatározott csoportjának bármely sebezhetőségét, beleértve az ilyen személy vagy személyek csoportjának ismert vagy előre jelzett személyiségjegyeit vagy társadalmi vagy gazdasági helyzetét, életkorát,*

[413] a mesterséges intelligencia rendszerek magas kockázatú jelen besorolása ideiglenes, a mesterséges intelligencia használatáról szóló rendelet tervezetének 2023. május 16-i állapota alapján

[414] Ez a felsorolás nem érinti azokat az eseteket, amikor a mesterséges intelligencia gyakorlata más uniós jogot sért, ideértve az adatvédelemre, az esélyegyenlőségre, a fogyasztóvédelemre vagy a versenyre vonatkozó uniós jogszabályokat is.

fizikai vagy szellemi képességeit, azzal a céllal vagy azzal a hatással, hogy az adott személy vagy az e csoporthoz tartozó személy viselkedését olyan módon torzítsa lényegesen, amely jelentős kárt okoz vagy valószínűsíthetően okoz az adott személynek vagy más személynek.

- *olyan biometrikus kategorizálási rendszerek forgalomba hozatala, üzembe helyezése vagy használata, amelyek a természetes személyeket érzékeny vagy védett tulajdonságok vagy jellemzők alapján vagy az ilyen tulajdonságokra vagy jellemzőkre való következtetés alapján kategorizálják. Ez a tilalom nem vonatkozik azokra a mesterséges intelligencia rendszerekre, amelyeket jóváhagyott terápiás célokra kívánnak használni, a velük kapcsolatba kerülő személyek vagy adott esetben a törvényes képviselőjük külön tájékoztatáson alapuló hozzájárulása alapján.*
- *olyan mesterséges intelligenciával működő rendszerek forgalomba hozatala, üzembe helyezése vagy használata, amelyek természetes személyek vagy azok csoportjainak szociális pontozására, értékelésére vagy osztályozására szolgálnak egy bizonyos időszak alatt, szociális viselkedésük vagy ismert, következtetett vagy előre jelzett személyes vagy személyiségjellemzőik alapján, és a szociális pontozás az alábbiak valamelyikéhez vagy mindkettőhöz vezet:*
    - *bizonyos természetes személyek vagy azok csoportjainak hátrányos vagy kedvezőtlen kezelése olyan társadalmi kontextusokban, amelyek nem kapcsolódnak ahhoz a kontextushoz, amelyben az adatokat eredetileg generálták vagy gyűjtötték*
    - *egyes természetes személyek vagy azok csoportjainak olyan hátrányos vagy kedvezőtlen bánásmódja, amely indokolatlan vagy aránytalan a társadalmi viselkedésükhöz vagy annak súlyosságához képest.*
- *olyan mesterséges intelligenciával működő rendszer forgalomba hozatala, üzembe helyezése vagy használata, amely természetes személyek vagy azok csoportjainak kockázatértékelését végzi annak érdekében, hogy felmérje a természetes személy bűnelkövetési vagy bűnismétlési kockázatát, vagy előre jelezze egy tényleges vagy potenciális bűncselekmény vagy közigazgatási bűncselekmény bekövetkeztét vagy megismétlődését egy természetes személy profilalkotásán vagy személyiségjegyek és jellemzők értékelésén alapulóan, beleértve a személy tartózkodási helyét, vagy természetes személyek vagy természetes személyek csoportjainak korábbi bűnelkövetési magatartását.*
- *olyan mesterséges intelligenciával működő rendszerek forgalomba hozatala, üzembe helyezése vagy használata, amelyek arcfelismerő adatbázisokat hoznak létre vagy bővítenek arcfelismerő adatbázisokat az internetről vagy a térfigyelő kamerák felvételeiből származó arcképek céltalan lekérdezésével.*
- *a természetes személy érzelmeire következtető mesterséges intelligenciával működő rendszerek forgalomba hozatala, üzembe helyezése vagy használata a bűnüldözés, a határigazgatás, a munkahelyi és oktatási intézmények területén.*

- *"valós idejű" távoli biometrikus azonosító rendszerek használata nyilvánosan hozzáférhető helyeken.*
- *a nyilvánosan hozzáférhető terekben rögzített felvételek elemzésére szolgáló mesterséges intelligencia rendszerek üzembe helyezése vagy használata "utólagos" távoli biometrikus azonosító rendszerek segítségével, kivéve, ha az uniós joggal összhangban lévő előzetes bírósági engedélyhez kötött, és szigorúan szükséges az EUMSZ 83. cikkének (1) bekezdésében meghatározott, bűnüldözési céllal már elkövetett konkrét súlyos bűncselekményhez kapcsolódó célzott kutatáshoz.*

A rendelet tervezetének alkotói véleménye szerint

- *a nyilvánosan hozzáférhető helyeken a természetes személyek "valós idejű" távoli biometrikus azonosítására szolgáló mesterséges intelligenciarendszerek használata különösen beavatkozik az érintett személyek jogaiba és szabadságaiba, és végső soron hatással lehet a lakosság nagy részének magánéletére, a folyamatos megfigyelés érzését keltheti, a biometrikus azonosítást a nyilvánosan hozzáférhető helyeken alkalmazó feleket ellenőrizhetetlen hatalmi pozícióba helyezi, és közvetve visszatartja őket a gyülekezési szabadság és más, a jogállamiság alapját képező alapvető jogok gyakorlásától.*
- *a természetes személyek távoli biometrikus azonosítására szolgáló mesterséges intelligencia rendszerek technikai pontatlanságai elfogult eredményekhez vezethetnek, és diszkriminatív hatásokkal járhatnak. Ez különösen abban az esetben fontos, ha mindez életkor, etnikai hovatartozás, nem vagy fogyatékosság tekintetében történik.*
- *a hatás azonnalisága és az ilyen "valós időben" működő rendszerek használatával kapcsolatos további ellenőrzések vagy korrekciók korlátozott lehetőségei fokozott kockázatot jelentenek a bűnüldözési tevékenységekben érintett személyek jogaira és szabadságaira nézve.*

Ezért meg kell tiltani e rendszerek használatát nyilvánosan hozzáférhető helyeken.

Magas kockázatú mesterséges intelligencia rendszerek

A rendelet tervezet III. sz. melléklete határozza meg a magas kockázatúnak minősített MI-technológiákat, melyekre forgalomba hozataluk előtt szigorú kötelezettségek vonatkoznak majd.

A rendelet tervezete alapján[415] *magas kockázatú MI-technológia például:*

- *természetes személyek személyes jellemzőire vonatkozó, biometrikus vagy biometrikus alapú adatok alapján történő következtetések levonására szánt mesterséges intelligencia rendszerek, beleértve az érzelemfelismerő rendszerek (kivéve azokat a biometrikus ellenőrzésre szánt mesterséges intelligencia alapú rendszerek, amelyek kizárólagos célja annak*

[415] a mesterséges intelligencia rendszerek magas kockázatú jelen besorolása ideiglenes, a mesterséges intelligencia használatáról szóló rendelet tervezetének 2023. május 16-i állapota alapján

megerősítése, hogy egy adott természetes személy az a személy, akinek vallja magát)

- *az oktatás és a szakképzés területén*
    - *az olyan MI-rendszerek, amelyek célja a hozzáférés meghatározása, vagy az, hogy lényegesen befolyásolja a természetes személyek oktatási és szakképzési intézményekbe való felvételére vagy beosztására vonatkozó döntéseket*
    - *az oktatási és szakképzési intézményekben tanulók értékelésére, valamint az ezen intézményekbe való felvételhez általában szükséges tesztek résztvevőinek értékelésére szánt mesterséges intelligencia rendszerek*
        - *olyan rendszerek, amelyeket arra szánnak, hogy egy személy számára a megfelelő oktatási szint értékelésére használják, és amelyek lényegesen befolyásolják, hogy az adott személy milyen szintű oktatásban és szakképzésben fog részesülni vagy milyen szinthez fog tudni hozzáférni.*
        - *az oktatási és szakképzési intézményekkel összefüggésben/az oktatási és szakképzési intézményeken belül a tanulók tesztek során tanúsított tiltott magatartásának megfigyelésére és felderítésére szánt mesterséges intelligencia rendszerek*
- *a foglalkoztatás, munkaerő-gazdálkodás és az önfoglalkoztatáshoz való hozzáférés területén*
    - *természetes személyek toborzására vagy kiválasztására szánt mesterséges intelligencia rendszerek (célzott álláshirdetések feladására, a pályázatok szűrésére, a jelöltek értékelésére interjúk vagy tesztek során)*
    - *olyan mesterséges intelligenciát alkalmazó rendszerek, amelyeket arra szánnak, hogy a munkaviszonyok megkezdését, előléptetését és megszüntetését, a feladatok egyéni viselkedésen vagy személyes tulajdonságokon vagy jellemzőkön alapuló kiosztását, illetve az ilyen kapcsolatokban részt vevő személyek teljesítményének és viselkedésének nyomon követését és értékelését érintő döntéseket hozzanak vagy érdemben befolyásolják.*
- *a hitelképesség értékelésére szánt mesterséges intelligencia rendszerek természetes személyek hitelképességének megállapítására vagy hitelpontszámuk megállapítására, kivéve a pénzügyi csalás felderítésére használt mesterséges intelligenciával működő rendszerek*
- *a természetes személyek egészség- és életbiztosításra való jogosultságával kapcsolatos döntések meghozatalára vagy a döntések lényeges befolyásolására szánt mesterséges intelligencia rendszerek*
- *a természetes személyek által kezdeményezett segélyhívások értékelésére és osztályozására szánt mesterséges intelligenciával működő rendszerek, illetve a sürgősségi elsősegélynyújtó szolgálatok - beleértve a rendőrségi és rendvédelmi, tűzoltói és orvosi segélynyújtó szolgálatokat -, valamint a sürgősségi egészségügyi betegelosztó rendszerek diszpécserközvetítésére vagy prioritás megállapítására szolgáló rendszerek.*

Korlátozott, illetve minimális kockázatú rendszerek

A javaslat szerint korlátozott kockázatúak az olyan rendszerek, mint például a csevegőrobotok. Ezek használatakor a felhasználóknak tisztában kell lenniük azzal, hogy egy géppel kommunikálnak, és ezen információ alapján dönthetnek arról, hogy folytatják-e vagy inkább abbahagyják az adott tevékenységet.

Az érintettek jogaira és szabadságaira, valamint biztonságára nézve minimális kockázatú rendszerek szabadon használhatóak lesznek, ilyen például a mesterséges intelligencián alapuló videojátékok vagy a spamszűrők.

AZ ADAT ÉLETÚTJA A SZERVEZETEN BELÜL

Az adatok életútjának feltérképezéséhez tudnunk kell, hogy

- ✓ milyen adatokat kezelünk (pontosan, nem csak körülbelül);
- ✓ milyen cél érdekében kezeljük ezeket az adatokat (csak úgy vannak, vagy használjuk is őket valamire, illetve jogszerűen vannak-e nálunk);
- ✓ ezen adatok elvesztése / megsemmisülése / kompromittálódása milyen károkat okozhat számunkra (lásd adatvédelmi incidenssel kapcsolatos problémák).

Az adat nem egy állandó valami – az adatok jönnek-mennek, gyűlnek, változnak, többszöröződnek, megsemmisülnek miközben és újra meg újra bejárják többé-kevésbé hasonló életútjukat úgy, hogy sokkal kevésbé nyomon követhetőek, mint például egy íróasztal vagy egy számítógép. Sőt, az adat fő jellemzője, hogy úgy tud „közlekedni", hogy közben az eredeti helyén is ott marad és az sem biztos, hogy valaha is kiderül, valaki „elvitte" (lemásolta, letöltötte, ellopta stb.) azokat.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A Hatósághoz 2019. december 29-én közérdekű bejelentés érkezett, amely arra hívta fel a figyelmet, hogy a https://www.lastminute.robinsontours.hu/partnerkapu_foglalasaim weboldalon keresztül bárki számára elérhetőek Ügyfél 1. természetes személy ügyfeleinek személyes adatai, így többek között utasok neve, elérhetőségei, lakcímadatok, személyi igazolvány és útlevélszámok, foglalással és utazással, úticéllal, szállással valamint a szerződéskötéssel kapcsolatos adatok. Az adatok https://www.robinsontours.hu/partnerkapu foglalasaim linken keresztül is elérhetőek voltak. A bejelentés szerint erre a bejelentő úgy jött rá, hogy internetes böngészés közben édesapja nevét írta be a Google keresőjébe, majd az egyik találaton keresztül, bármilyen jogosultság ellenőrzés nélkül sikerült megnyitnia egy adatbázist.

A Hatóság ellenőrizte a fenti linkeket és NAIH/2020/66/2., NAIH/2020/66/3. és NAIH/2020/66/5. ügyiratszámú feljegyzéseiben megállapította, hogy a linkek birtokában, azt a webböngészőbe beírva, bármilyen jogosultságellenőrzés, vagy más informatikai biztonsági intézkedés közbeiktatása nélkül a weboldalon – a bejelentő által állítottaknak megfelelően – elérhető egy adatbázis, amely különböző természetes személy ügyfelek személyes adatait tartalmazza. Az adatbázisban található adatok alapján valószínűsíthető, hogy a legtöbben az utazási irodaként működő Ügyfél 1. utazási szolgáltatásait igénybe vevő ügyfelek. A Hatóság arról is meggyőződött, hogy az adatbázisban tárolt adatokhoz a Google keresőben rákeresve (pl. egy utas nevére való keresés) is el lehet jutni. A tartalmakat tehát a Google keresőmotorja is felderítette, és abban ezeket kulcsszavas kereséssel elérhetővé tette. (...)
A linkeken keresztül elérhető adatbázisból lehetőség volt arra is, hogy az egyes ügyfelekkel kötött utazási szerződéseket bárki szabadon letölthesse pdf formátumban. (...)

A Hatóság (...) a magas kockázatot megalapozó körülményként értékeli, hogy az adatbázishoz mind a közérdekű bejelentő, mind a Hatóság hozzáfért, viszont az illetéktelen hozzáférések teljes száma és a hozzáférők személye a sérülékenység idejére vonatkozó teljes naplóállomány hiányában nem mérhető pontosan fel. A hozzáférők személyét és számát Ügyfél 1. utólag már nem tudja felmérni és azonosítani, amely az incidensben érintett személyes adatok további sorsával kapcsolatban nagyfokú bizonytalanságra, aggodalomra ad okot. Az adatkezelő az általa felmérhetetlen fokú és mértékű, de bizonyítottan megtörtént adatszivárgásnál csak az érintettek tájékoztatásával próbálhatja meg csökkenti jelen esetben az egyébként is magas kockázatokat.

A Hatóság megítélése szerint a magas kockázatot megalapozó további körülmények, hogy az adatbázisban kezelt személyes adatokat a Google is indexálta, azok ezen keresőmotoron keresztül is elérhetőek voltak, így azokra sokkal könnyebben rá lehetett akár egyszerű internetes böngészés, névre történő találomra való rákeresés során is bukkanni."[416]

Adatokkal foglalkozóként feladatunk, hogy ezeket a folyamatokat feltérképezzük mintegy pillanatképet alkotva az adatkezelési tevékenységeinkről, illetve a változásokat nyomon kövessük és ezeket a térképeket folyamatosan napra készen tartsuk.

Az adat életútja

1. Az adatok előállása (keletkezése)

Az adatok többé-kevésbé tudatosan kerülnek be a különféle adatkezeléseinkbe. Azért csak többé-kevésbé tudatosan, mert vannak olyan személyes adatok, amelyeket – annak ellenére, hogy nem kívánjuk kezelni őket – mégis a birtokunkban vannak.

Példa

A munkavállaló (alkalmazott) a céges e-mail fiókját még a leghatározottabb tiltásunk ellenére is magánlevelezésre használja. Még az is előfordulhat, ő maga ártatlan, csak az üzleti partner írta meg neki tájékoztatásul, hogy egy darabig nem tud vele találkozni személyesen mert a kocsijából kiszállva egy jégfolton elcsúszott,

[416] NAIH/2020/66/21. https://www.naih.hu/files/NAIH-2020-0066-21-hatarozat.pdf, utolsó letöltés: 2022-07-25

eltört a lába, most otthon lábadozik és még beletelik egy kis időbe mire olyan járógipszet kap, amivel el mer indulni.
A példa alapján láthatjuk, mennyi személyes adat lehet úgy egyetlen mondatban (ezek egy része ráadásul még különleges adat is), hogy azzal kapcsolatban adatkezelőként semmilyen adatkezelési célunk sincs, sőt valójában ezeket az adatokat nagyon nem szeretnénk kezelni. Mindez a céges (szolgálati) e-mail fiókba postázva, tiltás ide vagy oda. Ha pedig a fiók gazdája éppen nyaral vagy egyéb sürgős okból a főnökének be kellett lépnie a fiókjába, máris olyan személy is láthatta azt a közlést, akinek nem szánták azt.

- ✓ Megtiltottuk a céges (szolgálati) e-mail fiók privát célú használatát? *Meg.*
- ✓ El tudjuk kerülni privát adatnak a szervezetünk e-mail fiókjában landolását? *Nem.*
- ✓ Meg akarta szegni a munkavállaló (alkalmazott) a tiltásainkat? *Nem.*
- ✓ Meg akarjuk ismerni a csak a munkavállalónknak szánt bizalmas közlést? *Nem.*
- ✓ Akarjuk kezelni (tárolni, megtekinteni stb.) más privát adatát? *Nem, és mégis nálunk vannak ezek az adatok, akár akarjuk, akár nem.*
- ✓ Azzal, hogy a mi munkavállalónk e-mail fiókjában vannak ezek a személyes adatok, azzal elveszítették személyes és privát jellegüket? *Nem. Még akkor sem, ha nagyon szeretnénk.*

A példában bemutatott és a hasonló esetek miatt vagyunk kénytelenek rendszeresíteni olyan eljárási szabályokat, amelyek életbe léptetésével nem, vagy ha már mindenképpen, akkor csak a lehető legminimálisabb mértékben hatolunk bele a munkavállalóink (alkalmazottjaink) és levelezőpartnereik privát szférájába.

Példa

- ✓ *munkavállalónk (alkalmazottunk) az üzleti partner gyógyulófélben lévő képviselőjének vidám vicces videót küld vissza válaszul (a videóban látható sok cuki macskától/kutyától majd biztos jobban érzi magát) plusz javasolja, hogy nézegesse a tavalyi Karib-tengeri nyaralásán készült felvételeit, csak hogy kiszakadjon a zaklatott és fájdalmas jelenéből.*

A levélváltásokkal a kényszerűségből kezelt privát adatok száma sokszorozódik, ráadásul nemcsak a mi, hanem az üzleti partnerünk hivatalos tárhelyén is. Ezek után nem szabad csodálkoznunk, ha a munkavállaló e-mail fiókjának egy esetleges kinyitása/ellenőrzése giga-fejtörést okoz mind nekünk, mind a szervezetünk IT-szakembereinek, mind az adatvédelmi tisztviselőnknek.

Az ilyen helyzetek miatt is nagyon fontos, hogy tudatában legyünk annak, a szervezetünkön belül kihez és hogyan érkezhetnek be az adatok (például papír alapon a postával, elektronikus levélben gyűjtő e-mail címre, egyénileg kezelt hivatalos e-mail címekre, közös adatbázishoz hozzáféréssel stb.), hiszen már az első stádiumban, azaz az adatok kezelésének megkezdésekor is meg kell felelnünk az adatvédelmi alapkövetelményeinek (jogszerűség, célhoz kötöttség, adattakarékosság stb.).

2. Az adat tárolása

Az adatok nem csak úgy lógnak a levegőben, hanem tároljuk azokat valahol, akár papíron, akár elektronikus formában is állnak azok a rendelkezésünkre. A papír alapú irattározás hagyományai évszázadokra nyúlnak vissza, ha pedig fogy a hely, jöhet a selejtezés még akkor is, ha eredetileg nem akartuk ilyen „felesleges" elfoglaltsággal tölteni a rendelkezésünkre álló munkaórákat, mindennek keretrendszerét pedig hagyományosan az „Iratkezelési Szabályzat és Irattári Terv" szokta meghatározni. Ahogy azt is, mely iratot kell minősítettként kezelnünk, plusz tárolási és kezelési feltételeket generálva.

A digitális transzformáció ugyan csökkentheti a papírok mennyiségét, de nem feltétlen – dönthetünk úgy is, biztos ami biztos, legyen minden meg papíron és digitális formában is, illetve egyes szervezetek nehezebben állnak át az e-papírra, míg mások könnyebben és mind a mai napig bevált megközelítés az „*írd be az online felületre, aztán nyomtasd ki, pecsételd le és postán küld el"* megoldás. Sőt, mind a mai napig vannak olyan hivatalok, akik azzal kezdik az ügyfelektől kapott e-dokumentáció áttekintését, hogy kinyomtatják az egészet úgy, ahogy van.

Sokkal bonyolultabb a helyzet az elektronikus formában létező adatok esetén, azok ugyanis megfoghatatlanok és az átlag adatkezelő számára szinte nyom nélkül és követhetetlenül sokszorosíthatók. Az adatok lehetnek birtokunkban lévő adathordozón (laptopon, telefonon, memóriakártyán stb.), de központi szerveren vagy akár a felhőben is tárolhatjuk azokat, bárhol a nagyvilágban úgy, hogy adott esetben mi sem tudjuk, pontosan melyik joghatóság alatt vannak. És mivel nem folyóméterben tároljuk a polcon, fel sem tűnik, hogy egyre több tárhelyet foglalunk, ezen egyedül csak az előrelátóbb rendszergazdák szoktak aggódni.

Tovább bonyolítja a tárolás problémakörét az is, hogy az adatok lehetnek önálló adatbázisban, de akár közös adatkezelővel közös adatbázisban is, és akkor még a multinacionális vállalatcsoportok öt kontinenst felölelő adatbázisait még meg sem említettük.

Példa

Francia központú multinacionális vállalatcsoport

- ✓ *projektjét a lengyel kollégák készítik elő, melyhez algériai referenciát használnak,*
- ✓ *a tendert kiíró norvég céggel a beszállítói szerződést az osztrák leányvállalattal köti meg,*
- ✓ *a folyamat során bekerülnek a személyes adatok abba a globális adatbázisba, amelyet az Egyesült Királyságban jegyzett leányvállalat kezel, a tárhelyszolgáltató székhelye Kalifornia, a tárhelyszolgáltatás tényleges (fizikai) helye pedig Izland,*
- ✓ *a szerződést az értékhatár miatt a holland leányvállalat kötelékében dolgozó vezető jegyzi ellen (látva minden személyes adatot),*
- ✓ *a kanadai compliance csoport ellenőrzi az üzleti partnert és a megfelelőségét (pénzmosás, tiltólistákon szereplés stb., alaposan megvizsgálva minden egyes személyes adatot),*

- ✓ *a tényleges teljesítés Bulgáriában és Törökországban történik,*
- ✓ *az ügyfélszolgálat és szervízügyintézés Szlovákiában van,*
- ✓ *a számlát a horvát leány e-mail címén fogadják be és*
- ✓ *Indiában kezdeményezik a kifizetést,*
- ✓ *ha pedig visszaélés-bejelentésre adná a fejét bárki is a tenderrel és a szerződéssel kapcsolatban, azt egy bostoni ügyvédi iroda honlapján teheti meg,*
- ✓ *az adatvédelemmel, illetve érintetti jogokkal kapcsolatban pedig a németországi leányvállalat adatvédelmi tisztviselője tud érdemi felvilágosítást adni,*
- ✓ *a projekt teljesítésébe pedig számtalan más multi bonyolódik még bele, pl. logisztika, IT-infrastruktúra, biztosítás, pénzügyi és egyéb szolgáltatások terén, adatfeldolgozók, közös adatkezelők és együttműködő önálló adatkezelők kibogozhatatlan hálóját szőve.*

A személyes adatok esetében nem feltétel, hogy az adatok a fizikai térben együtt legyenek azokkal, akik hozzáférnek (ellentétben a papír alapon tárolt adatokkal), illetve a hozzáférők száma – alapesetben – nem módosítja az adatok minőségét.

Az egyre összetettebb adatkezelési konstrukciókban az egy adott adatbázis ugyanazon adatához kötődő számtalan adatkezelés miatt a tárolás és megsemmisítés követelményei messze túlmutatnak a hagyományos adattárolásban megszokott követelményeken, gondoljuk akár csak a hatalmas e-mail forgalom személyes adattartalmára, a különféle tárolási időtartamok és megsemmisítési időpontok automatizmusként folyamatba építésére, a redundáns szerverekre vagy a rendszeres biztonsági mentésekre és azok ki tudja hol tárolására. Hasonlóan problematikus lehet a különböző adatbázisok összevezetése, az adatok kombinálása és azokból újabb és újabb adat előállítása.

A dán adatvédelmi hatóság (Datatilsynet) gyakorlatából

A Datatilsynet megrovásban részesítette a dán Egészségügyi Adatvédelmi Hivatalt (Sundhedsdatastyrelsen), mivel megsértve a biztonsági követelményeket személyes adatokat tárolt egy olyan szerveren, ahol azokhoz az alkalmazottak hozzáférhettek annak ellenére, hogy a meglévő belső iránymutatások tiltották az ilyen tárolást. Az adatvédelmi hatóság úgy ítélte meg, hogy ezek az iránymutatások nem elegendőek abban az esetben, amennyiben az adatkezelő nem ellenőrzi, hogy a gyakorlatban valóban betartják-e azokat.

A Hivatal egy korábbi alkalmazottja a Hivatal belső iránymutatásai és eljárásai ellenére tévedésből álnevesített adatkészleteket tárolt a Microsoft Azure szerverein, amelyeket a feladatok kezelésére használtak. Az adatok polgárokkal kapcsolatos álnevesített bizalmas információkat tartalmaztak, amelyeket a megbízható alkalmazottak „dekódolhattak". A Hivatal csak egy évvel később fedezte fel, hogy az adatokat olyan helyen tárolták, ahol az nem volt megengedett.

Az adatvédelmi hatóság hangsúlyozta, hogy az adatkezelőnek

- ✓ *megfelelő technikai és szervezési intézkedéseket kell végrehajtania a kockázatnak megfelelő biztonsági szint biztosítása érdekében.*

- ✓ *belső iránymutatásokat és eljárásokat kell bevezetnie, amelyek megtiltják a személyes adatok tárolását olyan rendszerekben, amelyeket nem ilyen tárolásra szántak.*
- ✓ *rendszeresen (manuálisan vagy automatikusan) ellenőriznie kell azt is, hogy a személyes adatok (akár tévedésből, akár nem) mégis ott kerültek-e tárolásra.*

A Hivatal nem tett eleget ez utóbbi követelménynek.
Mivel a személyes adatokat álnevesítették, és a szerverhez csak az arra felhatalmazott alkalmazottaknak volt hozzáférése, a Datatilsynet csak megrovást alkalmazott az adatkezelővel szemben.[417]

3. Az adatok „használata”

Nem azért gyűjtünk adatokat, hogy azok csak úgy álljanak az adatraktárunkban, egyszer csak jó lesz valamire alapon (ez egyébként is tilos a GDPR 5. cikkben foglalt alapelvei alapján), a birtokunkban lévő adatokat adatkezelési céljaink mértékében használjuk is.

Példa:

Egy gyártással foglalkozó társaság bérszámfejtői a különféle szervezeti egységektől, így – többek között – a termeléstől, a HR (személyzeti) osztálytól, munkavédelemmel foglalkozó szervezeti egységtől, biztonsági szolgálattól stb. kapott információk segítségével dolgoznak:

- ✓ *a műszakvezetők jelentése alapján a munkavállalókhoz hozzárendelik az adott hónapban nyújtott teljesítményünket,*
- ✓ *korrigálják az adatokat a szabadságos napokkal meg a betegállományban töltött napokkal,*
- ✓ *a jól dolgozókat bónusszal jutalmazzák,*
- ✓ *hozzácsapják még a különféle cafeteria meg egyéb belső szabályzatok alapján járó juttatásokat (például home office pótlék stb.),*
- ✓ *levonják a levonandókat (például névre kiadott munkaeszköz elvesztése vagy a céges autó saját hibás összetörése miatt fizetendő összeget stb.),*
- ✓ *kiszámolják, egy adott munkavállaló mennyi fizetést érdemel az adott hónapban (elszámolási időszakban),*
- ✓ *majd jöhet a bruttó nettósítása, azaz a különféle adó- és társadalombiztosítási kötelezettségek teljesítése az állam felé,*
- ✓ *a különféle okok miatti kötelező levonások levonása (például gyerektartás összege) és pénzügyi rendezése (a megadott bankszámlaszámra átutalása stb.),*
- ✓ *a végén pedig a munkavállaló az általa megadott bankszámlára megkapja a maradék, immáron nettó összeget.*

[417] Sundhedsdatastyrelsen får kritik for manglende kontrol med personoplysninger i it-miljø, https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/sundhedsdatastyrelsen-faar-kritik-for-manglende-kontrol-med-personoplysninger-i-it-miljoe, utolsó letöltés: 2022. 09. 04.

Ezek az események kisebb-nagyobb módosulással ismétlődnek minden hónapban, az óra körbejár, a munkáltató pedig fáradhatatlanul gyűjtögeti-rendszerezi és használja a rendelkezésére álló adatokat annak érdekében, hogy a szervezet célkitűzéseit megvalósítsa (azaz a társaság a termékeit jó áron értékesítse, ebből hasznot szerezzen és finanszírozni tudja további működését a tulajdonosok legnagyobb megelégedésére).

4. Az adatok megosztása

Vannak olyan adatkezelések, amelyek szigorúan megmaradnak a szervezet berkein belül, azonban vannak olyan adatok is, amelyeket meg kell osztanunk másokkal.

Példa:

- ✓ *a munkavállalók jövedelmével kapcsolatos adatokat – jogi kötelezettség alapján és a mindenkori hatályos vonatkozó jogszabályokban előírt mértékben – meg kell küldenünk az adóhivatalnak,*
- ✓ *a szervezet által szervezett felnőttoktatásban részt vevők adatait meg kell küldenünk az ezen adatok nyilvántartására szakosodott állami nyilvántartásba,*
- ✓ *a munkavállalók adatait meg kell osztanunk a foglalkozás-egészségügyi szolgáltatóval, aki elvégzi a munkakörök ellátásához szükséges foglalkozás-egészségügyi alkalmassági vizsgálatokat,*
- ✓ *amennyiben olyan baleset éri a munkavállalót, amely esetére a munkáltató kötött csoportos biztosítást, abban az esetben a munkavédelemre szakosodott adatfeldolgozónk kivizsgálja és jelenti az esetet oda, ahova jelentenie kell, majd a biztosítónak is meg kell küldenünk a balesettel kapcsolatos adatokat,*
- ✓ *hatósági ellenőrzés során meg kell adnunk az adott ellenőrzéssel érintett munkavállalóink adatait,*
- ✓ *csapatépítő buli szervezése esetén át kell adnunk a résztvevők adatait a szálláshelynek, az étkezést, valamint a buszt biztosító cégnek.*

Az adatmegosztásos kötelezettségek folyamatosan változnak, a szervezet felelőssége ezen adattovábbítások végrehajtása, miközben az érintettek alig, vagy egyáltalán nem tudják befolyásolni a személyes adataik akár kontinenseken átívelő vándorlását.

Az adatátadások – mint adatkezelési műveletek – esetében ugyanúgy jogalapra kell hivatkoznunk, mint egyéb adatkezelési tevékenységek esetében, és mint az előző példákból is látható, adatkezelőként gyakran előfordulhat, hogy az adatmegosztásokat nem jogi kötelezettségre hivatkozva végezzük.

Például:

- ✓ *a munkavállalóink számára olyan céges autót biztosítunk, amelyet flottaüzemeltető cégtől bérlünk, és amelynek üzemeltetéssel kapcsolatban bizonyos adatokat át kell adnunk (pl. a gépjármű vezetésére felhatalmazottak neve, kilométeróraállás stb.),*
- ✓ *a fejvadászcég átadja a jelöltek nevét,*

- ✓ *Kínában folyamatban lévő projekt miatt a munkavállalóinknak ki kell utaznia bizonyos munkafolyamatok elvégzéséhez és ennek érdekében szállást meg repülőjegyet foglalunk a számukra,*
- ✓ *a munkavállalóink számára céges hitelkártyát biztosítunk a külföldi kiküldetésük időtartamára,*
- ✓ *az alkalmazottjaink gyermekeinek kedvezményes nyári tábort szervezünk és a tábort ténylegesen szervezőnek átadjuk a résztvevők adatait,*
- ✓ *irodát bérlünk és az irodaház üzemeltetőjének átadjuk a munkavállalóink és az általunk fogadott üzleti partnereink adatait annak érdekében, hogy azok beléphessenek az irodaház területére.*

Az adatvédelmi jogszabályok megkívánják, hogy – az elszámoltathatóság elvének megfelelve – az adatmegosztásainkkal az érintettek felé el tudjunk számolni (pl. adatfeldolgozási megállapodás, közös adatkezelés tárgyában készült megállapodás, rendszeres/eseti átadásról szóló megállapodás, adattovábbítási nyilvántartás vezetése stb.).

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„(…) az adatok begyűjtése és továbbítása önmagában általában nem elkülönült adatkezelés, csak egy adatkezelési folyamat első művelete, amely az érdemi adatkezelést készíti elő, és az érdemi adatkezelés nélkül nincs saját célja és eredménye. Az egy célt és egy eredmény elérését – jelen esetben Importőr érdekéből történő felmérést – szolgáló adatkezelési műveletek nem vizsgálhatóak egyenként, azok jogalapja, jogszerűsége attól függ, hogy az összes egy célt szolgáló adatkezelési művelet jogszerű-e, azok egyike sem valósít meg adatvédelmi jogsértést.”[418]

5. Az adatok archiválása

Az archiválást ne keverjük össze a biztonsági mentés készítésével.

A rendszeres biztonsági mentés elengedhetetlen adataink védelme szempontjából, célja lehet például

- az adatvesztés megelőzése, amelyet okozhat hardverhiba, vírus, szoftverhiba, fizikai sérülés, vagy akár emberi hiba és bűncselekmény (pl. számítógép ellopása) is. A rendszeres biztonsági mentések lehetővé teszik, hogy az adatokat helyreállítsuk és megakadályozzuk az értékes adataink végleges elvesztését.
- olyan rosszindulatú, például zsarolóvírosus támadások elleni védelem, amelyek célja az adataink megszerzése, titkosítása vagy tönkretétele, majd váltságdíj kérés a visszaállításhoz. A biztonsági mentések lehetővé teszik a fertőzött rendszer visszaállítását a támadás előtti állapotba, és a segítségükkel minimalizálhatjuk a károkat.
- helyreállíthatóság és folytonosság biztosítása, adott esetben megkönnyítve a munka folytatását, minimalizálva az időbeli kiesést.

[418] NAIH-2857-20/2021

- idő és energia megtakarítása, mivel egy esetleges rendkívüli esemény (pl. adatvesztés, támadás stb.) esetén az adatok újra előállítása vagy helyreállítása sokkal időigényesebb és stresszesebb lehet, mint a rendszeres biztonsági mentés.

Olyan nincs, hogy a birtokunkban lévő összes adat aktív adat – az adatok egy részére aktuálisan nincs szükségünk, ám ez nem mindig jelenti egyben azt is, hogy már soha nem is lesz rá szükségünk, azaz megszűnt az adatokkal kapcsolatos adatkezelési célunk. Minden valamirevaló adatkezelő tudja, bármikor jöhet olyan hivatalos megkeresés, amelynek megfelelve áshatjuk elő az irattárunk (tárhelyeink) legmélyéről a szükséges adatokat, illetve az is előfordulhat, hogy bíróság előtt kell az archívumból előbányászott adatokkal alátámasztanunk az álláspontunkat.

Példa

- ✓ *adóvizsgálatnál sok évre visszamenőleg kell elővarázsolnunk az összes teljesítési igazolást meg egyéb, a kifizetések jogszerűségét alátámasztó adatot,*
- ✓ *egykori munkavállalónk beperli a munkáltatónkat (mint adatkezelőt) munkahelyi baleset következtében elszenvedett tartós egészségkárosodása miatt,*
- ✓ *diszkrimináció miatt jelentenek fel minket (mint adatkezelőt),*
- ✓ *érintetti kérelmet kell teljesítenünk.*

Az adatok „régisége” relatív, hiszen másként „régi” egy belépőrendszerben nyilvántartott, a rendszerrel védett épületben történt mozgással kapcsolatos adat és másként egy húsz évvel korábbi, akkoriban forradalmian új technológiával pózoló fejlesztőmérnök fotója.

Az adatok archiválásának célja az adataink hosszú távú megőrzése és megfelelőségük, illetve a mi megfelelőségünk biztosítása:

- az archiválása lehetővé teszi az adataink hosszú távú megőrzését, archívumokban vagy más tárolási rendszerekben. Fontos, hogy az adataink mindaddig elérhetők és „épek” maradjanak, ameddig erre nekünk szükségünk van, például jogszabályban meghatározott megőrzési kötelezettségünk miatt.
- az adatok archiválása lehetővé teszi a tárolási erőforrásaink hatékonyabb kihasználását. Az aktív adatokat, amelyeket intenzíven használunk, tárolhatóak a fő tárolórendszereinkben, míg a kevésbé aktív vagy inaktív adatok átkerülhetnek az archívumokba. Ez csökkentheti a tárolási költségeinket és javíthatja az adatokhoz való hozzáférést a rendszerekben.
- az archivált adatok értékes erőforrást jelenthetnek a kutatásainkhoz és elemzéseinkhez, különösen akkor, ha szükségünk van hosszú távú adatok összehasonlítására és elemzésére a trendek azonosításában, illetve a történelmi összefüggések megértésében.

Az adatvédelemre vonatkozó jogszabályok alapján az adat életútjának vége mindig annak függvénye, van-e jogszerű adatkezelési célunk az adott adattal kapcsolatban – ha nincs, akkor vagy másik jogszerű célra kell hivatkozunk (ha találunk ilyet), vagy véglegesen be kell szüntetnünk az adott adat kezelését (selejtezés, törlés stb.)

Példa

- ✓ *úgy döntünk, a régi kutatások során készült feljegyzésekre, jegyzőkönyvekre és felvételekre már nincs szükségünk (azaz megszűnt az adatkezelési célunk), azonban szeretnénk egy házi múzeumot létesíteni, amelyben a cég történetét és eredményeit meséljük el az utókornak és itt ki szeretnénk állítani a kutatási naplókat és a felvételek egy részét (új adatkezelési célt határozunk meg).*
- ✓ *megőrizzük egy adott projekt pénzügyi elszámolásával kapcsolatos adatokat mindaddig, amíg erre jogszabály alapján kötelezettségünk van, ezen időszak után pedig megsemmisítjük a projekt teljesítésével és pénzügyi elszámolásával kapcsolatos adatokat azok személyes adattartalmával együtt.*

6. Az adatok megsemmisítése

Az adatvédelmi alapelveknek köszönhetően az adatok többsége nem örökszavatos, azaz ha az adatkezelési céljukat elérték már nincs szükség rájuk. Miért tartanánk meg olyan személyes adatot, amely tekintetében a jogi igény érvényesíthetősége már elévült és egyébként is mindenféle szempontból érdektelen a ma és a holnap számára is?

Vannak olyan adatok, amelyek nem, vagy csak évtizedek elteltével selejtezhetőek, ilyenek például egyes cégiratok vagy a munkavállalók jogszabályban meghatározott adatai (például a nyugdíjszámításhoz szükséges adatok). De vajon az, hogy a munkavállalók gyermekei öt évvel ezelőtt mit kértek a céges Mikulástól, az fontos még bárkinek is? Kizárt, hacsak nem vállalat- és kultúrtörténeti szempontból… Ez esetben pedig még mindig anonimizálhatjuk az adatokat és már meg is oldottuk, hogy ne vonatkozzon rájuk a GDPR.

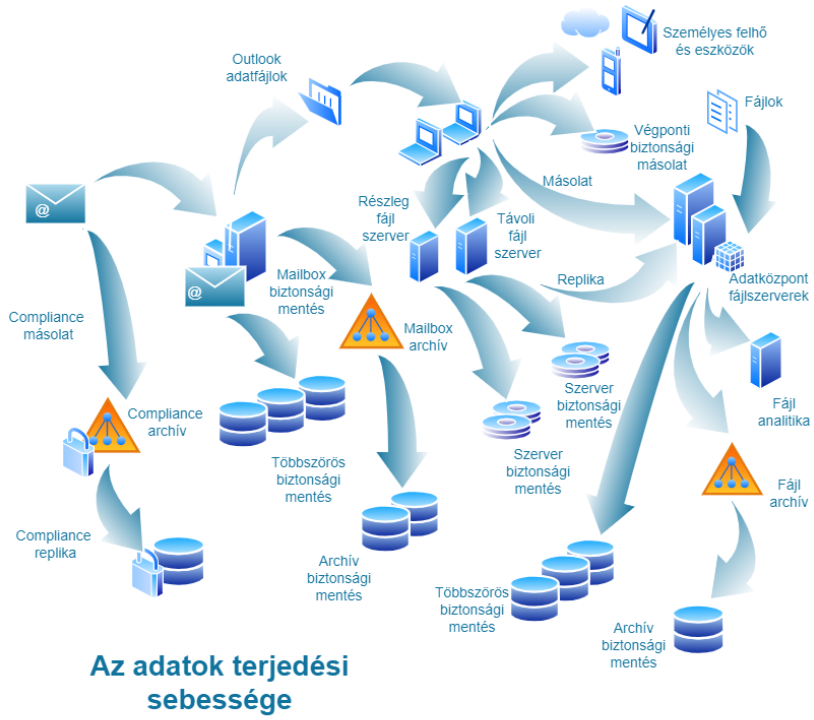
Adatkezelőként törekednünk kell arra, hogy amennyiben az adatok megsemmisítésére (törlésére) vállalkozunk, akkor ez a megsemmisítés (törlés) visszafordíthatatlan legyen – jöhet a papírok ledarálása után a felügyelt újrahasznosítás, illetve az elektronikus adatok visszaállíthatatlan törlése.

Az adatok multiplikálódása

Minél összetettebb az IT rendszerünk, annál nagyobb az esélye annak, hogy egyetlen személyes adat röpke idő alatt megsokszorozódik és belekerül különböző aktív fájlokba és archiválódik biztonsági mentésekben. És míg régen a papírmásolatok viszonylag könnyen nyomon követhetőek voltak (például a másolati példányok elosztási listáin keresztül), addig a digitális adatok szinte észrevétlenül és megállíthatatlanul multiplikálódhatnak.

A gyakran követhetetlen sokszorozódás nemcsak a törlés miatt okozhat problémát, hanem sziszifuszi feladatot eredményezhet a hibás adatok helyesbítésénél és az érintetti kérelmek teljesítésénél is, mivel nemcsak azt kell tudnunk megmondanunk, hogy melyik adat miért, mikor és hova került, hanem adott esetben minden egyes példányban (papíron, adatbázisban) korrigálnunk kell a hibás adatot.

A törlési kérelmek („elfeledtetés joga”, tiltakozás és hozzájárulás visszavonásának érvényesítése) esetén amennyiben egy adatot törölnünk kell, akkor ez a törlési kötelezettség az adatvédelmi szabályok szellemiségét követve minden egyes feltalálási-tárolási helyre vonatkozik. Ezek felkutatása régebben még viszonylag könnyű feladat volt (adat feketével kisatírozva vagy az egész papír dossziéból kiemelve és lezúzva, másolati példányok elégetve stb.), napjainkban azonban a teljes és visszaállíthatatlan törlés követelménye meglehetősen magasra helyezi a lécet az informatikai szakemberek előtt.



Ezek után nem csodálkozhatunk, ha egy adott adat törlésére kiadott parancsra az IT szakemberek többsége csak legyint, „aki ezt kitalálta, az sem ismeri a modern rendszereket” és annyit tesz, hogy a könnyen elérhető, látható helyekről eltünteti azt, ami eltüntetni rendeltetett. Mi, adatkezelők pedig reménykedünk, sem az érintett hatóság, sem pedig más sem fogja soha megtalálni azokat a különféle mentésekben, naplófájlokban és egyéb helyeken kallódó személyes adatokat, amelyeket elviekben visszaállíthatatlanul törölnünk kellett volna.

És mit tehetünk? Legegyszerűbb, ha adminisztratív eszközökkel megelőzzük a személyes adatok felesleges multiplikálódását, illetve amint erre módunk van – az adatkezelési céljaink függvényében – anonimizáljuk az adatokat.

Mire kell másolat?

Adatkezelőként hajlamosak vagyunk papírt papírra halmozni, a kupacok növelésére pedig mi a legkézenfekvőbb? Egyrészt a másolat másolatát is begyűjteni (nehogy elvesszen a „fontos" irat, soha nem árt belőle még egy példány), másrészt úgy készítünk okmányokról (okiratokról) digitális- és papírmásolatot, hogy ezen másolatok puszta létezése is messze meghaladja az adatvédelem alapelveit figyelembe vevő szükséges és arányos adatkezelést.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„(…) bekért, a személyazonosság igazolására alkalmas hatósági igazolványról (azaz a személyazonosító igazolványról, vezetői engedélyről vagy útlevélről, a továbbiakban együtt: hatósági igazolvány) készített ***elektronikus másolatok gyűjtése, tárolása****, illetve az annak felhasználásával megvalósuló* ***adategyeztetés*** *is a* ***GDPR hatálya alá tartozó adatkezelés*** *az azokon rögzített személyes adatokra tekintettel (…)*

A Hatóság álláspontja szerint pusztán egy – hitelesnek nem tekinthető – okmánymásolat alapján utólag rendkívül nehezen bizonyítható az, hogy az okmány bemutatásakor az okmányt felmutató személy ténylegesen megegyezett azzal a személlyel, akinek a képmását az okmány tartalmazta."[419]

Az okmányokról másolat készítése sok esetben azon a téves feltevésen alapszik, miszerint a másolat felhasználható a későbbiekben bizonyításra (arra csak az eredeti alkalmas vagy a hitelesített másolat), miközben a másolatok olyan adatokat tartalmazhatnak, amelyeket nem kezelhetünk a másolás alapját adó adatkezelés keretében (lásd alapelvek, adattakarékosság, célhoz kötöttség stb.).

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Az árvaság, félárvaság olyan szempont, amit az Egyetem a Korm. rendelet[420] *16. § (2), illetve (3) bekezdése alapján köteles figyelembe venni.*

A Hatóság álláspontja szerint megfelelő gyakorlat, hogy az Egyetem az árvaság vagy félárvaság eseteit a halotti anyakönyvi kivonattal tartja szükségesnek igazolni, ugyanis ezen okmány tudja alátámasztani a halál tényét.

A teljes halotti anyakönyvi kivonat azonban a következő adatokat tartalmazza: az elhalt házassági nevét, születési családi és utónevét, nemét, családi állapotát, születési helyét és idejét vagy életkorát, igazolt nem magyar állampolgárságát, hontalanságát vagy ismeretlen állampolgárságát, magyar állampolgárságának megszűnését, a haláleset helyét és idejét, az elhalt apjának és anyjának születési családi és utónevét, az elhalt házastársának vagy bejegyzett élettársának születési családi és utónevét, a halál tényének bírósági határozattal történt megállapítása

[419] NAIH/2020/3535/2

[420] A felsőoktatásban részt vevő hallgatók juttatásairól és az általuk fizetendő egyes térítésekről szóló 51/2007. (III. 26.) Korm. rendelet

esetén a bíróság megnevezését, a határozat számát, a határozat jogerőre emelkedésének időpontját, a holtnak nyilvánítás esetén a határozatot hozó bíróság megnevezését, a határozat számát, a határozat jogerőre emelkedésének időpontját.

A teljes okmány tehát olyan adatokat is tartalmaz, amely kezelése nem szükséges az Egyetem számára az elbírálás során: elegendő, ha az okmányból kitűnik a halál ténye, illetve, ha az elhunyt személye beazonosítható.

A halotti anyakönyvi kivonat teljes másolatának kezelése a GDPR 5. cikk (1) bekezdés c) pontjába [az adattakarékosság elvébe] *ütközik.*

Mivel a halál tényén és az elhunyt nevén túl további adat kezelése nem szükséges a jogszabály által előírt feltétel érvényesítéséhez, ezáltal az adatkezelés jogalap nélküli, a GDPR 6. cikk (1) bekezdését is sérti."[421]

A másolati példányok problémája még az is, hogy adott esetben nem hiányoznak, ha elvesznek (észrevétlenül elemelhetőek), illetve sok selejtezési szabályzat a másolatok leselejtezését és megsemmisítését nem is köti olyan formai követelményekhez, mint az eredeti példányokét (például úgy rendelkezik a szabályzat, hogy nem kell jegyzőkönyvet felvenni a másolatok bármi módon megszüntetéséről).

Példa

Adatkezelésünk céljának szempontjából „felesleges" adat lehet például a jogosítványon szereplő fénykép és az okmányt kiállító személy aláírása, ezért azt nem is kezelhetjük jogszerűen. Ilyen esetekben javasolt eljárás az (az adatvédelemre vonatkozó alapelveknek megfelelve), hogy a papír vagy digitális másolat készítése és tárolása helyett az eredeti irat megtekintésével egyidejűleg feljegyezzük az adott okirat, például a végzettséget igazoló oklevél azonosító, illetve egyéb, az adatkezelésünk szempontjából releváns adatait.
A visszaélések elkerülése érdekében folyamodhatunk ahhoz a megoldáshoz is, hogy két alkalmazott egyszerre, együttesen nézi meg az adott eredeti iratot („négy szem elve"), illetve nyilatkoztathatjuk is a dokumentumot bemutatót, hogy az általa megadott adatok (az összes, nemcsak az adott oklevélben szereplők) megfelelnek a valóságnak.

Természetesen vannak olyan esetek, amikor elkerülhetetlen az okmánymásolatok kezelése jogszabály – például a Pmt.[422] – rendelkezése alapján. Az is előfordulhat, hogy korrekten körülhatárolt és megfogalmazott közfeladat ellátására/jogos érdekre hivatkozva döntünk úgy, hogy kezelnünk kell az okmány másolatot, ez esetben azonban ezt a döntésünket meg kell indokolnunk és az adatkezelés megkezdése előtt szükségességi-arányossági / érdekmérlegelési tesztet kell végeznünk érdekeink alátámasztása érdekében.

[421] NAIH/2020/54/4. https://www.naih.hu/hatarozatok-vegzesek?download=325:1-rendszeres-szocialis-osztondijakkal-kapcsolatos-adatkezeles-a-budapesti-muszaki-es-gazdasagtudomanyi-egyetemen-modositasokkal-egyseges-szerkezetben, utolsó letöltés 2022. 08. 21.
[422] 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról

Példa

A veszélyes anyagokkal dolgozó termelőüzemben a szakhatóság rendszeresen ellenőrzi a munkavégzés megfelelőségét és a vállalat egyszerűbbnek véli az okmánymásolatokat a helyszínen tartani, mint abban bízni, hogy a munkavállalók mindenkor maguknál tartják a munkakörükhöz elengedhetetlen végzettségük igazolásához szükséges papírokat (pl. igazolásokat speciális tanfolyamok elvégzéséről stb.). A cég attól is félhet, hogy amennyiben az ellenőrzés nem talál rendben minden papírt, abban az esetben a „nem megfelelő" munkavállalónak el kell hagynia a termelési területet és ez akár a termelés időleges leállását is okozhatja, miközben a gyakorlatban azt tapasztalták, hogy a hatóság emberei az eredeti okiratokról készült szkennelt másolatokat is elfogadják a végzettség igazolásához.

Az ilyen esetekben az adatkezelő felelőssége alátámasztani – akár gyakorlati példákkal is – azt, hogy pontosan miért is folyamodnak az okiratmásolatok kezeléséhez és ezzel a gyakorlattal hogyan kívánják elfogadható mértékűre csökkenteni azt a sérelmet, ami az érintettek érdeket, jogait és szabadságait érheti. Az értékelés során az is figyelembe vehető, hogy amennyiben egy hirtelen hatósági ellenőrzés során kiderül, hogy az érintett nem tartotta magánál a kötelezően magánál tartandó okiratot, akkor a hanyagsága miatt kieső munkaórákra nem kap fizetést, sőt, ha a hatóság döntése alapján a termelést is le kell állítani, ez a feledékenység a többi, kevésbé feledékeny munkavállalót is negatívan érintheti stb.

A másolatok – attól függetlenül, hogy bizonyító erővel nem rendelkeznek – pontosan ugyanazon személyes adatokat tartalmazzák, mint az eredeti iratok, így azok biztonságos kezelésére fokozott figyelmet kell fordítanunk.

KIK KEZELHETIK AZ ADATOKAT ÉS MILYEN KONSTRUKCIÓBAN?

A kérdésre, miszerint mi az az adatkezelés, a legtöbb adatvédelmileg alulképzett, ámde adatkezeléssel foglalkozó adatkezelő rögtön rávágja, ő bizony olyat nem csinál. Pedig igen, még akkor is, ha ő azt nem számítja annak, amivel a munkaideje döntő többségét eltölti. Valójában sokkal több minden számít adatkezelésnek, mint amit elsőre gondolnánk.

Példa

- ✓ *a biztonsági szolgálat egy tagja állandóan nézi az irodaházban elhelyezett kamerák által közvetített képet? Adatkezelés.*
- ✓ *a gyerekek egy kívánságládába leadhatják, mit kérnek karácsonyra? Adatkezelés.*

Az adatvédelmi jogszabályok, még ha nem is eresztik valami bő lére a magyarázatokat, de tételesen felsorolják, mi számít adatkezelésnek.

A GDPR alapján az adatkezelés személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így

- ✓ a gyűjtés,
- ✓ rögzítés,
- ✓ rendszerezés,
- ✓ tagolás,
- ✓ tárolás,
- ✓ átalakítás vagy megváltoztatás,
- ✓ lekérdezés,
- ✓ betekintés,
- ✓ felhasználás,
- ✓ közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján,
- ✓ összehangolás vagy összekapcsolás,
- ✓ korlátozás,
- ✓ törlés, illetve
- ✓ megsemmisítés.[423]

Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele.[424]
Adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges.[425]
Adatmegsemmisítés: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése.[426]

[423] GDPR 4. cikk 2. pont
[424] Infotv. 3.§ 12. pont. Az Infotv. 2.§ (2) bekezdése alapján a GDRP rendelkezéseit az Infotv. 3.§ 12. pontjában foglalt kiegészítésekkel kell alkalmazni.
[425] Infotv. 3.§ 13. pont. Az Infotv. 2.§ (2) bekezdése alapján a GDRP rendelkezéseit az Infotv. 3.§ 13. pontjában foglalt kiegészítésekkel kell alkalmazni.
[426] Infotv. 3.§ 16. pont. Az Infotv. 2.§ (2) bekezdése alapján a GDRP rendelkezéseit az Infotv. 3.§ 16. pontjában foglalt kiegészítésekkel kell alkalmazni.)

Adatkezelés például, ha adatkezelőként

- ✓ *az adókedvezmény érvényesítése céljából megkérdezzük, a munkavállalónak vannak-e gyermekei és ha igen, elkérjük a különböző hatóságok/hivatalok által megkövetelt adatokat (gyűjtés),*
- ✓ *nyilvántartásba vesszük a gyermekek adatait (rögzítés),*
- ✓ *az össze-vissza adatokból táblázato(ka)t készítünk vagy a már rendszerezett adatbázisából különféle riportokat hívunk le (rendszerezés),*
- ✓ *a gyermekek adatait megőrizzük mindaddig, amíg azt jogszabály előírja számunkra (tárolás),*
- ✓ *a papír alapon összegyűjtött nyilatkozatokból az adatokat digitalizáljuk (átalakítás vagy megváltoztatás),*
- ✓ *a céges Mikulás ünnepségre készülve az adatbázisból kikutatjuk, mely munkavállalóknak van óvodás korú gyermeke (lekérdezés),*
- ✓ *biztonsági őr a kamerák képét élőben nézve látja, ahogy a munkavállalók a gyermekeikkel együtt megérkeznek az ünnepségre (betekintés),*
- ✓ *kimutatást készítünk, hogy megtudjuk, hány munkavállalónak adhatunk iskolakezdési támogatást és ez hozzávetőlegesen mekkora forrást igényel (felhasználás),*
- ✓ *a belső faliújságra/intranetre/zárt Facebook csoport posztjába kitesszük a Mikulás ünnepségen készült fotókat bizonyítva, milyen jó volt a hangulat és milyen hálásak voltak az apróságok (közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján),*
- ✓ *a munkakörökhöz és a munkakört betöltő munkavállalókhoz hozzárendeljük a munkavégzéshez szükséges munkavédelmi eszközöket, illetve azok pótlásának szükségességét (összehangolás vagy összekapcsolás),*
- ✓ *a téves lakcímet tévesként megjelöljük és korlátozzuk az ahhoz való hozzáférést mindaddig amíg a munkavállaló hitelt érdemlően nem bizonyítja, mi a helyes lakcíme (korlátozás),*
- ✓ *a munkavállaló kérésére töröljük azt a kamerafelvételt, amin az éppen saját cipőfűzőjének köszönhetően hasra esett (törlés), illetve*
- ✓ *lezúzzuk a szokásos éves selejtezés alkalmával leselejtezett iratokat (megsemmisítés).*

Ha kétségünk van, hogy amit csinálunk az adatkezelés-e, szinte biztos, hogy a válasz igen lesz.

Szereplők I.: az adatkezelő és a közös adatkezelő

Az adatkezelés nem magányos elfoglaltság, hiszen nemcsak mi kezelünk egyedül személyes adatot az EGT-tagállamok területén, ráadásul ezt a tevékenységet nemcsak egyedül, hanem más szereplőkkel együttműködve is végezhetjük.

Az adatvédelmi szabályok különböző szereplőket nevesítenek. Ezek a szereplők különböző felelősségi körrel rendelkeznek, a szerepük behatárolásának kiindulási alapja pedig mindig az, hogy a szóban forgó adatkezelés kapcsán ki határozza meg az adott adatkezelés célját és a cél eléréséhez szükséges eszközöket.

A szerepek beazonosítása az esetek többségében egyszerű, a bonyolultabb esetek azonban kifoghatnak az átlag adatkezelő tudásán és többek között éppen az ilyen kérdések megválaszolására vezette be a GDPR az adatvédelmi tisztviselő pozícióját.

Az adatkezelések főbb szereplői:

- ✓ **az adatkezelő** (például a munkáltatók, önkormányzatok, állami hivatalok, rendőrség, óvodák és iskolák, golfklubok, egyesületek, gyülekezetek stb.),
- ✓ **a közös adatkezelő** (például közösen marketing kampányoló cégek, együtt kutató intézmények stb.), illetve
- ✓ **az adatfeldolgozó** (az, aki azt csinálja, ami eredetileg az adatkezelő feladata lenne, de az valami miatt nagyon nem akarja, vagy nem tudja megcsinálni. Ilyen tevékenység például a tárhelyszolgáltatás, a könyvelés, a bérszámfejtés, a futárszolgálat és a biztonsági szolgálat amennyiben az adatkezelő szervezetén kívüli szervezet/egyén végzik ezt a tevékenységet).

Természetesen fontos szereplők az érintettek (az ő személyes adataik nélkül nem is beszélhetünk adatkezelésről) és a címzettek is.

A szerepek elhatárolásához az EDPB iránymutatást[427] adott ki, nekünk pedig még az adatkezelés megkezdése előtt ki kell találnunk, hogy az adott adatkezelésben milyen szerepet töltünk be.

Adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely *a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza*; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.[428]

A belga hatósági gyakorlatból

A bank alkalmazottja nem önálló szervezet, és nem tekinthető az adatkezelő helyett eljáró adatfeldolgozónak.[429]

Az osztrák bírósági gyakorlatból

Egy olyan közösségi hálózat, mint a Facebook puszta használata önmagában nem teszi a felhasználót adatkezelővé. Ezt az indokolja, hogy a Facebook általános felhasználója nem teszi lehetővé a Facebook számára, hogy nem elhanyagolható mennyiségű felhasználói adatot szerezzen meg. A bíróság véleménye szerint

[427] Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0 Adopted on 07 July 2021, https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf
[428] GDPR 4. cikk 7. pont
[429] LG Rostock – 3 O 762/19
https://www.vzbv.de/sites/default/files/downloads/2020/11/25/lg_rostock_15.09.2020.pdf, utolsó letöltés: 2022-07-25

ellenkező esetben a Facebook minden felhasználója adatkezelő lenne, és ez nem lenne összeegyeztethető a GDPR szándékával.[430]

Közös adatkezelők: ha *az adatkezelés céljait és eszközeit két vagy több adatkezelő közösen határozza meg.*[431]

A német bírósági gyakorlatból

A bíróság úgy ítélte meg, hogy a Google Analytics használata esetében az ezt az eszközt használó weboldal üzemeltetője és a Google közös adatkezelő lesz.

A Google a GDPR 4. cikk 7. pontja alapján nem minősül a honlapszolgáltató adatfeldolgozójának, mivel a Google nem kizárólag a honlapszolgáltató általi felhasználás céljából kezeli az adatokat, hanem más harmadik fél szolgáltatókhoz hasonlóan kifejezetten fenntartja a jogot arra, hogy az adatokat saját céljaira is kezelje. Az a tény, hogy az alperes és a Google a GDPR 28. cikke szerinti adatfeldolgozási megállapodást kötött, nem változtat ezen az értékelésen.[432]

A közös adatkezelők átlátható módon, a közöttük létrejött megállapodásban határozzák meg a GDPR szerinti kötelezettségek teljesítéséért fennálló, különösen az érintett jogainak gyakorlásával és az információk rendelkezésre bocsátásával, kapcsolatos feladataikkal összefüggő felelősségük megoszlását, kivéve azt, amikor az adatkezelőkre vonatkozó felelősség megoszlását a rájuk alkalmazandó uniós vagy tagállami jog határozza meg. Amennyiben közös adatkezelők vagyunk, ezen megállapodásunknak megfelelően tükröznie kell a közös adatkezelőként az érintettekkel szembeni szerepünket és a velük való kapcsolatunkat. A megállapodás lényegét az érintett rendelkezésére kell bocsátanunk.

A dán adatvédelmi hatóság (Datatilsynet) gyakorlatából

A hatóság tájékoztatta a Varde önkormányzatot, hogy a GDPR szabályai szerint nem minősül közös adatkezelőnek az a munkavállaló, akit a személyes adatok kezelésével kapcsolatos belső felelősséggel bíztak meg.[433]

Az érintett ezen megállapodás feltételeitől függetlenül mindegyik adatkezelő vonatkozásában és mindegyik adatkezelővel szemben gyakorolhatja a GDPR szerinti jogait.

---

[430] 6Ob56/21k, https://www.ris.bka.gv.at/Dokumente/Justiz/JJT_20210623_OGH0002_0060OB00056_21K0000_000/JJT_20210623_OGH0002_0060OB00056_21K0000_000.pdf, utolsó letöltés: 2022. 07. 25.

[431] GDPR 26. cikk (1) bekezdés

[432] N° de dossier : DOS-2019-02288, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-56-2021.pdf, utolsó letöltés 2022. 07. 25.

[433] Journalnummer: 2018-423-0018, https://www.datatilsynet.dk/afgoerelser/afgoerelser/2020/aug/tilsyn-med-udarbejdelse-af-fortegnelser-i-varde-kommune, utolsó letöltés: 2022. 07. 25.

Szereplők II.: az adatfeldolgozó

Adatkezelőként dönthetünk úgy, hogy bizonyos feladatokat kiszervezünk, például könyvelő céget bízunk meg vagy biztonsági vállalkozást szerződtetünk a területünkre belépők ellenőrzésére és figyelésére. Az ilyen típusú megbízottak adatfeldolgozóink lesznek, és míg adatkezelőként mi önállóan határozzuk meg az adatkezelés célját és eszközeit, addig az adatfeldolgozóink nem határozhatják meg önállóan az adatkezelés célját (például azt, hogy ellenőrizzék-e az őrzésükre bízott területünkre belépőket), az adatfeldolgozói megállapodás függvényében abban van döntési jogosultságuk, hogy milyen eszközökkel végzik a feladatukat (például használnak-e kutyát vagy sem a járőrözéshez).

Kik a „tipikus" adatfeldolgozók?

Példa

- ✓ *a számlázó,*
- ✓ *a könyvelési tanácsadó / adószakértő*
- ✓ *a bérszámfejtő,*
- ✓ *a futár,*
- ✓ *a fuvarozó,*
- ✓ *a tárhelyszolgáltató,*
- ✓ *az iratmegőrző,*
- ✓ *az ügyfélszolgálatos / marketinges/ szervízes,*
- ✓ *a biztonsági szolgáltatást nyújtó szerződéses partner.*

Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.[434]

Adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége.[435]

Az olasz adatvédelmi hatóság (Garante per la protezione dei dati personali, „Garante") gyakorlatából

Az aiComply Srl, mint adatfeldolgozó a bolognai repülőtérnek, mint adatkezelőnek biztosította a „WB confidential" visszaélésbejelentő rendszer alkalmazást a bejelentések kezelésére. Az adatfeldolgozó az alkalmazással kapcsolatban két további adatfeldolgozót vett igénybe, az Agic Technology Srl speciális segítségnyújtási tevékenységet, az A1Tech Srl pedig az IT-infrastruktúrát felügyelte.

Az adatvédelmi hatóság megállapította, hogy

- ✓ *az alkalmazáson belül továbbított és tárolt személyes adatokat nem titkosították,*
- ✓ *a három adatfeldolgozónak közös, nem névre szóló rendszer-adminisztrátori hozzáférése volt az alkalmazáshoz,*

[434] GDPR 4. cikk 8. pont

[435] Infotv. 3. cikk 17. pont. Az Infotv. 2.§ (2) bekezdése alapján a GDRP rendelkezéseit az Infotv. 3.§ 17. pontjában foglalt kiegészítésekkel kell alkalmazni.

- ✓ *az aiComply nem tájékoztatta a repülőteret, mint adatkezelőt a két további adatfeldolgozó (al-adatfeldolgozók) igénybevételéről.*

A Garante úgy döntött, hogy

- ✓ *mind az adatkezelő, mind az adatfeldolgozó köteles megfelelő technikai és szervezési intézkedéseket végrehajtani a hatáskörükön és illetékességükön belüli biztonsági szint biztosítása érdekében. A hiányzó titkosítás és a nem névre szóló rendszer-adminisztrátori hozzáférés megosztása két másik vállalkozással nem felel meg a GDPR 32. cikkében foglaltaknak.*
- ✓ *az adatfeldolgozó a két al-adatfeldolgozó igénybevételére nem kért engedélyt az adatkezelőtől, miközben a két al-adatfeldolgozó személyes adatokat dolgozott fel, ami megkövetelte volna a közreműködő szervezetek, a kezelt adatok és a hatáskörök pontos közlését az adatkezelővel. Ellenkező esetben nem biztosítható, hogy az adatkezelő továbbra is teljes mértékben ellenőrzése alatt tartsa a nevében végzett adatkezeléseket, ami sérti a GDPR 28. cikkét.*

A Garante 20 ezer eurós bírságot szabott ki az adatfeldolgozóra.[436]

Ha az adatkezelést az adatkezelő nevében más végzi, az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés GDPR követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására. Az adatkezelő és adatfeldolgozó együttműködésére és felelősségi körükre a GDPR 28. és 29. cikkek tartalmaznak részletes rendelkezéseket.

Az adatvédelmi szabályok nem foglalkoznak a szerződéses kapcsolatok polgári jogi vetületével (ki, mikor, mit és mennyiért stb.), csakis GDPR hatálya alá tartozó kérdésekre összpontosítanak és olyan kérdéseket rendez, mint például adatvédelmi incidens esetén kinek mi a feladata, valamint hogyan történik az érintetti jogok érvényesítése.

A lengyel adatvédelmi hatóság (UODO) gyakorlatából

Az adatvédelmi hatóság rámutatott, hogy amennyiben az adatkezelés az adatkezelő nevében történik, a GDPR 28. cikk (1) bekezdésének megfogalmazása szerint „az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés e rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására”.

A felek olyan hosszú távú együttműködése, amelyet nem támasztanak alá rendszeres és szisztematikus auditok vagy ellenőrzések, nem garantálja, hogy az adatfeldolgozó megfelelően ellátja a jogszabályban előírt és az adatkezelővel megkötött adatfeldolgozási megállapodásból eredő feladatokat. A múltban pozitívan értékelt

[436] Ordinanza ingiunzione nei confronti di aiComply S.r.l. – 10 giugno 2021 [9685947]. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685947, utolsó letöltés: 2022. 07. 25.

együttműködés csak kiindulópont lehet annak ellenőrzésénél, hogy az adatfeldolgozó elegendő garanciát nyújt-e a megfelelő technikai és szervezési intézkedések végrehajtására annak érdekében, hogy az adatkezelés megfeleljen a GDPR követelményeinek és megfelelően védje az érintettek jogait. A GDPR 28. cikkének (1) bekezdésében meghatározott követelmény ugyanis minden olyan adatkezelőre vonatkozik, aki üzleti tevékenysége során a személyes adatok kezeléséhez egy adatfeldolgozó erőforrásait vagy szolgáltatásait veszi igénybe.

A személyes adatok kezelésére vonatkozó adatfeldolgozási megállapodás puszta aláírása az adatfeldolgozó megfelelő értékelése nélkül nem tekinthető az adatfeldolgozónak a GDPR követelményeinek való megfelelésére vonatkozó ellenőrzési eljárás lefolytatására vonatkozó kötelezettség teljesítésének. [437]

Adatkezelőként teljes felelősséget kell vállalnunk az érintettek felé azokért, akik a megbízásunk alapján a „kiszervezett" munkát végzik számunkra – és ez a felelősség akkor is fennáll, ha az adatfeldolgozónk szakmailag nem áll a helyzet magaslatán.

Példa

- ✓ *az általunk megbízott külsős biztonsági szolgálat megsérti az alkalmazottjaink jogait és szabadságait (például rejtett kamerát használ), akkor azért ugyanúgy felelünk, mintha saját magunk jártunk volna így el;*
- ✓ *az általunk megbízott informatikai vállalkozás úgy programozza az ügyfeleinkkel kapcsolatos adatbázisunkat, hogy ahhoz jogosulatlan személyek is hozzáférnek, sőt adott esetben még a keresőmotorok is indexálják, akkor mi is felelünk a bekövetkezett adatvédelmi incidensért függetlenül attól, hogy nem értünk a programozáshoz és éppen ezért a problémáról sem tudhattunk;*
- ✓ *az adatfeldolgozónk a nevünkben kipostázott személyes adatokat tartalmazó dokumentumot rossz címre küldi.*

Adatkezelőként nemcsak a közvetlenül nekünk dolgozó adatfeldolgozóért, hanem az egész adatfeldolgozói láncolatért felelünk.

Példa

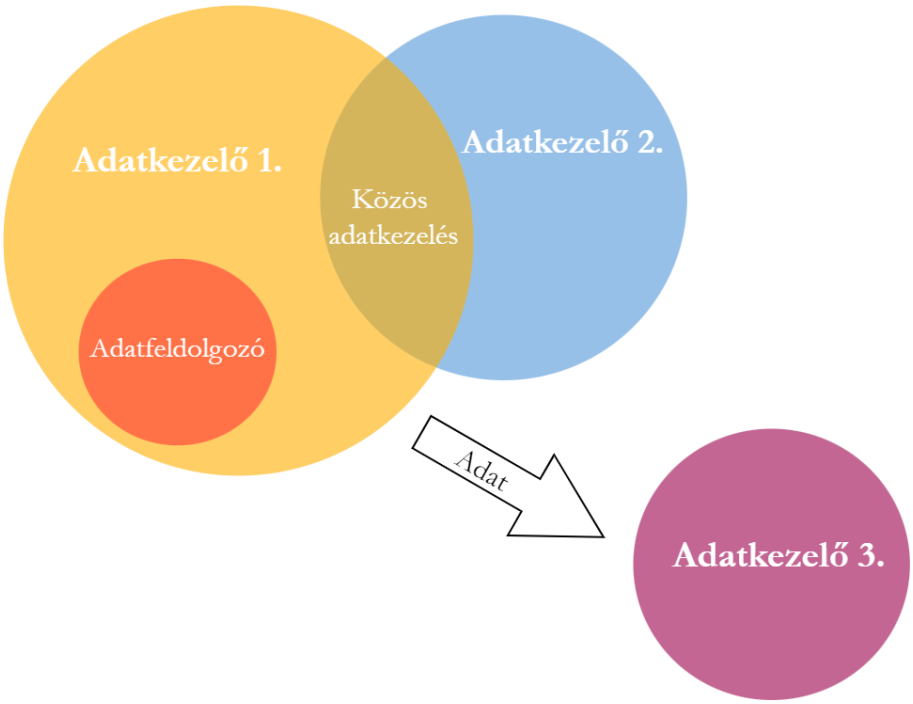
- ✓ *a könyvelésünket kiszervezzük, a könyvelő cég nem akar bajlódni az örökké változó szabályzókkal és továbbpasszolva a nyűgjét alvállalkozót bíz meg a bérszámfejtéssel,*
- ✓ *az általunk megbízott informatikai cég a rendszerfelügyeletünk egyes elemeit további alvállalkozóra bízza,*
- ✓ *szerződést kötünk egy vállalkozással a papír alapú dokumentumaink digitalizálására és tárolására, az pedig a dossziéhegyek biztonságos tárolására raktározással foglalkozó céget bíz meg.*

Az ilyen esetekben a köztünk és az adatfeldolgozó közötti megállapodásnak ezt a viszonyrendszert is tükröznie kell, azaz rendelkeznünk kell az al-adatfeldolgozók („további adatfeldolgozók") felelősségi viszonyairól is (értesítés adatvédelmi incidens esetén, érintetti jogok érvényesítése, audit lefolytatása stb.).

[437] DKN.5130.2215.2020, https://www.uodo.gov.pl/decyzje/DKN.5130.2215.2020, utolsó letöltés 2022. 07. 25.

Akkor most ki kicsoda?

Amennyiben az adatkezelő – közös adatkezelő – adatfeldolgozó Bermuda-háromszögében vergődünk, segítséget nyújthat egy olyan kérdéssor, amely a legfőbb ismérvek alapján tesz kísérletet az aktuális pozíciónk meghatározására.



Példa

Munkavállalók adatait kell kezelnünk a szervezetünk üzleti céljainak eléréséhez (gyártáshoz, értékesítéshez, profit realizálásához stb.). A humán erőforrással együtt járnak a munkavállalók személyes adatai is, ezek hiányában nem tudjuk a munkaerőt felvenni, a munkavégzést megszervezni, valamint a javadalmazás kérdése is megoldhatatlan lesz, és akkor még nem is beszéltünk az adóhivatal és egyéb, adatgyűjtésre és nyilvántartásra szakosodott hivatalok hihetetlen adatéhségéről.

De nemcsak a munkavállalóinkkal jár együtt adat, hanem a kereskedelmi partnereinkkel, ügyfeleinkkel és a diákjainkkal is attól függően, adatkezelőként milyen nemzetgazdasági szektorban tevékenykedünk. Tovább bonyolíthatja a helyzetünket, ha nemcsak a saját szervezetünk, hanem más szervezet számára is végzünk adatkezelést, például fuvarozunk, könyvelünk, IT-rendszert felügyelünk, tárhelyet szolgáltatunk vagy iratokat raktározunk.

Az, hogy egy-egy adatkezelés esetén milyen szerepet veszünk fel (azaz milyen felelősségi körrel jár az, amit csinálunk), az mindig annak az élethelyzetnek az

elemzésével dönthetjük el, amelyhez szervesen kapcsolódik az adott adatkezelésünk. Milyen kérdéseket érdemes feltennünk a behatároláshoz-meghatározáshoz?

Adatkezelők vagyunk?

Mi döntünk arról, hogy az adott adatokat gyűjtsük vagy ne gyűjtsük?

- ✓ *mi döntjük el, hogy nyilvántartjuk a beosztottak számára kiadott szekrényeket?*
- ✓ *mi döntjük el, hogy ki és hogyan regisztrálja azt, hogy ki és milyen járművel lép be a szervezetünk területére?*

Mi döntünk arról, hogy mi legyen az adatkezelés célja?

- ✓ *munkáltatóként iskolakezdési támogatást adunk a munkavállalóinknak, akkor ezen adatkezelés megkezdése és megszüntetése tekintetében mienk a döntés joga?*
- ✓ *mi döntjük el, hogy pénzügyileg támogatjuk a munkavállalóink esetében a gyermekük magánóvoda ellátását?*

Mi döntünk arról, hogy egy adatkezelés során pontosan mely személyes adatokat gyűjtsük? (Ha felmerül egy adatkezelés igénye, akkor azt is el kell döntenie valakinek, ehhez pontosan milyen adatokra van szükség az adott adatkezelés céljának eléréséhez.)

Ha mérni szeretnénk a munkavállalóink teljesítményét, akkor el kell határoznunk, hogy milyen adatok, ismérvek alapján kívánjuk ezt megtenni.

- ✓ *Milyen és honnan származó objektív adatokra támaszkodhatunk?*
- ✓ *Kitől és milyen szubjektív véleményt kívánunk „mérvadónak" venni?*
- ✓ *Milyen formában, milyen időközönként akarjuk az értékelést megvalósítani, valamint hol és hogyan kívánjuk a későbbiekben ezen információkat tárolni?*
- ✓ *Mennyiben fogja befolyásolni egy adott munkavállaló karrierjét ez az értékelés?*

Mi döntünk arról, hogy az adatkezelési cél eléréséhez mely érintettekről gyűjtünk adatokat?

- ✓ *szeretnénk, ha a munkavállalóink véleményeznék az új munkavédelmi bakancsot – ebben az esetben csak azok véleményét fogjuk kikérni, akik ténylegesen is rendelkeznek a bakancsról információval (nemcsak kaptak, hanem használták is);*
- ✓ *csak a fehérgalléros munkavállalóinknak biztosítunk a céges e-mail fiókot és az internet-hozzáférést.*

Realizálunk (kereskedelmi) hasznot vagy más előnyt az adatkezelésből? (kivéve azokat az eseteket, amikor a szolgáltatásainkért másik adatkezelőtől kapunk ellenértéket)

- ✓ *azért üzemeltetünk marketing célú adatbázist és azért küldünk ki direkt marketing leveleket az adatbázisban lévő címekre, mert termékeinket/szolgáltatásainkat bemutatva szeretnénk arra ösztönözni a címzetteket, hogy nálunk vásároljanak / a mi szolgáltatásainkat vegyék igénybe.*

Az adatkezelés köztünk és az ügyfelünk közötti szerződés következménye?

- ✓ *természetes személlyel kötünk szerződést hűtőgép értékesítése tárgyában és a szerződés teljesítéséhez szükséges adatokat kezeljük, például a szerződésben vállalt házhozszállításhoz a vevő által megadott szállítási címet és a telefonszámát.*

Az adatkezelésben érintettek az alkalmazottjaink?

- ✓ *meghatározzuk, hogy melyik alkalmazottunknak, melyik oktatáson kell részt vennie;*
- ✓ *meghatározzuk a műszakbeosztást;*

Hozunk az adatkezelés részeként vagy eredményeként döntést az érintettek személyével kapcsolatban?

- ✓ *eldöntjük, hogy bevezetjük a hónap dolgozója versenyt és az előre meghirdetett pontozási rendszer alapján az első helyezettnek oda is adjuk ezt a címet;*
- ✓ *a jogszabály által meghatározott keretek között meghatározzuk, ki mikor legyen szolgálatban /szabadságon;*
- ✓ *az ittas munkavállalót elbocsátjuk.*

Hozunk szakmai döntést az adatkezelés során az érintettel kapcsolatban?

- ✓ *minősítjük a szervezetünk természetes személy beszállítóit annak érdekében, hogy eldöntsük, a legközelebbi céges családi napra melyik helyi őstermelőtől vegyünk gyümölcsöt és zöldséget;*
- ✓ *teljesítményük alapján minősítjük a munkavállalóinkat.*

Van közvetlen kapcsolatunk az érintettekkel?

- ✓ *az érintettek a mi vevőink, a mi szolgáltatásainkat veszik igénybe, és ha panaszkodni akarnak, azt nálunk tehetik meg;*
- ✓ *az érintettek a munkavállalóink.*

Teljes autonómiánk van az adott adatkezeléssel kapcsolatban?

- ✓ *van – megszondáztathatjuk a láthatólag munkára alkalmatlan állapotban lévő portásunkat és dönthetünk úgy, hogy az ittas állapota miatt a továbbiakban nem kívánjuk, hogy a munkavállalónk legyen;*
- ✓ *nincs – a hónap dolgozója versenyt nem mi találjuk ki, hanem a cégünk anyavállalata, és nemcsak kitalálja, hanem meghatározza a szempontrendszert és a végén ő hagyja jóvá a javaslatunk alapján a cím kiérdemlőjét.*

Megbízunk mást annak érdekében, hogy a nevünkben személyes adatokat kezeljen?

- ✓ *megbízunk vállalkozót, hogy a kamerarendszerünket üzemeltesse;*
- ✓ *megbízunk vállalkozót, hogy a munkavállalóink bérszámfejtésével kapcsolatos feladatokat elvégezze;*
- ✓ *megbízunk vállalkozót, hogy a munkavállalóinkat műszakkezdésre busszal a telephelyünkre szállítsa.*

Közös adatkezelők vagyunk?

Az adott adatkezeléssel kapcsolatban más adatkezelőkkel közös célunk van?

- ✓ *másik szervezettel közösen üzemeltetünk óvodát/focipályát;*
- ✓ *másik szervezettel közös reklámkampányt indítunk;*
- ✓ *másik szervezettel közösen folytatunk kutatást.*

Ugyanabból a célból kezeljük az adatokat, mint egy másik adatkezelő?

- ✓ *egy másik szervezettel együtt ugyanazt a nyilvántartást használjuk annak érdekében, hogy különböző, egymásra épülő szolgáltatásokat nyújthassunk ugyanannak az ügyfélkörnek (például utazásszervezés).*

Ugyanazt az adatállományt[438] (adatbázist) használjunk egy másik adatkezelővel?

- ✓ *az anyavállalat és a leányvállalatok ugyanazt a központi adatbázist használják a munkavállalókkal kapcsolatos adatkezelésekre (oktatás szervezése, e-mail címek és telefonszámok nyilvántartása stb.);*
- ✓ *megállapodás alapján kutakodunk a fejvadász cég adatbázisában annak érdekében, hogy alkalmas jelölteket találjunk a megüresedett pozícióink betöltéséhez.*

[438] adatállomány: az egy nyilvántartásban kezelt adatok összessége, Infotv. 3.§ 21. pont

Egy másik adatkezelővel együtt terveztük meg az adott adatkezelést?

- ✓ *másik szervezettel közösen terveztük meg a reklámkampányt és közösen alakítottuk ki és üzemeltetjük a promóciós honlapot;*
- ✓ *a partner céggel együtt terveztük meg a közös kutatásunkkal kapcsolatos adatkezeléseket.*

Egy másik adatkezelővel közös információ menedzsmentünk van?

- ✓ *egy másik szervezettel közösen üzemeltetjük azt az applikációt, amelyben a közös projektünk előrehaladását és eredményeit adminisztráljuk.*

Adatfeldolgozók vagyunk?

Mások instrukcióit követjük az adatkezeléssel kapcsolatban?

- ✓ *más szervezeteknek digitalizálunk és tárolunk iratokat és ezen szervezetek utasításai alapján kell eljárnunk (hogyan adminisztráljuk a digitalizálás folyamatát, hol tároljuk a digitális másolatokat, mit tegyünk az eredeti papír alapú dokumentációval stb.);*
- ✓ *megbízónk közli velünk, ezentúl nem két őrt, hanem hármat kér a kettes számú portára, és többet nem akar kutyát látni az őrbódéban.*

Egy másik adatkezelő adta át nekünk a személyes adatokat vagy mondta meg, hogy mely adatokat gyűjtsük?

- ✓ *nemcsak a saját áruinkat szállítjuk, hanem szabad kapacitásainkat kihasználva más szervezeteknek is vállalunk fuvarozást, ehhez pedig meg kell adniuk a szükséges adatokat (honnan hova, kitől kinek és mit, valamint a helyszínen kit kell keresni);*
- ✓ *megkaptunk egy listát annak érdekében, hogy végig hívjuk az azon szereplőket, akarnak-e előfizetési csomagot váltani a közeljövőben.*

Nem a mi döntésünk, hogy adatokat gyűjtsünk az érintettektől?

- ✓ *kitelepült promóciós kampány keretében a megbízónk utasítása alapján gyűjtjük az érdeklődők adatait, hogy a kampány zárultával a megbízónk alkalmazottai fel tudják venni az érdeklődőkkel a kapcsolatot;*
- ✓ *leszerződtünk imázsfilm készítésére és a megbízónk utasításai alapján, a megbízó által meghatározott helyszínen és munkavállalókkal vesszük fel a munkafolyamatokat, a végén pedig a kész filmet az összes eredeti felvétellel együtt átadjuk a megbízónknak.*

Nem mi határozzuk meg az adatkezelés célját, jogalapját vagy azt, hogy milyen célra lesznek használva az adatok?

- ✓ *megbízás alapján különféle szervezetek honlapjait üzemeltetjük, illetve a szükséges mértékben (megrendelésre) fejlesztjük azokat.*

Nem mi határozzuk meg, hogy megosztjuk-e az adatokat?

- ✓ *bérszámfejtést végzünk megbízónk számára, akinek az utasítása alapján a havi adatokat elküldjük az adóhatóságnak, illetve a könyvelést végző cégnek;*
- ✓ *flottakezelés céljából telematikai alkalmazást üzemeltetünk és az ügyfelünk utasít minket, hogy az egyik megbízójának adjunk a hozzáférést bizonyos adatokhoz, mert szeretné nyomon követni a nagy értékű árujának teljes fuvarozási folyamatát.*

Nem mi határozzuk meg, hogy meddig tároljuk az adatokat?

- ✓ *digitalizálással, archiválással és irattárolással foglalkozunk és a megbízónk utasítása alapján selejtezzük ki azokat az adatokat, amelyekre már nincs szüksége;*
- ✓ *elektronikus megfigyelőrendszert üzemeltetünk és a megbízónk utasítása alapján az adatokat (felvételeket) 14 nap után töröljük.*

Ugyan hozhatunk döntéseket abban, hogy hogyan kezeljük az adatokat, de ezeket a döntéseket szerződéses kötelezettségünk keretében hozzuk, illetve bizonyos döntésekhez, bár mi hozzuk meg azt, de kell a megbízónk engedélye is?

- ✓ *marketing megbízásunk alapján dönthetünk, arról, hogy mikor milyen témában küldhetünk ki direkt marketing levelet és kiknek, de csakis a megbízónkkal kötött szerződés keretein belül;*
- ✓ *eldönthetjük, hogy az adott megbízás teljesítéséhez melyik szoftvert / felhőszolgáltatót /futárszolgálatot használjuk.*

Nem vagyunk érdekeltek az adatkezelés eredményében? (A megbízási díjunkat attól függetlenül megkapjuk, hogy a tevékenységünk mekkora üzleti hasznot hoz a megbízónknak.)

- ✓ *megbízónk utasítása alapján hírleveleket küldünk ki, ám az, hogy ezen, hírlevelek milyen hasznot (bevételnövekedést) eredményeznek a megbízónknál, abban nem vagyunk érdekeltek (és nem is tőlünk függ, a mi feladatunk csupán a hírlevelek kiküldése a rendelkezésre álló aktuális címlista alapján).*

Mi az a felhő?

A felhőszolgáltatás egy olyan szolgáltatás, amelynek segítségével nem saját magunknál, hanem másoknál tartjuk az adatainkat, olyan helyen, amelyet internet segítségével érünk el. Ha például e-mailt küldünk (gmail, hotmail stb.), máris felhőben járunk és a különféle appok használata is nagyrészt felhők segítségével történik.

A felhőszolgáltatás alaptípusai (nem kizárólagos felsorolás, a szolgáltatások köre napról napra változik-fejlődik):

- ✓ a felhőszolgáltató szoftverszolgáltatást nyújt az interneten keresztül („SaaS”[439], például e-mail szolgáltatás, irodai szoftverek stb.)
- ✓ a felhőszolgáltató az alkalmazás üzemeltetéséhez szükséges környezetet biztosítja („PaaS”[440], például webshophoz)
- ✓ a felhőszolgáltató az infrastruktúrát (virtuális gépet és más erőforrásokat) biztosítja, az operációs rendszert és az alkalmazásokat a felhasználó működteti („IaaS”[441])
- ✓ a felhőszolgáltatás adattárolást biztosít, mint szolgáltatás („STaaS”[442]).

A felhőszolgáltatók általában adatfeldolgozó szerepkört töltenek be, a felelősségük is ehhez igazodik.

A szlovén adatvédelmi hatóság (IP) gyakorlatából

Az IP megállapította, hogy az adatkezelő és az adatfeldolgozó közötti megállapodás nem pontos leírása a felhőalapú számítástechnikai szolgáltató és ügyfelei között megosztott felelősségnek, mivel mind az adatkezelő, mind az adatfeldolgozó meghatározzák az adatkezelés céljait és eszközeit, ezért a hatóság kötelezte a felhőszolgáltatót, hogy közös adatkezelői megállapodást kössön az ügyfeleivel.

A vizsgálata során az IP megállapította, hogy az adatkezelő felhőalapú számítástechnikai üzleti modelljének alapgondolata az összetett technikai sajátosságok kezelése volt úgy, hogy az ügyfelei számára – egyszerűsítve a technikai szempontokat – lehetővé tegye számukra, hogy teljes mértékben a kért adatok tartalmára összpontosítsanak. Az ügyfeleknek alig vagy egyáltalán nem volt befolyásuk a felhőszolgáltató által az adatkezelés során alkalmazott technikai és szervezési intézkedésekre.

Az IP hangsúlyozta, hogy egy szervezet adatkezelői vagy adatfeldolgozói státuszának ténybeli meghatározásnak kell lennie, nem pedig pusztán formális megjelölésnek. Amennyiben az „adatfeldolgozó” ténylegesen beleszólhat az adatkezelés alapvető céljaiba és eszközeibe, akkor ténylegesen adatkezelőnek minősül, nem pedig adatfeldolgozónak és felel a GDPR-nak való megfelelésért, és amennyiben a két szervezet közötti megállapodás alapján mindketten felelősek az adatvédelmi szabályoknak való megfelelésért, akkor mindketten adatkezelők.

[439] „Software as a Service”
[440] „Platform as a Service”
[441] „Infrastructure as a Service”
[442] ’Storage as a Services”

Ebben az esetben a felhőszolgáltató ügyfeleinek nem volt hatásköre a GDPR-nak való technikai megfelelés biztosítására és a felhőszolgáltató járt el adatkezelőként, mivel meghatározta azokat a technikai folyamatokat, amelyekkel az adatokat kérték, kezelték és továbbították, valamint azt, hogy milyen alfeldolgozókat alkalmaztak. A felhőszolgáltató és ügyfelei tehát egyaránt meghatározták az adatkezelés céljait és eszközeit, ezért megállapodásuk valójában közös adatkezelés, nem pedig adatfeldolgozás, tehát a köztük lévő kapcsolatot közös adatkezelésre vonatkozó megállapodásnak kell szabályoznia. [443]

Milyen előnyei vannak a felhőszolgáltatásnak?

Amennyiben megfelelő színvonalú szolgáltatót választunk, ezzel

- ✓ optimalizálhatjuk a költségeinket (például használatarányosan fizetünk a szolgáltatásért, nem kell beruháznunk drága IT infrastruktúrára) és a szükségletünk függvényében rugalmasan bővíthetjük-csökkenthetjük a rendelkezésünkre álló erőforrásokat;
- ✓ bizonyos területeken áthárithatjuk a kvalifikált munkaerőforrás felkutatásának, megbízásának és oktatásának-foglalkoztatásának költségeit és egyéb vonzatát;
- ✓ csökkenthetjük a mobil eszközeinken tárolt adatmennyiséget, ezzel is redukálva a kockázatot például mobiltelefon, tablet vagy notebook elvesztése/ellopása esetén;
- ✓ adott esetben a felhőszolgáltatók magasabb szintű adatvédelmet tudnak biztosítani például a fizikai biztonság (24 órás őrzés), biztonsági másolat (backup), földrajzi kitettség csökkentése (pl. redundáns szerver), azonnali incidens észlelés és reagálás, szoftverfrissítés, vírusvédelem stb. területén.

Természetesen a felhőszolgáltatások igénybevétele számos kockázatot is hordoz, mint például

- ✓ nem természetes személyként nem tudunk élni az adathordozhatósági joggal (az adatmigrációs igényünk érvényesítésével);
- ✓ nehéz szolgáltatót váltanunk az eltérő formátumok használata (az interoperabilitás hiánya) miatt, így a szolgáltató „foglyul ejtheti" az adatainkat;
- ✓ nem mindig egyértelmű, hogy az adataink ténylegesen milyen joghatóság alatt vannak tárolva, ez pedig komoly adatvédelmi és adatbiztonsági problémát generálhat (lásd harmadik országba adattovábbítás[444] követelményei a GDPR alapján);
- ✓ nem mindig egyértelmű, hogy nekünk egynek tűnő szolgáltatás keretében valójában hány felhőszolgáltató szolgáltatását vesszük igénybe (például akkor, amikor a felhőszolgáltató nem csak a saját szolgáltatását, hanem számunkra ismeretlen alvállalkozók kínálatából összevegyített szolgáltatásmixet nyújt);
- ✓ ha a felhőszolgáltató csődbe megy vagy a hatóságok az egyik ügyfél adataival együtt a mi adatainkat is lefoglalják, abban az esetben kétséges, hogy hogyan

[443] 0612-23/2019/19. https://gdprhub.eu/images/8/89/IP_%28Slovenia%29_-_0612-23-2019-19.pdf, utolsó letöltés: 2022. 07. 29.
[444] harmadik ország: minden olyan állam, amely nem EGT-állam [Infotv. 3.§ 24- pont]

és mikor kapjuk vissza azokat, a kiszolgáltatottságunk pedig tovább fokozódik, ha a tényleges tárhely harmadik országban van;
- ✓ a nem megfelelő információbiztonsággal működő tárhelyszolgáltató fokozottan vonzhatja azokat a hackereket, akik egyébként nem találják támadásra méltónak a mi adatainkat;[445]
- ✓ bizonyos események időlegesen csökkenthetik az adatainkhoz a hozzáférést (például a felhőszolgáltató másik ügyfele ellen intézett hálózati támadás stb.);
- ✓ a felelősségi viszonyok sok esetben nincsenek megfelelően szabályozva (például az adatfeldolgozásra vonatkozó megállapodások, illetve a harmadik országba továbbítás problémája nincs megfelelően rendezve) és ezért a szolgáltatást igénybe vevők, illetve az érintettek érdekei, jogai és szabadságai nagymértékben sérülnek.

Bármilyen kockázatai is van a felhőnek, egyre nagyobb a piaci és társadalmi nyomás ezen szolgáltatások igénybevételére, a digitalizáció lassan a „legmaradibb" adatkezelőt is rákényszeríti a felhőszolgáltatások igénybevételére (honlap, e-mail cím fenntartása, vállalatirányítási szoftverek stb.).

Az adatvédelmi jog a felhőszolgáltatókat ugyanúgy kötelezi az adatvédelem előírásainak betartására, mint a sima „földi" szolgáltatókat (lásd például a nemzetközi adattovábbításra vonatkozó előírásokat), illetve nemzeti szinten is egyre több megszorításnak lehetünk tanúi (például van olyan ország, amely tiltja a saját állampolgárai különleges adatainak idegen joghatóság alatti tárolását stb.).

Szereplők III.: címzettek és harmadik felek

Kik azok a címzettek?

Címzett: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel, vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak.[446]

Azok a közhatalmi szervek, amelyekkel hivatalos feladataikkal kapcsolatos jogi kötelezettségeik keretében személyes adatokat közölnek, így például az adó- és vámhatóságok, a pénzügyi nyomozóegységek, a független közigazgatási hatóságok, valamint az értékpapírpiacok szabályozásáért és felügyeletéért felelős pénzügyi hatóságok nem tekinthetők címzettnek, amikor olyan személyes adatokat kapnak, amelyek az uniós vagy a tagállami jog alapján egy konkrét közérdekű vizsgálat lefolytatásához szükségesek. A közhatalmi szervek által küldött, adatközlés iránti

[445] Lásd pl. supply chain attacks típusú támadások (pl. Solarwinds 2021), A Solarwinds incidens Kiberbiztonsági elemzés, Nemzeti Kibervédelmi Intézet, https://nki.gov.hu/wp-content/uploads/2021/09/NBSZ-NKI-Kiberbiztons%C3%A1gi-elemz%C3%A9s-a-SolarWinds-incidensr%C5%91l.pdf
[446] GDPR 4. cikk 9. pont

megkereséseket írásban, indokolással ellátva és eseti alapon kell benyújtani, és azok nem vonatkozhatnak teljes nyilvántartási rendszerekre, illetve nem eredményezhetik nyilvántartási rendszerek összekapcsolását. A személyes adatok említett közhatalmi szervek általi kezelése során be kell tartani az adatkezelés céljának megfelelően alkalmazandó adatvédelmi szabályokat. [447]

A 29. cikk szerinti adatvédelmi munkacsoport gyakorlatából

„A GDPR címzett definíciója alapján „a címzettnek nem kell harmadik félnek lennie. Ennek következtében az egyéb adatkezelők, közös adatkezelők és adatfeldolgozók, akik vagy amelyek részére az adatokat továbbítják, szintén „címzettnek" minősülnek, és a harmadik fél címzettekre vonatkozó tájékoztatás mellett az ilyen címzettekről is tájékoztatást kell nyújtani.

A személyes adatok tényleges (megnevezett) címzettjeit vagy a címzettek kategóriáit kell megadni. A tisztességes eljárás elvével összhangban az adatkezelőknek az érintettek számára leginkább releváns információkat kell rendelkezésre bocsátaniuk a címzettekkel kapcsolatban. A gyakorlatban ez általában a megnevezett címzetteket jelenti, hogy az érintettek pontosan tudják, ki rendelkezik a személyes adataikkal. Ha az adatkezelők úgy döntenek, hogy a címzettek kategóriáit adják meg, az információnak a lehető legkonkrétabbnak kell lennie, és magában kell foglalnia a címzett típusát (pl. az általa végzett tevékenységekre való utalással), az érintett szakmát, az ágazatot és alágazatot, valamint a címzettek tartózkodási helyét."[448]

Egy adott adatkezelés során a címzettek léte nagyon fontos momentum lehet, például a GDPR alapján

- ✓ a címzettek felé történő adattovábbításról az érintetteket tájékoztatnunk kell,[449] ha pedig
- ✓ valamely harmadik országbeli címzett vagy valamely nemzetközi szervezet részére kívánjuk továbbítani a személyes adatokat, akkor külön garanciát kell biztosítanunk atekintetben, hogy az adattovábbítás során nem sérül meg az érintetti jogok egyenszilárdságú védelme;[450]
- ✓ a hozzáférési jog gyakorlása során is tájékoztatást kell tudnunk adni a címzettekről,[451] valamint

[447] GDPR (31) preambulumbekezdés
[448] A 29. cikk szerinti munkacsoport Iránymutatás az (EU) 2016/679 rendelet szerinti átláthatóságról, Elfogadás időpontja: 2017. november 29. WP260 rev.01, https://www.naih.hu/files/wp260rev01_hu.pdf, utolsó letöltés: 2022. 08. 20.
[449] „Ha a személyes adatok jogszerűen közölhetőek más címzettel, a címzettel történő első közléskor arról az érintettet tájékoztatni kell." [GDPR (61) preambulumbekezdés]
[450] „a személyes adatoknak az Unióból harmadik országbeli adatkezelőknek, adatfeldolgozóknak, egyéb címzetteknek vagy nemzetközi szervezetek részére történő továbbítása esetén nem sérülhet a természetes személyeknek az Unióban e rendelettel biztosított védelem szintje" [GDPR (101) preambulumbekezdés]
[451] „minden érintett számára biztosítani kell a jogot arra, hogy megismerje különösen (…) a személyes adatok címzettjeit [GDPR (63) preambulumbekezdés]

- ✓ a személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség kapcsán is vannak kötelezettségeink.[452]

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A GDPR 13.-14. cikke tartalmazza, hogy az adatkezelőknek minimálisan mely adatkezelési körülményekről kell tájékoztatniuk az érintetteket. Ez természetesen nem jelenti korlátját annak, hogy az adatkezelő ennél pontosabb tájékoztatást adjon. Ebből eredően a Hatóság kifejezetten jó gyakorlatnak tartja, ha az adatkezelők nem csupán a címzetteket vagy azok kategóriáit jelölik meg a tájékoztatóban, hanem azt is, hogy részükre mely személyes adatokat milyen célból továbbítják. Az átláthatóság érdekében érdemes a fentiekről táblázatos formában tájékoztatni az érintetteket.”[453]

Kik azok a harmadik felek?

Harmadik fél: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.”[454]

Az osztrák bírósági gyakorlatból

A szövetségi közigazgatási bíróság megállapította, hogy az a hozzájárulás, amely az első adatkezelő kapott az adatok második adatkezelőnek történő továbbításához, nem terjed ki a második adatkezelőtől harmadik félnek történő továbbításra, kivéve, ha az eset körülményeiből másként nem következik.

Az ügy két érintettje magánóvodába járó gyermek. A magánóvoda – az érintettek törvényes képviselőinek hozzájárulásával – átadott a székhelye szerinti önkormányzatnak (az adatkezelőnek) egy listát, amely az óvodába járó összes gyermek nevét, születési dátumát és felvételi dátumát tartalmazta. Mivel az önkormányzat nem kívánta viselni a más településen lakóhellyel rendelkező gyermekek költségeit, levelet küldött minden szülőnek, amelyben arra kérte őket, hogy vigyék el a levelet a lakóhelyük szerinti önkormányzathoz, és kérjék anyagi támogatásukat. Ez a levél tartalmazta az óvoda önkormányzatnak küldött listáját, valamint egy másik listát is a hiányzási napokkal, az összes nappal és az egyes gyermekek számított költséghányadával.

[452] „Az adatkezelő minden olyan címzettet tájékoztat a 16. cikk, a 17. cikk (1) bekezdése, illetve a 18. cikk szerinti valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.” [GDPR (19) preambulumbekezdés]
[453] NAIH/2018/4017/2/V, https://www.naih.hu/files/Adatved_allasfoglalas_NAIH-2018-4017-2-V_uzleti_titok.pdf, utolsó letöltés 2022. 08. 20.
[454] GDPR 4. cikk 10. pont

Az adatkezelő (az önkormányzat) nem kérte az érintettek törvényes képviselőinek a hozzájárulását mielőtt a levelet kiküldte volna az összes szülőnek. Az érintettek – akiket törvényes képviselőik képviseltek – panaszt nyújtottak be az adatvédelmi hatósághoz. Az adatvédelmi hatóság (DSB) helyt adott a panasznak, majd a szövetségi közigazgatási bíróság (Bundesverwatungsgericht – BVwG) helybenhagyta a DSB határozatát.

A bíróság megállapította, hogy az óvoda vezetője a levelek küldése tekintetében a GDPR 4. cikkének (10) bekezdése szerinti harmadik félnek minősül, az óvoda vezetőjének adott hozzájárulás pedig nem terjedt ki az önkormányzatra, valamint az adatoknak a többi törvényes képviselővel való közlésére sem.[455]

A GDPR alapján valamely harmadik fél jogos érdeke jogalapot is teremthet az adatkezelésre, feltéve, hogy az érintett érdekei, alapvető jogai és szabadságai nem élveznek elsőbbséget, figyelembe véve az adatkezelővel való kapcsolata alapján az érintett észszerű elvárásait. Az ilyen adatkezelések esetében akkor is biztosítani kell az érintettek számára a jogot arra, hogy az egyedi helyzetükre vonatkozó adataik kezelése ellen tiltakozzanak, ha egyébként a személyes adataik jogszerűen kezelhetők, mert az adatkezelésre közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtásához, illetve az adatkezelő vagy egy harmadik fél jogos érdekei alapján van szükség. Adatkezelőként a személyes adatok további kezelése érdekében bizonyítanunk kell, hogy az érintett érdekeivel vagy alapvető jogaival és szabadságaival szemben a mi kényszerítő erejű jogos érdekünk elsőbbséget élvezhet.

GDPR

- ✓ Az adatkezelő feladatai [GDPR 24. cikk, (74)-(77) és (83) preambulumbekezdések]
- ✓ Közös adatkezelők [GDPR 26. cikk, (79) preambulumbekezdések]
- ✓ Az adatfeldolgozó [GDPR 28. cikk, (81) preambulumbekezdések]
- ✓ Az adatkezelő vagy az adatfeldolgozó irányítása alatt végzett adatkezelés [GDPR 29. cikk]

Iránymutatások

- ✓ Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0 Adopted on 07 July 2021, https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

[455] W1012208238-1/5E, https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20211207_W101_2208238_1_00/BVWGT_20211207_W101_2208238_1_00.pdf, utolsó letöltés 2022. 07. 31.

Szereplők IV.: adatvédelmi tisztviselő

Adatkezelőként vagy adatfeldolgozóként mikor kell adatvédelmi tisztviselőt (DPO)[456] kijelölni?

Amikor

a) az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságok;
b) az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé;
c) az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok GDPR 9. cikk szerinti különleges kategóriáinak és a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukba.

A görög adatvédelmi hatóság (HDPA) gyakorlatából

A HDPA 75 ezer eurós bírságot szabott ki a Turisztikai Minisztériumra, mert a Minisztérium nem nevezett ki adatvédelmi tisztviselőt, valamint nem jelentett be egy olyan adatvédelmi incidenst, amely lehetővé tette, hogy a kormányzati platformon a hitelesítő adataikat megadó polgárok megismerhessék más személyek személyes adatait – beleértve a teljes nevet, az adóazonosító számot, a társadalombiztosítási számot, a postai címet, a telefonszámot, az e-mail címet, valamint a rokkantsági státuszt.

A HDPA megállapította, hogy

- ✓ *a Turisztikai Minisztérium a platform valamennyi felhasználójának személyes adataiért felelős adatkezelő, és mint ilyen, a GDPR értelmében felelős volt az adatvédelmi incidensért és az adatvédelmi tisztviselő hiányáért;*
- ✓ *a Minisztérium az adatvédelmi incidenst követően „ad hoc" incidenskezelési eljárást alkalmazott és ebben az eljárásban nem tárta fel az incidens forrását, és még a különböző megkérdezett felek vizsgálatát követően is csak találgatni tudott az incidens okát illetően;*
- ✓ *az adatkezelő a biztonsági intézkedések meghatározása során nem vette figyelembe a természetes személyek jogaira és szabadságaira vonatkozó kockázatokat.*[457]

[456] Data Protection Officer
[457] ΑΠΟΦΑΣΗ 55/2021, https://www.dpa.gr/sites/default/files/2022-01/55_2021anonym.pdf, utolsó letöltés: 2022. 08. 29.

Egy vállalkozáscsoport közös adatvédelmi tisztviselőt is kijelölhet, ha az adatvédelmi tisztviselő valamennyi tevékenységi helyről könnyen elérhető – tehát magyar leányvállalat esetében nem biztos, hogy az Egyesült Államokban székelő DPO a GDPR előírásainak megfelelő adatvédelmi tisztviselő lesz, tekintettel arra, hogy a kijelölt személynek

- szakmai rátermettséget kell tanúsítania és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismeretével kell rendelkezzen (nem biztos, hogy elvárhatjuk egy USA-beli jogásztól, hogy ismerje az adatvédelem magyar munkajogi vetületeit, lásd például a munkavállalók Mt. szerinti ellenőrzése);
- valamint el kell tudnia látnia mindazokat a feladatokat, amelyeket a GDPR előír.

Amennyiben az adatkezelő vagy az adatfeldolgozó közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv, közös adatvédelmi tisztviselő jelölhető ki több ilyen szerv számára, az adott szervek szervezeti felépítésének és méretének figyelembevételével.

Adatkezelőként adatvédelmi tisztviselőt természetesen akkor is kijelölhetünk, ha az nem kötelező.

Az adatvédelmi tisztviselő az alkalmazottunk is lehet, de akár szolgáltatási szerződés keretében is elláthatja a feladatait; a nevét és az elérhetőségét a felügyeleti hatósággal közölnünk kell.[458]

Milyen jogállása van az adatvédelmi tisztviselőnek?

Adatkezelőként biztosítanunk kell

- ✓ hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben be tudjon kapcsolódni;
- ✓ számára azokat a forrásokat, amelyek a DPO feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek;
- ✓ hogy a DPO a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. Az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatjuk el és szankcióval nem sújthatjuk, továbbá közvetlenül a legfelsőbb vezetésnek kell, hogy felelősséggel tartozzon;
- ✓ hogy az érintettek a személyes adataik kezeléséhez és a GDPR szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhassanak.

A luxemburgi adatvédelmi hatóság (CNPD) gyakorlatából

A CNPD 18 .700 eurós bírságot szabott ki egy vállalatra az adatvédelmi tisztviselő szerepével és pozíciójával kapcsolatos jogsértések miatt, és felszólította a vállalatot, hogy négy hónapon belül hozza összhangba gyakorlatát a GDPR rendelkezéseivel.

[458] https://naih.hu/index.php/adatvedelmi-tisztviselo-bejelento-rendszer

A CNDP megállapította, hogy az adatkezelő

- ✓ *elmulasztotta közzétenni adatvédelmi tisztviselője elérhetőségét. Az adatkezelő nyilvános honlapja nem tartalmazta az adatvédelmi tisztviselő közvetlen elérhetőségét, ezért az érintettek nem tudtak közvetlenül kapcsolatba lépni az adatvédelmi tisztviselővel;*
- ✓ *nem biztosította, hogy az adatvédelmi tisztviselőt megfelelően és időben bevonják a személyes adatok védelmével kapcsolatos valamennyi kérdésbe. Az adatvédelmi tisztviselőt csak meghívás alapján vagy ad hoc jelleggel vonták be különböző belső ülésekbe vagy bizottságokba, de nem volt meghatározott szabály vagy gyakoriság arra vonatkozóan, hogy az adatvédelmi tisztviselőt milyen gyakorisággal kell bevonni ezekbe a bizottságokba;*
- ✓ *nem biztosította, hogy az adatvédelmi tisztviselő kellő önállósággal tudja ellátni feladatát. Az adatvédelmi tisztviselő és az adatkezelő legmagasabb szintű vezetése között több hierarchikus közvetítő is létezett, ezért az adatvédelmi tisztviselő nem tudott közvetlenül az adatkezelő legmagasabb vezetői szintjének beszámolni, és nem rendelkezett a GDPR 38. cikkének (3) bekezdésének megfelelő mértékű önállósággal és függetlenséggel;*
- ✓ *nem biztosította, hogy az adatvédelmi tisztviselő megfelelően ellenőrizni tudja az adatkezelő adatkezelési gyakorlatának a GDPR-nek való megfelelését. Az adatkezelőnél nem létezett olyan ellenőrzési terv vagy eljárás, amely formalizálta és biztosította volna, hogy az adatvédelmi tisztviselő képes legyen megfelelően ellenőrizni az adatkezelő adatfeldolgozási gyakorlatának a GDPR-nek való megfelelését.*[459]

Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti. Az Infotv. alapján az adatvédelmi tisztviselő jogviszonyának fennállása alatt és annak megszűnését követően is titokként megőrzi a tevékenységével, annak ellátásával kapcsolatban tudomására jutott személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy körülményt, amelyet az őt alkalmazó adatkezelő vagy adatfeldolgozó nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni.[460]

A DPO más feladatokat is elláthat, azonban e feladatokból nem fakadhat összeférhetetlenség.

[459] Délibération n° 41FR/2021 du 27 octobre 2021, https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-41FR-2021-sous-forme-anonymisee.pdf, utolsó letöltés 2022. 08. 29.
[460] Infotv. 25/M. § (2) bekezdés

Az olasz adatvédelmi hatóság (Garante per la protezione dei dati personali, „Garante") gyakorlatából

A hatóság megállapította, hogy az adatkezelő azáltal, hogy az adatvédelmi tisztviselőt bízta meg a bírósági eljárásokban való képviselettel, az adatvédelmi tisztviselőt összeférhetetlenségi helyzetbe hozta, megsértve a GDPR 38. cikkének (6) bekezdését. Különösen azért, mert ez azt eredményezte, hogy az érintett úgy érezte, hogy nem tud kapcsolatba lépni az adatvédelmi tisztviselővel a személyes adatainak kezelésével kapcsolatos kérdésekkel és a GDPR 38. cikkének (4) bekezdése szerinti jogainak gyakorlásával kapcsolatban.[461]

Milyen feladatai vannak az adatvédelmi tisztviselőnek?

Az adatvédelmi tisztviselő legalább a következő feladatokat ellátja:

a) tájékoztat és szakmai tanácsot ad nekünk, továbbá az adatkezelést végző alkalmazottjaink részére a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeinkkel kapcsolatban;
b) ellenőrzi a GDPR-nak, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá a személyes adatok védelmével kapcsolatos belső szabályainknak való megfelelésünket, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzetünk tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
c) kérésünkre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
d) együttműködik a felügyeleti hatósággal és
e) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

A lengyel adatvédelmi hatóság (UODO) gyakorlatából

Az UODO 50 ezer zlotyra bírságolta a Varsói Élettudományi Egyetemet (SGGW), mivel egy adatvédelmi incidens során több mint 80 ezer, az elmúlt 5 évből származó, az egyetemre jelentkező személyekre vonatkozó adat került nyilvánosságra.

Egy egyetemi alkalmazott a magántulajdonú számítógépét üzleti célokra használta, többek között az SGGW-re jelentkező egyetemi hallgatók személyes adatainak kezelésére. A munkavállaló számítógépét ellopták, amelynek következtében mintegy 100 ezer érintett személyes adata került veszélybe. Ráadásul a nyilvántartások az elmúlt 5 év felvételizőinek adatait tartalmazták, holott az SGGW-nél az előírt tárolási időszak a felvételi eljárás befejezésétől számított 3 hónap volt. Az adatok

[461] Ordinanza ingiunzione nei confronti di Comune di Policoro – 9 giugno 2022 [9794895] – https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9794895, utolsó letöltés: 2022. 10. 21.

között szerepeltek többek között az elérhetőségi adatok, a bizonyítványok osztályzatai, a tanulmányi átlagok, valamint az a szakterület, amelyre a felvételiző jelentkezett.

Az UODO megállapította, hogy

- ✓ *az SGGW nem hozott megfelelő technikai és szervezési intézkedéseket az adatkezelés kockázatainak megfelelő kezelése érdekében;*
- ✓ *az adatvédelmi tisztviselő (DPO) nem vette kellő mértékben figyelembe az adatkezelési műveletekkel kapcsolatos kockázatokat;*
- ✓ *az SGGW az adatvédelmi tisztviselőt nem vonta be a felvételi eljárásba, beleértve az erre a célra használt informatikai rendszer működését is;*
- ✓ *az adatvédelmi tisztviselő fokozott bevonása csökkenthette volna a nem megfelelő adatkezelési műveletek kockázatát.*[462]

[462] ZSOŚS.421.25.2019, https://www.uodo.gov.pl/decyzje/ZSO%C5%9AS.421.25.2019, utolsó letöltés: 2022. 08. 29.

ADATVÉDELEM ÉS ADATBIZTONSÁG KOCKÁZAT ALAPÚ MEGKÖZELÍTÉSE – KOCKÁZATMENEDZSMENT

A kockázat mindazon elemek és események bekövetkeztének a valószínűsége, amelyek hátrányosan érinthetik az adatkezelő működését. A kockázat lehet egy esemény vagy következmény, amely lényegi befolyással van az adatkezelő szakmai célkitűzéseire.

A kockázat lehet:

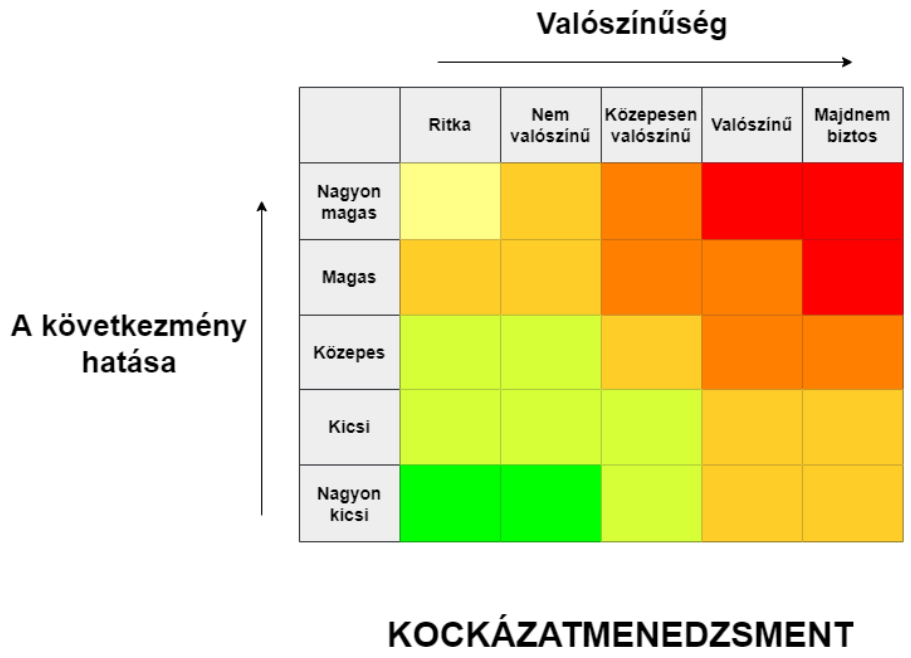
- ✓ eredendő kockázat, azaz a szabálytalanságok vagy a megvalósítás során fellépő hibák előfordulásának kockázata, illetve
- ✓ maradvány kockázat, azaz a kockázat csökkentésére tett azonnali válaszlépések (szervezeten belül működő kontroll) után még fennálló kockázat.

A kockázatok forrása lehet az adatkezelőre nézve külső eredetű kockázat, vagy az adatkezelő saját tevékenysége (vagy annak hiánya) miatt kialakuló kockázat.

A természetes személyek jogait és szabadságait érintő – változó valószínűségű és súlyosságú – kockázatok származhatnak a személyes adatok kezeléséből, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek, különösen, ha az adatkezelésből

- ✓ *hátrányos megkülönböztetés, személyazonosság-lopás vagy személyazonossággal való visszaélés, pénzügyi veszteség, a jó hírnév sérelme, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, az álnevesítés engedély nélkül történő feloldása; vagy*
- ✓ *bármilyen egyéb jelentős gazdasági vagy szociális hátrány fakadhat; vagy*
- ✓ *ha az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy nem rendelkezhetnek saját személyes adataik felett; vagy*
- ✓ *ha olyan személyes adatok kezelése történik, amelyek faji vagy etnikai származásra, vagy politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utalnak, valamint, ha a kezelt adatok genetikai adatok, egészségügyi adatok vagy a szexuális életre, büntetőjogi felelősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó biztonsági intézkedésekre vonatkoznak; vagy*
- ✓ *ha személyes jellemzők értékelésére, így különösen munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet, egészségi állapot, személyes preferenciák vagy érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére vagy előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából; vagy*
- ✓ *ha kiszolgáltatott személyek – különösen, ha gyermekek – személyes adatainak a kezelésére kerül sor; vagy*
- ✓ *ha az adatkezelés nagy mennyiségű személyes adat alapján zajlik, és nagyszámú érintettre terjed ki.*[463]

[463] GDPR (75) preambulumbekezdés



A kockázatra adott reakciók lehetnek:

- ✓ **a kockázat átadása** – ebben az esetben a kockázat bekövetkezésének valószínűsége nem csökken, hatása nem változik, azonban a kockázatviselő személye mó-dosul, például biztosítást kötünk az adott kockázat tekintetében.
- ✓ **a kockázat elviselése** – ebben az esetben az egyes tevékenységeink olyanok, hogy a napi működésünk során minden beavatkozás nélkül automatikusan kezelhető a felmerülő kockázat, ezért nincs szükség külön beavatkozásra. Az is előfordulhat, hogy azonosítottuk és felmértük a kockázatot, de nincs lehetőségünk annak kezelésére (pl. technikai akadályokba, időkorlátba vagy anyagi korlátba ütközik). A kockázat elviselése akkor különösen indokolt, ha a válaszintézkedés költségigénye aránytalanul magas.
  A kockázat elviselése tekintetében célszerű tudatos döntést hoznunk és a kockázatot figyelemmel kell kísérnünk annak érdekében, hogy az elfogadható határokon belül maradjon.
- ✓ **a kockázat kezelése** (mérséklése) esetén a célunk, hogy az eredeti célunkhoz igazodó elfogadható szintű költségigényű kockázati stratégia bevetésével a lehető legkisebb szintre csökkentsük az adott kockázati tényező hatását (pl. álnevesítés, anonimizálás stb.)
- ✓ **a kockázatos tevékenység befejezése** (a kockázat elkerülése) döntés esetén a kockázatot figyelembe véve úgy döntünk, hogy az adott adatkezelési tevékenységet megszüntetjük, illetve felfüggesztjük mindaddig, ameddig a kockázatok nem mérsékelhetők az általunk elfogadhatónak tartott szintre, vagy azt át nem tudjuk adni egy másik szervezetnek.

Adatvédelmi hatásvizsgálat

Számtalan esetben előfordulhat, hogy egyes adatkezeléseink – különösen új technológiákat alkalmazó típusa – jellegükre, hatókörükre, körülményükre és céljaikra tekintettel valószínűsíthetően magas kockázattal járnak a természetes személyek jogaira és szabadságaira nézve. Az ilyen esetekben az adatkezelést megelőzően hatásvizsgálatot kell végeznünk annak érdekében, hogy kiderítsük, a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.[464]

A norvég adatvédelmi hatóság (Datatilsynet) gyakorlatából

A Datatilsynet 4.900 eurós bírságot szabott ki egy önkormányzatra, amiért a tanulóknak a Strava fitneszalkalmazást kellett használniuk a tornaórákon anélkül, hogy előzetesen kockázatértékelést és adatvédelmi hatásvizsgálatot végeztek volna, illetve a biztonsági előírások sem voltak megfelelőek.

Alesund település két középiskolájának tanárai a Covid19 világjárvány idején megkövetelték tanulóiktól a Strava fitneszalkalmazás letöltését a tornaórákon való használatra. A tanárok az alkalmazás nyomkövető funkcióit annak igazolására használták, hogy a diákok otthon elvégezték az előírt gyakorlatokat, például egy bizonyos távolságot kerékpárral megtettek. Az alkalmazás használatának kötelezővé tétele előtt sem az önkormányzat, sem az iskolák, sem pedig a tanárok nem végeztek kockázatértékelést, illetve adatvédelmi hatásvizsgálatot sem.

Az Datatilsynet szerint az önkormányzat többszörösen megsértette a GDPR-t, többek között

- ✓ *elmulasztották az adatkezelés biztonságához szükséges technikai és szervezeti intézkedések kialakítását;*
- ✓ *nem végeztek kockázatértékelést az alkalmazás használatára vonatkozóan.*

Az adatvédelmi hatóság azt is megjegyezte, hogy a Strava Inc. általában adatkezelőnek minősül az alkalmazásban kezelt személyes adatok tekintetében, azonban ebben az esetben az önkormányzat az adatkezelő, mivel a tanárok (az iskolák) voltak azok, akik a diákok személyes adatainak kezelésének céljáról és módjáról döntöttek.[465]

[464] GDPR 35. cikk
[465] 20/02147-6 KBK/-, https://www.datatilsynet.no/contentassets/aceb0267e82e4404bd3e8b2e8987f458/vedtak-om-overtredelsesgebyr-ved-bruk-av-treningsappen-strava--alesund-kommune.pdf, utolsó letöltés 2022. 07. 31.

Adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégeznünk:

a) természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;
b) személyes adatok különleges kategóriái, vagy büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése; vagy
c) nyilvános helyek nagymértékű, módszeres megfigyelése.

Azt, hogy mikor van szükségünk hatásvizsgálatra az adatvédelmi jogszabályok által adott kritériumok alapján azt nekünk, az adatkezelőnek kell eldöntenünk (az irányadó szempont, hogy mennyire kockázatos az adott adatkezelés az érintettek jogai és szabadságai tekintetében). Természetesen olyan esetekben is végezhetünk hatásvizsgálatot, amely nem szerepel a felsorolásban.

A GDPR nevesít néhány esetet a kötelező hatásvizsgálatra

- ✓ *nagymértékű adatkezelési műveletek, amelyek jelentős mennyiségű személyes adat regionális, nemzeti vagy szupranacionális szintű kezelését célozzák, és amelyek az érintettek jelentős számára hatással lehet, és amelyek például az adatok érzékenysége folytán valószínűsíthetően magas kockázattal járnak,*
- ✓ *azok az adatkezelési műveletek, amelyeknél nagy arányban a technológia elismert állásának megfelelő új technológiát alkalmaznak,*
- ✓ *adatkezelési műveletek, amelyek magas kockázattal járnak az érintettek jogaira és szabadságaira nézve, különösen, ha az említett műveletek megnehezítik az érintettek számára, hogy a jogaikat gyakorolják.*
- ✓ *amikor az a személyes adatkezelés célja, hogy konkrét természetes személyekkel kapcsolatban döntést lehessen hozni azt követően, hogy elvégzik a természetes személyek személyes jellemzőinek szisztematikus és kiterjedt értékelését az említett adatokon alapuló profilalkotás alapján, a személyes adatok különleges kategóriáira, a biometrikus adatokra vagy a büntetőjogi felelősség megállapítására és a bűncselekményekre vagy a kapcsolódó biztonsági intézkedésekre vonatkozó adatok kezelését követően.*
- ✓ *a nyilvános helyek nagymértékű megfigyelése, különösen, ha ezt elektronikus optikai eszközök alkalmazásával hajtják végre, valamint*
- ✓ *az olyan egyéb műveletek esetében, amelyeknél az illetékes felügyeleti hatóság úgy ítéli meg, hogy az adatkezelés valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve, különösen mivel megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek, vagy mivel az említett műveletekre szisztematikusan és nagy számban kerül sor.*

A személyes adatok kezelése nem tekinthető nagymértékűnek, ha az adatkezelés egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adataira vonatkozik, ilyen esetekben az adatvédelmi hatásvizsgálatot nem kell kötelezővé tenni.

Bizonyos körülmények között észszerűnek és gazdaságosnak bizonyulhat az adatvédelmi hatásvizsgálat nem egyetlen projekt tekintetében történő lefolytatása, például ha több adatkezelő közös alkalmazást vagy adatkezelési környezetet kíván bevezetni valamely ágazat vagy szegmens, vagy valamely széles körben végzett horizontális tevékenység tekintetében. [GDPR (91)-(92) preambulumbekezdés]

A 29. cikk szerint Adatvédelmi Munkacsoport is ad támpontot[466] adatvédelmi hatásvizsgálatot megkövetelő adatkezelések tekintetében.

Adatkezelés leírása	***Az adatvédelmi hatásvizsgálat oka (lényeges szempontok)***
Betegek genetikai és egészségügyi adatait kezelő kórház (kórházi információs rendszer)	✓ *különleges adatok vagy fokozottan személyes jellegű adatok* ✓ *kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok.* ✓ *nagy számban kezelt adatok*
Kamerarendszer használata a vezetői magatartás megfigyelésére az autópályákon. Az adatkezelő intelligens videóelemző rendszer használatát tervezi járművek kiszűrése és automatikus rendszámfelismerés céljából	✓ *módszeres megfigyelés* ✓ *technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása*
Az alkalmazottai tevékenységeit módszeresen megfigyelő, így az alkalmazottak munkaállomását, internetes tevékenységeit stb. nyomon követő vállalkozás	✓ *módszeres megfigyelés* ✓ *kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok*
A közösségi médiából származó nyilvános adatok gyűjtése profilalkotás céljából	✓ *értékelés vagy pontozás* ✓ *nagy számban kezelt adatok* ✓ *adatkészletek egymással való megfeleltetése vagy összevonása* ✓ *különleges adatok vagy fokozottan személyes jellegű adatok*
Országos hitelminősítési vagy csalásellenes adatbázist létrehozó pénzügyi vállalkozás	✓ *értékelés vagy pontozás.* ✓ *joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal* ✓ *megakadályozza, hogy az érintett a jogait gyakorolja vagy szolgáltatást vegyen igénybe vagy szerződést érvényesítsen*

[466] WP 248 rev.01. 13. oldal

	✓ *különleges adatok vagy fokozottan személyes jellegű adatok*
Kutatási projektekben vagy klinikai vizsgálatokban részt vevő, kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos, álnevesített, különleges személyes adatok tárolása archiválás céljából	✓ *különleges adatok* ✓ *kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok* ✓ *megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek*

Amennyiben úgy döntünk, hogy az adott adatkezelés mégsem jár „valószínűsíthetően magas kockázattal" (bár az iránymutatás alapján akár azzal is járhatna), a döntésünket indokolnunk és dokumentumokkal igazolnunk kell, az adatvédelmi hatásvizsgálat mellőzésének okait és az adatvédelmi tisztviselőnk álláspontját pedig rögzítenünk kell.

Az olasz adatvédelmi hatóság (Garante per la protezione dei dati personali, „Garante") gyakorlatából

A Garante 84 000 eurós bírságot szabott ki a bolzanói önkormányzatra a munkavállalók válogatás nélküli megfigyelése miatt. Az önkormányzat egyik alkalmazottja szerint a munkáltatója az alkalmazottak hálózati forgalmát és egyéni internet-hozzáféréseit figyelte, megsértve a jogszerűség, a pontosság és az adatok minimalizálása elvét. Az önkormányzat olyan rendszert használt az internet-hozzáférések nyilvántartására, amely lehetővé tette a meglátogatott internetes oldalak kronológiájának és az egyes oldalak böngészés idejének tömeges, folyamatos és válogatás nélküli megfigyelését, nyomon követését és szűrését, valamint az egyes alkalmazottakhoz kapcsolódó adatok hosszú ideig történő tárolását és megőrzését. A bejelentő szerint a megfigyelésre úgy került sor, hogy a munkavállalókat nem tájékoztatták az internet-hozzáférés lehetséges ellenőrzéséről.

A Garante a vizsgálat során feltárta, hogy

- ✓ *az önkormányzat mintegy tíz éven keresztül olyan rendszert használt a munkavállalók internetes böngészésének nyomon követésére és szűrésére, amely egy hónapig tárolta a munkavállalók adatait és hálózatbiztonsági célokból jelentéseket is készített.*
- ✓ *a rendszert az egyes alkalmazottak által látogatott weboldalakra vonatkozó adatok megelőző és általános gyűjtését végezte, és bár a munkáltató az ágazati szabályozásban előírtaknak megfelelően megállapodást kötött a szakszervezetekkel az adatgyűjtésről, az nem felelt meg a GDPR alapelveinek.*
- ✓ *az önkormányzat nem tájékoztatta megfelelően a munkavállalókat az adatkezelésről, amely olyan adatkezelési műveleteket tett lehetővé, amelyek szükségtelenek és aránytalanok voltak a belső hálózat védelmének és biztosításának céljához képest, illetve a rendszer a szakmai tevékenységhez nem kapcsolódó, a munkavállalók magánéletével kapcsolatos információkat is gyűjtött.*
- ✓ *az önkormányzat elmulasztotta az adatvédelmi hatásvizsgálat elvégzését.*

A Garante álláspontja szerint az internet helytelen használatának kockázatát csökkentő igény nem vezethet a munkavállaló magánélethez fűződő elvárásainak teljes megsemmisítéséhez a munkahelyen még akkor sem, ha a munkavállaló a munkáltató által rendelkezésre bocsátott hálózati szolgáltatásokat használja.

A bírság kiszabásán kívül a Garante kötelezte az önkormányzatot, hogy hozzon technikai és szervezési intézkedéseket

- ✓ *a munkavállalók munkaállomásaihoz kapcsolódó adatok anonimizálására,*
- ✓ *a rögzített webes navigációs naplókban szereplő személyes adatok törlésére, valamint*
- ✓ *frissítse a szakszervezeti megállapodásban meghatározott belső eljárásokat.*[467]

A GDPR alapján a felügyeleti hatóságoknak össze kell állítaniuk egy olyan listát,[468] amelyen szerepelnek azok az adatkezelések, amelyek esetében kötelező adatvédelmi hatásvizsgálatot végeznünk.

A görög adatvédelmi hatóság (HDPA) gyakorlatából

A görög adatvédelmi hatóság 6 millió euróra, illetve 3,25 millió euróra bírságolta a COSMOTE mobil távközlési vállalatot és annak anyavállalatát, az OTE-t.

2020-ban a COSMOTE mobil távközlési vállalat külső kibertámadást szenvedett el, melyben érintett volt az egyik szerveren tárolt 30 GB-os, 2020. 09. 01. és 2020. 09. 05. közötti időszakra vonatkozó személyes adatokat tartalmazó fájl. A fájl több millió előfizetői adatot tartalmazott (telefonszámok, bázisállomás koordinátái, IMEI, IMSI, időbélyeg, hívás időtartama, szolgáltatói azonosító, előfizetési terv, életkor, nem, egy felhasználóra jutó átlagos bevétel).

A COSMOTE általános gyakorlata az volt, hogy begyűjtötte a telefonszámokat, a bázisállomás koordinátáit, IMEI-ket, IMSI-ket, időbélyegeket, a hívások időtartamát és a szolgáltatói azonosítókat. Ezeket az adatokat három hónapig tárolta az hibakezelési rendszerében a kommunikáció átvitelében előforduló műszaki hibák vagy hibák felderítéséhez (a cég jogszabályi kötelezettsége, hogy hatékony hibakezelési rendszerrel rendelkezzen a zavartalan szolgáltatás biztosítása érdekében).

A cég a három hónap elteltével nem törölte az adatokat, hanem kiegészítette azokat az előfizetési terv, az életkor, a nem és az egy főre jutó átlagos bevétel adataival, majd ezt a fájlt „anonimizálta" és 12 hónapig tárolta, statisztikai célokra felhasználva (mobilhálózata kialakításának optimalizálására).

A HDPA megállapította, hogy a COSMOTE

[467] Ordinanza ingiunzione nei confronti di Comune di Bolzano – 13 maggio 2021 [9669974], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9669974, utolsó letöltés 2022. 07. 31.
[468] NAIH hatásvizsgálati listája: https://naih.hu/hatasvizsgalati-lista

- ✓ *megsértette az elektronikus hírközlési adatvédelmi irányelvet nemzeti jogba ültető jogszabályt, mivel a forgalmi adatok egy korlátozott részhalmazának és nem az összes forgalmi adatnak a tárolása elegendő lett volna a hibaelhárítás céljára, valamint az adatok három hónapig tárolása szintén nem volt szükséges e célból.*
- ✓ *nem dokumentálta megfelelően az adatvédelmi hatásvizsgálatot, és nem bizonyította, hogy minden kockázatot figyelembe vett.*
- ✓ *megsértette az átláthatóság elvét, mert bár tájékoztatta az előfizetőket az adatkezelésről, az értesítés nem volt elég pontos a hibakezelés célját illetően, mivel csak „a szerződés kiszolgálásáról" és „a hálózati problémák megoldásáról és a szolgáltatás javításáról" szólt. Az értesítés nem említette a három hónapos tárolási időt sem.*
- ✓ *a statisztikai célú adatkezelést anonimizált adatokkal kellett volna végezni, azonban a cég mechanizmusa csak álnevesítette az adatokat, ami nem volt elegendő, mivel a COSMOTE továbbra is hozzáférhetett a személyes kulcshoz, és így visszafejthette az adatokat.*
- ✓ *elmulasztott megfelelő műszaki és szervezési intézkedéseket tenni a szolgáltatásai biztonságának, valamint a nyilvános elektronikus hírközlési hálózat biztonságának védelme érdekében. A HDPA vizsgálata hat sebezhetőséget is feltárt, amelyeket a határozat bizalmas melléklete részletez.*
- ✓ *és az OTE (az anyavállalat) nem dokumentálta, hogy együttműködésük hogyan épült fel, így nem lehetett bizonyítani, hogy betartották-e az integritás és bizalmas kezelés elvét. A két társaságnak az együttműködést és a felelősség megosztását vagy közös adatkezelésre vonatkozó megállapodásra kellett volna alapoznia (amennyiben közös felelősségről van szó), vagy adatfeldolgozó megállapodásra (amennyiben az adatkezelés kiszervezéséről van szó). Mivel egyiket sem tették meg, a COSMOTE megsértette az elszámoltathatóság elvét is.*

A HDPA megállapította, hogy az OTE (annak ellenére, hogy nem rendelkezett megfelelő, a szerepét meghatározó megállapodással) elmulasztotta a megfelelő technikai és szervezési intézkedések végrehajtását, függetlenül attól, hogy közös adatkezelőként vagy adatfeldolgozóként járt el.[469]

Az adatvédelmi hatásvizsgálatunknak ki kell terjednie legalább az alábbiakra:

- ✓ a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljaink ismertetésére, beleértve adott esetben az érvényesíteni kívánt jogos érdeket;
- ✓ az adatkezelés céljainkra figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
- ✓ az érintettek jogait és szabadságát érintő kockázatok vizsgálatára;
- ✓ a kockázatok kezelését célzó (biztonsági) intézkedések bemutatására, például a személyes adatok védelmét és a GDPR előírásaival való összhang igazolására szolgáló, az érintettek és egyéb személyek jogait és jogos érdekeit figyelembe vevő garanciákra, biztonsági intézkedésekre és

[469] ΑΠΟΦΑΣΗ 4/2022, https://www.dpa.gr/sites/default/files/2022-01/4_2022%20anonym%20%282%29_0.pdf, utolsó letöltés: 2022. 07. 31.

mechanizmusokra. Az elemzésnek ki kell térnie arra is, hogy az egyes kockázatok bekövetkeztére mekkora esélyünk van, illetve, hogy a tervezett biztonsági intézkedések valóban hatékonyan tudják kezelni a kockázatokat;

- ✓ a kockázatkezelési tervünkre, amelynek ki kell terjednie
  - azon konkrét intézkedéseinkre, amelyekkel az érintettek jogaira és szabadságaira kockázatot jelentő elemeket meg szeretnénk szüntetni, illetve csökkenteni;
  - azon személyek megnevezésére, akikkel szükség esetén egyeztetni tudunk ezen intézkedések tárgyában;
  - mikorra és milyen források segítségével ültetjük át ezeket az intézkedéseket a gyakorlatba;
  - az intézkedésektől milyen eredményeket várunk el és hogyan fogjuk azokat mérni;
  - az intézkedések végrehajtásával, illetve az eredményesség ellenőrzésével kapcsolatban kik a felelősök;
- ✓ a megállapítások és intézkedések teljes körű dokumentálására.

Az üzleti érdekek, a közérdek védelmének vagy az adatkezelési műveletek biztonságának sérelme nélkül kikérhetjük az érintettek vagy képviselőik véleményét is a tervezett adatkezelésről, sőt bevonhatunk jogászokat, közgazdászokat, szociológusokat és egyéb olyan szakembereket, akik szaktudása segítheti az adatvédelmi hatásvizsgálatunkat.

A 29. cikk szerinti adatvédelmi munkacsoport gyakorlatából

A biometrikus adatok kezelésével járó speciális kockázatok miatt a munkacsoport azt ajánlja, hogy már az ilyen típusú adatokat kezelő rendszerek tervezési szakaszában hajtsuk végre az adatvédelmi hatásvizsgálatot, és vegyük figyelembe az alábbiakat:

- ✓ *a gyűjtött információk célja és jellege;*
- ✓ *a rendszer pontossága és a pontatlanság kihatásai;*
- ✓ *a választott jogalap és a jogszerűség követelményeinek teljesíthetősége;*
- ✓ *a szükséges biztonsági technikák és eljárások a személyes adatok engedély nélküli hozzáférés elleni védelme érdekében;*
- ✓ *a magánéletbe kevésbé beavatkozó intézkedéseket már meghoztuk-e; van-e alternatív eljárás a biometrikus eszközön kívül (mint például a személyi igazolvány elkérése);*
- ✓ *a megőrzési időre (releváns időtartamra) és az adatok törlésére vonatkozó döntések;*
- ✓ *alkalmazunk-e automatikus döntési mechanizmust és rendelkezünk-e megfelelő tartalékeljárással;*
- ✓ *hogyan kívánjuk az érintetti jogokat biztosítani.*

Figyelmet kell fordítanunk a megfelelő adatvédelmi intézkedésekre és arra is, hogy hogyan találunk megfelelő megoldásokat a hatásvizsgálat során azonosított adatvédelmi kockázatok enyhítésére.[470]

[470] 29. cikk szerinti adatvédelmi munkacsoport 3/2012. sz. vélemény a biometrikus technológiák terén történt

A francia adatvédelmi hatóság (CNIL) szoftvere ötleteket ad a kockázatcsökkentés kategóriáira is, mind logikai, mind fizikai, mind pedig szervezeti (adminisztratív) szempontból.

A hatásvizsgálat nem egyszeri folyamat, ha változnak az adatkezelés feltételei (kockázatai), újra le kell folytatnunk azt.

Vannak azonban olyan esetek, amikor nem tudjuk a kockázat mértékét elfogadható mértékűre csökkenteni, ilyen például,[471]

- ✓ ha az érintettek olyan jelentős vagy akár visszafordíthatatlan következményekkel szembesülnek, amelyekkel nem tudnak leküzdeni (például adatokhoz való jogosulatlan hozzáférés, amely az érintettek életét fenyegető veszélyt, elbocsátást vagy pénzügyi nehézséget eredményez), és/vagy
- ✓ ha egyértelműnek tűnik, hogy kockázat be fog következni (például azért, mert az adatok megosztásának, felhasználásának vagy terjesztésének módja miatt nem lehet csökkenteni az adatokhoz hozzáférő személyek számát, vagy a közismert sebezhetőségre nem készül javítókészlet).

Amennyiben nem tudunk megfelelő intézkedéseket hozni a kockázatok elfogadható szintre való csökkentésére, azaz a fennmaradó kockázatok továbbra is jelentősek, akkor kötelező konzultálnunk a felügyeleti hatósággal („előzetes konzultáció”[472]).

A tagállami jog előírhatja, hogy az adatkezelők konzultáljanak a felügyeleti hatósággal, és szerezzék be a felügyeleti hatóság előzetes engedélyét akkor is, ha valamely közérdek alapján ellátandó feladat végrehajtásához kapcsolódóan kezelnek személyes adatokat, ideértve a személyes adatoknak a szociális védelemhez és a népegészségügyhöz kapcsolódó kezelését is.

Az olasz adatvédelmi hatóság (Garante per la protezione dei dati personali, „Garante”) gyakorlatából

A GDPR 36. cikkének (5) bekezdése alapján az olasz Egészségügyi Minisztérium benyújtotta a „Covid-19 Alert System” (és annak hivatalos mobilalkalmazása, az „Immuni”) adatvédelmi hatásvizsgálatát az olasz adatvédelmi hatóságnak, mely ismertette a minisztérium által az adatkezelés megfelelő biztonsági szintjének biztosítása érdekében elfogadott technikai és szervezési intézkedéseket.

A hatóságnak a GDPR 36. cikkével összhangban döntenie kellett a tervezett adatkezelés GDPR szerinti megfelelőségéről. A Garante felhatalmazta az Egészségügyi Minisztériumot az adatkezelés megkezdésére, azonban egy sor, 30 napon belül végrehajtandó további intézkedést előírt az adatkezelés biztonságának megerősítése érdekében:

fejleményekről, 2012. április 27, 00720/12/HU WP193, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_hu.pdf, utolsó letöltés: 2022.08.19

[471] WP 248 rev.01. 22. oldal

[472] GDPR 36. cikk

- ✓ *az algoritmus pontos leírása az adatvédelmi hatásvizsgálatban a konfigurációs paraméterek, feltételezések és egyéb tényezők megadásával, valamint a tudományos közösség számára történő hozzáférhetővé tétele;*
- ✓ *a felhasználók világos és érthető tájékoztatást kapjanak az algoritmusról (infografikák és hasonló eszközök segítségével is);*
- ✓ *tájékoztatni kell a felhasználókat arról a lehetőségről, hogy az alkalmazás olyan expozíciós értesítéseket generálhat, amelyek nem mindig tükrözik a tényleges kockázati állapotot (hamis „pozitív eredmények”);*
- ✓ *lehetővé kell tenni a felhasználók számára az alkalmazás ideiglenes kikapcsolását egy könnyen hozzáférhető funkció segítségével;*
- ✓ *megfelelő módszerek meghatározása az alkalmazás háttértárában lévő analitika védelmére, elkerülve az azonosítható alanyokhoz való újbóli hozzárendelés minden formáját;*
- ✓ *megfelelő biztonsági intézkedések és anonimizálási technikák elfogadása a ténylegesen követett konkrét céloknak megfelelően, a beépített és alapértelmezett adatvédelem elveivel összhangban;*
- ✓ *a hatásvizsgálat és az adatvédelmi szabályzatok integrálása a törlési és tiltakozási jog gyakorlásának módjával kapcsolatban;*
- ✓ *az adatfeldolgozók és az adatkezelési tevékenységekben részt vevő egyéb alanyok szerepének részletesebb leírása, kiemelve az érintetteket érintő esetleges kockázatokat;*
- ✓ *a felhasználók IP-címét csak a rendellenességek és támadások észleléséhez feltétlenül szükséges mértékben tárolja, majd törölje;*
- ✓ *intézkedések végrehajtása a rendszergazdák által az operációs rendszerekben a hálózaton és az adatbázisokon végzett műveletek nyomon követésének biztosítása érdekében (nem csak a be- és kijelentkezés).*[473]

GDPR

- ✓ Adatvédelmi hatásvizsgálat [GDPR 35. cikk és a (75), (84), (89)-(93) preambulumbekezdések]
- ✓ Előzetes konzultáció [GDPR 36. cikk és a (94)-(96) preambulumbekezdések]

Szakirodalom

- ✓ A 29. cikk szerinti Adatvédelmi Munkacsoport: Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e, WP248rev.01, Az elfogadás időpontja: 2017. április 4., a legutóbbi felülvizsgálat és elfogadás időpontja: 2017. október 4. (továbbiakban: WP248rev.01)

[473] Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid 19- App Immuni – 1° giugno 2020 [9356568], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9356568, utolsó letöltés 2022. 07. 31.

Az adatvédelmi incidens

Az adatvédelmi incidens a legkockázatosabb esemény, ami történhet az általunk kezelt adatokkal.

Az adatvédelmi incidens fogalma

A GDPR szerint az adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes

- ✓ megsemmisítését,
- ✓ elvesztését,
- ✓ megváltoztatását,
- ✓ jogosulatlan közlését vagy
- ✓ az azokhoz való jogosulatlan hozzáférést eredményezi.

Az adatvédelmi incidensek a fentiek alapján lehetnek

- ✓ bizalmassági incidensek (a személyes adatok véletlen vagy felhatalmazás nélküli közlése, illetve az ezekhez való hozzáférés);
- ✓ sértetlenséggel kapcsolatos incidensek (a személyes adatok véletlen vagy jogtalan megváltoztatása);
- ✓ hozzáférhetőséggel kapcsolatos incidensek (a személyes adatok véletlen vagy jogtalan megsemmisítése vagy ezek elvesztése).

Egy adatvédelmi incidens akár több kategóriába is besorolható, például egy hacker az általa megtámadott rendszerben a fájlokat nemcsak lemásolja, hanem azok egyik felét módosítja, míg a másik felét visszaállíthatatlanul törli.

Adatkezelőként a feladatunk az adatok, illetve az adatokon keresztül az érintettek jogainak és szabadságainak védelme, ezért mindent meg kell tennünk annak érdekében, hogy az adatvédelmi incidensek előfordulását és azok kockázatát a lehető legkisebb mértékűre csökkentsük.

Természetesen olyan adatkezelő nem létezik, akinél esélye sincs egy adatvédelmi incidensnek, hiszen elég csak egy munkatársnak figyelmetlennek lenni és máris megtörténik a baj, rossz helyre lesz elküldve egy e-mail / nem titkos másolatban lesznek benne a címzettek vagy ledarálás nélkül lesz kidobva a szelektív gyűjtőbe egy irat.

A holland adatvédelmi hatóság gyakorlatából

A holland adatvédelmi hatóság olyan e-mailt küldött ki, amelyben az e-mail címek hosszú listája mindenki számára láthatóan a másolat („CC:”) mezőben szerepelt, ahelyett, hogy a titkos másolat („BCC:”) mezőben lett volna elrejtve. Az e-mail 38 újságíró és szerkesztő e-mail címét tette közzé és egy olyan kampány keretében küldték ki, amelynek célja az volt, hogy felhívja a figyelmet a GDPR szabályaira.

Az újságírók megérdeklődték, a hatóság bejelentette-e saját magát önmagánál. Igen, bejelentette.[474]

Az adatvédelmi incidens oka a munkavállalók véletlen hibájától a külső fenyegetésig (ipari kémkedés, kiberbűnszervezetek tevékenysége) bármi lehet, a mi feladatunk pedig annak megoldása, hogy a lehető legfelkészültebbek legyünk, azaz legyen eljárásrendünk az ilyen események kezelésére.

A spanyol adatvédelmi hatóság (AEPD) gyakorlatából

Benidorm városa adatvédelmi incidensről értesítette az AEPD -t, mely során tudatta a hatósággal, hogy a pszichopedagógiai segélyekről szóló ideiglenes határozatának közzététele során a segélyt kérelmezőkre vonatkozó adatokat tettek közzé.

A nyilvánosságra került információk között voltak

- ✓ *azonosító adatok (név és vezetéknév, a szülők személyi azonosítója, kiskorúak neve és vezetékneve)*
- ✓ *gazdasági adatok (kezelési költségek, bankszámla, összeg és halasztás)*
- ✓ *egészségügyi adatok (az alkalmazott kezelés és annak vége), valamint*
- ✓ *egyéb adatok (iskola és az elutasítás indoklása).*

Az AEPD megállapította, hogy a GDPR 4. cikkének 12. pontja szerinti „adatvédelmi incidens" történt az önkormányzati honlapon a pszichopedagógiai segélyekről szóló ideiglenes határozat közzététele során. Mivel a vizsgálat kimutatta, hogy Benidorm városi tanácsa észszerű protokollokkal rendelkezett az ilyen incidensekre, és időben reagált a hatás minimalizálása, valamint a jövőbeni megismétlődés elkerülése érdekében, nem szabtak ki bírságot. Az adatvédelmi incidens miatt egyetlen érintett sem nyújtott be panaszt vagy lépett kapcsolatba az AEPD-vel.[475]

Az adatvédelmi incidensek különösen károsak lehetnek az érintettek magánélethez és adataik védelméhez való jogaira nézve, hiszen az incidens eredményeképp elveszítik az ellenőrzést a személyes adataik felett.

Az incidens következménye lehet *– többek között –*

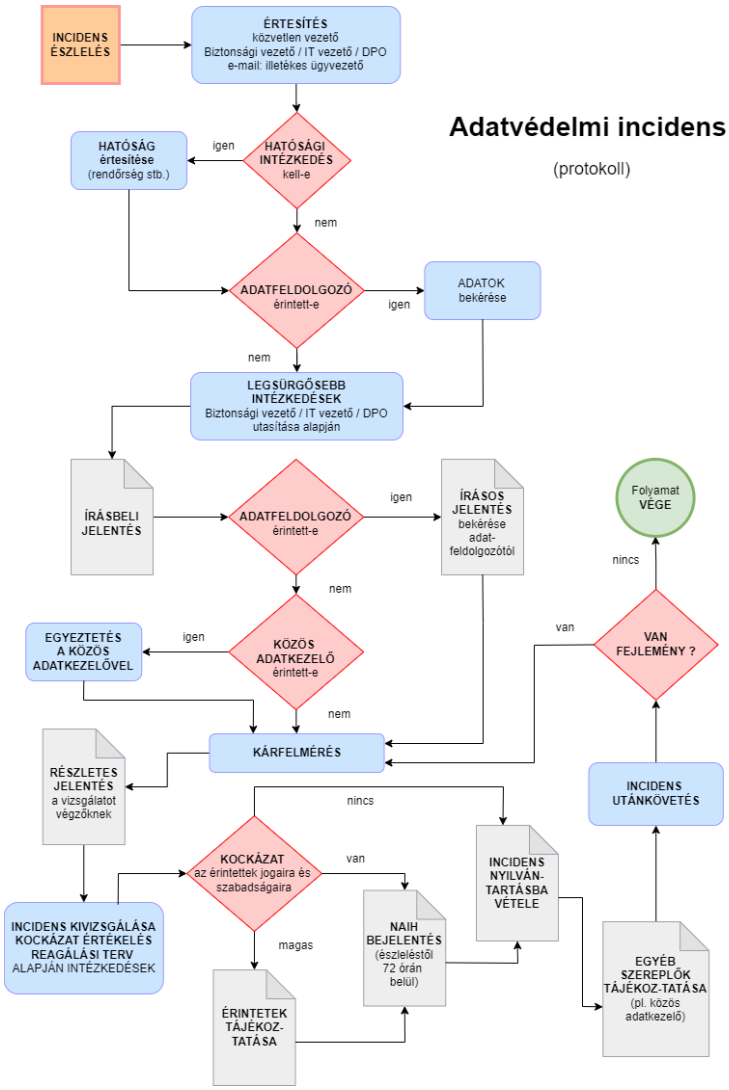
- ✓ *az érintettek személyazonosságának ellopása;*
- ✓ *az érintettek bűncselekmény áldozatává válhatnak, például zaklatják őket;*
- ✓ *elveszthetik a megélhetésünket, pénzügyi veszteség vagy vagyoni kár érheti őket;*
- ✓ *szakmai titoktartás által védett személyes adataik bizalmas jellege megsérül;*
- ✓ *úgy profilozzák az érintetteket, ahogy azt nagyon nem szeretnék, és olyan következményei vannak a profilozásnak, amelyre nagyon, de nagyon nem vágynak;*

[474] Graham Cluley: Data protection authority reports itself to itself after data breach, June 3, 2019, https://grahamcluley.com/data-protection-authority-reports-itself-to-itself-after-data-breach/

[475] Procedimiento Nº: E/08452/2019, https://www.aepd.es/es/documento/e-08452-2019.pdf, 2022. 07. 31.

- ✓ *az érintettek legprivátabb élete kerül napvilágra (vallási meggyőződésük, világnézetük, egészségi állapotuk, szexuális életük stb.);*
- ✓ *magánéleti válságba kerülhetnek; és akár*
- ✓ *a hírnevük is csorbulhat.*

Az érintettek általában nem tudják, hogy az adatvédelmi incidens történt a személyes adataikkal kapcsolatban, ezért nem képesek megtenni a szükséges lépéseket annak érdekében, hogy megvédjék magukat annak negatív következményeitől, például módosítsák a felhőszolgáltatónál kompromittálódott jelszavukat vagy letiltassák a hitelkártyájukat. Éppen ezért a GDPR bizonyos esetekben előírja, hogy kötelező értesítenünk a felügyeleti hatóságot, illetve az érintetteket az adatvédelmi incidens megtörténtéről és töredelmesen be kell vallanunk mindazokat a körülményeket és hatásokat, amelyeket ilyenkor a GDPR alapján be kell vallanunk.



Az adatvédelmi incidens bejelentése a felügyeleti hatósághoz

A GDPR meglehetősen rövid időt határidőt szab a bejelentésre:

- ✓ amennyiben adatkezelők vagyunk, abban az esetben kötelesek vagyunk bizonyos incidenseket indokolatlan késedelem nélkül, ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomásunkra jutott, bejelenteni az illetékes hatóságnak. Ha a bejelentést 72 órán belül nem tettük meg, akkor meg kell adnunk a késedelem okát és kizárólag akkor mentesülünk a bejelentési kötelezettség alól, ha igazolni tudjuk, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal az érintett személyek jogaira és szabadságaira nézve.
- ✓ amennyiben adatfeldolgozók vagyunk, az adatvédelmi incidenst az arról való tudomást szerzésünket követően indokolatlan késedelem nélkül be kell jelentünk az adatkezelőnek, ugyanis a 72 óra a mi tudomásszerzésünk időpontjától ketyeg nem pedig attól az időponttól, amikor az incidensről értesítettük a megbízónkat.

Az incidensről igen részletes értesítést kell küldenünk az adatvédelmi hatóság felé annak érdekében, hogy a hatóság – a bejelentésünk alapján indított – vizsgálat keretében meg tudja vizsgálni, kinek róható fel az eset.

A máltai adatvédelmi hatóság (IDPC) gyakorlatából

Az IDPC 65 ezer eurós bírságot szabott ki a C-Planet informatikai vállalatra, mivel az nem jelentett be egy adatvédelmi incidenst, és nem hajtott végre megfelelő technikai intézkedéseket az adatvédelmi incidens megelőzésére. Az adatvédelmi incidens azt is feltárta, hogy a személyes és különleges adatkategóriák kezelésére megfelelő jogalap nélkül került sor, és hogy az érintettek nem kapták meg a GDPR 14. cikke szerinti tájékoztatást.

2020. április 1-jén a média beszámolt a C-PLANET adatvédelmi incidenséről, amelynek során nyilvánosságra került a máltai választók személyes adatait (335 ezer választópolgár politikai véleményét) tartalmazó adatbázis.
Az IDPC hivatalból vizsgálatot indított, mely során arra a következtetésre jutott, hogy a C-PLANET volt az adatbázis adatkezelője és semmilyen ténybeli elem sem támasztotta alá a C-PLANET azon álláspontját, hogy egy harmadik fél lett volna az adott adatbázis adatkezelője.

Az IDPC az adatkezelés jogszerűségével kapcsolatban arra a következtetésre jutott, hogy bár az adatok egy részét a választási nyilvántartásból gyűjtötték, ebben az esetben is szükség volt a GDPR 6. cikkének (1) bekezdése szerinti megfelelő jogalapra. Az IDPC a kezelt, nem nyilvánosan hozzáférhető személyes adatokat is figyelembe vette, mint például az érintettek szavazóurnaszámát, szavazási okmányának számát, körzetét, születési dátumát, telefonszámát és nemét, melyek a vonatkozó máltai jogszabály alapján csak a politikai pártok számára állnak rendelkezésre. A Választási Bizottság megerősítette, hogy ezeket az adatokat nem bocsátották a vizsgálatban említett párt delegáltak rendelkezésére.

Az adatok különleges kategóriáira is hivatkoztak, mivel az adatbázis 1-4-ig azonosított számokat tartalmazott, amelyek az érintettek politikai véleményére utalnak, az IDPC szerint a GDPR 9. cikkének (2) bekezdése szerinti kivételek egyike sem volt alkalmazható ezen adatok jogszerű feldolgozására.

Az IDPC az érintettek tájékoztatásával kapcsolatban megállapította, hogy az adatkezelő az adatokat harmadik féltől szerezte be és köteles lett volna tájékoztatni az érintetteket az adatkezelési műveletek részleteiről, ami alapvető feltétele az adatkezelés átláthatóságának és tisztességességének biztosításának, valamint annak, hogy az érintettek gyakorolhassák a személyes adataik feletti ellenőrzést. Az adatkezelő nem a GDPR 14. cikkében előírt módon tájékoztatta az érintetteket.

Az IDPC az adatvédelmi incidens bejelentésére vonatkozó kötelezettséggel kapcsolatban úgy ítélte meg, hogy az adatvédelmi incidens magas kockázattal járt az egyénekre nézve, figyelembe véve a következő elemeket: az érintett adatok érzékenysége, a megsértett adatok nagy mennyisége, az egyénekre nézve a kár kockázata, az egyének könnyű azonosíthatósága, az érintett egyénekre nézve a következmények súlyossága és az érintett egyének száma.

A magas kockázat miatt az adatkezelőnek legkésőbb 72 órával azután, hogy tudomására jutott a jogsértés, értesítenie kellett volna az IDPC-t, és az érintetteket is tájékoztatnia kellett volna az incidensről.

Mindezeken kívül az adatkezelőknek és az adatfeldolgozóknak a tudomány és a technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket kellett volna végrehajtania. A szakértői jelentés szerint ezek a technikai intézkedések hiányoztak, különös tekintettel az adatok jellegét és az érintett kockázatot figyelembe véve.

Az IDPC a határozatában figyelembe vette még az adatbázis méretét, valamint azt a tényt, hogy a szóban forgó adatokat más adatokkal összevetették vagy kombinálták. Az adatkezelő nem értékelte a kockázatokat és az adatkezelési tevékenységek hatását, és így lehetetlenné tette egy olyan kockázat kezelését, amelyet még csak nem is azonosított előzetesen. [476]

[476] The Commissioner issues the decision on the personal data breach suffered by C-Planet (IT Solutions) Ltd, https://idpc.org.mt/idpc-publications/idpc-issues-decision-on-cplanet-data-breach/, utolsó letöltés: 2022. 07. 31.

Az adatvédelmi incidenssel kapcsolatos – hatóság felé történő – bejelentésünknek minimum az alábbiakra kell kitérnie:

- ✓ ismertetnünk kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- ✓ közölnünk kell az adatvédelmi tisztviselőnk vagy a további tájékoztatást nyújtó egyéb kapcsolattartónk nevét és elérhetőségeit;
- ✓ ismertetnünk kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- ✓ ismertetnünk kell az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseinket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseinket.

Ha és amennyiben nem lehetséges az információkat egyidejűleg közölnünk, azokat további indokolatlan késedelem nélkül később részletekben is közölhetjük. A bejelentést a hatóság nyomtatvánnyal segíti, amely megtalálható a hatóság honlapján.

A kutatás során kitértünk arra a kérdésre, hogy a megkérdezettek miként értékelik azt, hogy érintettek voltak-e már adatvédelmi incidensben. A 300 feldolgozott kérdőíven a megkérdezettek csak 15 esetben válaszoltak „igen”-nel, a többi megkérdezett nem írt választ, feltehetően a kiberbiztonsági, illetve az adatvédelmi incidens fogalma nem volt ismert a számukra. A kérdésünk („véleménye szerint kerültek-e már illetéktelen kezekbe az Ön személyes adatai”) arra irányult, hogy a megkérdezettek tisztában vannak-e azzal, hogy adataik egyáltalán illetéktelen kezekbe kerülhetnek. Valószínűsíthető, hogy a fő probléma az, hogy az érintettek gyakorlatilag fel sem tudják mérni azt, hogy a tárolt adataikat bárki illetéktelenül megszerezheti tudtukon kívül és emiatt kialakul bennük egy „hamis” biztonságérzet.

Az ír adatvédelmi hatóság (DPC) gyakorlatából

A DPC 70 ezer eurós bírságot szabott ki a University College Dublinra (UCD), amiért adatkezelőként nem hajtott végre megfelelő biztonsági intézkedéseket, a szükségesnél hosszabb ideig tárolta az adatokat, valamint nem értesítette indokolatlan késedelem nélkül a DPC-t az adatvédelmi incidensről.

A DPC vizsgálatot indított az UCD ellen miután az hét adatvédelmi incidensről értesítette. A bejelentések olyan esetekre vonatkoztak, amikor illetéktelen harmadik személyek hozzáférkőztek az UCD e-mail fiókjaihoz, illetve amikor az UCD e-mail fiókjainak bejelentkezési adatait az interneten közzétették.

A DPC megállapította, hogy az UCD

- ✓ *az e-mail szolgáltatásában nem kezelte a személyes adatokat oly módon, hogy megfelelő technikai és szervezési intézkedésekkel biztosította volna a személyes adatok megfelelő biztonságát;*
- ✓ *egy e-mail fiókban személyes adatokat olyan formában tárolt, amely az érintettek azonosítását a személyes adatok feldolgozásának céljához szükségesnél hosszabb ideig tette lehetővé;*

- ✓ *az egyik adatvédelmi incidenst csak 13 nappal azután jelentette be, hogy tudomást szerzett róla.*[477]

A hatóság az incidens miatt figyelmeztetésben részesíthet minket, de akár bírságot is kiszabhat ránk. Ha pedig az incidens létrejöttében közreműködött az adatfeldolgozónk is, a hatóság őt sem fogja kímélni.

Amennyiben adatkezelők vagyunk és olyan adatfeldolgozót (alvállalkozót) bíztunk meg adatfeldolgozás végzésével, aki hozzáértése hiányában adatvédelmi incidenst okozott, az ő tettéért ugyanúgy felelünk, mintha mi követtük volna el az incidenshez vezető cselekményeket. A hatóság előtt nem hivatkozhatunk arra, hogy a megbízottunk volt az inkompetens – a mi felelősségünk, hogy szakmailag megfelelő alvállalkozóra bízzuk a személyes adatok kezelését, és ne csak megbízzuk, hanem rendszeresen ellenőrizzük is atekintetben, hogy hogyan felel meg a GDPR előírásainak.

Érintettek tájékoztatása

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve, abban az esetben indokolatlan késedelem nélkül tájékoztatnunk kell őket az adatvédelmi incidensről. A tájékoztató tartalmát szabályozza a GDPR annak érdekében, hogy minden olyan információt megadjunk, amely segíti az érintetteket az incidens okozta kellemetlenségek, illetve kár enyhítésében, valamint leküzdésében.

Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetnünk kell az adatvédelmi incidens jellegét, és

- ✓ közölnünk kell legalább az adatvédelmi tisztviselőnk vagy a további tájékoztatást nyújtó egyéb kapcsolattartónk nevét és elérhetőségeit;
- ✓ ismertetnünk kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- ✓ ismertetnünk kell az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseinket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseinket.

A holland adatvédelmi hatóság gyakorlatából

2019 októberében egy rosszindulatú harmadik fél jogosulatlanul hozzáfért a Transavia Airlines C.V. rendszereihez (az azokban található személyes adatokhoz), ami adatvédelmi incidenshez vezetett. A kár korlátozása és a történtek feltárása érdekében a Transavia külső szolgáltatót bízott meg.

A támadónak egy olyan automatizált módszerrel, amelyben gyakran használt jelszavakat próbál ki rövid idő alatt („jelszóspray”), valamint korábbi, harmadik fél által elkövetett adatvédelmi incidensekből ismert felhasználói adatok

[477] DPC Case Reference: IN-19-7-4, https://www.dataprotection.ie/sites/default/files/uploads/2021-02/17.12.2020_Decision_IN-19-7-4_UniversityCollegeDublin.pdf, utolsó letöltés 2022. 07. 31.

felhasználásával („credential stuffing”) sikerült behatolnia a Transavia rendszereibe.

A jogosulatlan hozzáféréshez használt felhasználói fiók a legmagasabb jogosultságokkal rendelkezett a rendszer egyes tartományaiban, és a Transavia HR-rendszere és az Active Directory közötti összekötő kapocsként használták. Ez lehetővé tette a támadó számára a rendszerek feltárását és célzott megközelítést:

- ✓ *egyes rendszereken a nyomok eltávolítása érdekében törölte a naplófájlokat;*
- ✓ *behatolásteszt segítségével sebezhetőségeket talált a Transavia informatikai rendszerében;*
- ✓ *hálózati dokumentációt, üzleti és egyéb különféle dokumentumokat, valamint hat postafiókot másolt.*

Az adatvédelmi incidens hatása:

a) *érintettek: utasok, alkalmazottak, beszállítók és álláskeresők. Az esettel kapcsolatban készült szakértői jelentés szerint az incidens körülbelül 80 ezer utast, körülbelül 3 ezer alkalmazottat, kétszáz beszállítót és tíz álláskeresőt érintett.*

b) *érzékeny adatok: SSR-kódok („Special Service Request”) használatával a Transavia igyekszik szolgáltatásait az utasok igényeihez igazítani. Ezekből a kódokból közvetett módon érzékeny/különleges személyes adatok (egészségügyi adatok) származtathatók (pl. kerekesszéket használó, vak vagy siket). A szakértői jelentés szerint 367 személy egészségügyi adatai kerültek kiszivárogtatásra.*

A Transavia a GDPR 34. cikkében meghatározottaknak eleget téve összesen 81 ezer érintettet azonosított és értesített, mivel ezen érintettek jogaira és szabadságaira nézve magas kockázat állhatott fenn.

Az adatvédelmi hatóság vizsgálata szerint a Transavia nem hozott megfelelő technikai és szervezési intézkedéseket:

- ✓ *az alkalmazott jelszavak gyengék voltak. Volt ugyan irányelv a jelszavakra, de a támadásban használt általános fiókok jelszavai nem feleltek meg az előírt követelményeknek. Ennek oka a Transavia téves kockázatértékelése volt, miszerint a felhasználói fiókok esetében nagyobb az esélye egy sikeres jelszóspray-támadásnak vagy hitelesítő adatokkal való feltöltést célzó támadásnak, mint az általános fiókok esetében.*
- ✓ *nem volt jól megvalósítva a többfaktoros hitelesítés (MFA), a CITRIX-környezethez MFA nélkül is hozzá lehetett férni. A kockázatértékelés alapján a Transavia úgy döntött, hogy az MFA bevezetését fokozatosan hajtja végre, azaz először csak a felhasználói fiókoknál, később pedig az általános fiókoknál vezeti be. Ennek eredményeképpen a többfaktoros hitelesítést az általános fiókok esetében még nem vezették be, amikor az adatvédelmi incidens bekövetkezett.*
- ✓ *hiányzott a hálózati szegmentáció. A hálózati szegmentálással a felhasználók csak a számukra szükséges szegmensekhez kapnak hozzáférést, ez pedig drasztikusan csökkenti az illetéktelen hozzáférés esélyét.*

- ✓ *bizonyos naplófájlokat eltávolítottak, ami jelentősen megnehezítette, hogy a bekövetkezett adatvédelmi incidensről teljes képet lehessen utólag alkotni. Bár a Transavia egy külső, IT-biztonságra szakosodott céggel dolgozott együtt, amely – többek között – azért tudta nyomon követni a gyanús viselkedést, mert a tevékenységeket naplózták, bizonyos kritikus naplózási műveleteket nem hajtottak végre, illetve egyes naplófájlokat el is lehetett távolítani.*

Az adatvédelmi hatóság véleménye szerint minél szélesebb körű az adatok kezelése és minél érzékenyebbek ezek az adatok, annál nagyobbak az adatbiztonsággal szemben támasztott követelmények. A Transavia esetében kb. 25 millió utas adatait tartalmazó rendszerekhez férhetett hozzá a támadó, ráadásul ezen adatok egy része egészségügyi adat. A hatóság arra a következtetésre jutott, hogy az érintettek jogaira és szabadságaira jelentett különböző valószínűségű és súlyosságú kockázat ezen incidens esetében különösen magas, mivel a személyes adatok rosszindulatú felhasználása az érintettek számára jelentős anyagi és nem anyagi kárt okozhatott volna.
A hatóság 400 ezer euró közigazgatási bírságot szabott ki a Transavia Airlinesra.[478]

Bizonyos körülmények között mentesülhetünk az érintettek tájékoztatásának kötelezettsége alól, például, ha olyan technikai és szervezési védelmi intézkedéseket hajtottunk végre, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat.

Példa

- ✓ *nem kell értesítenünk a hatóságot, ha olyan telefont vagy laptopot loptak el a cégünktől (munkavállalónktól), amely bár tartalmazott személyes adatokat, ám olyan titkosítással volt védve, amely nem törhető fel. Az incidenst ebben az esetben is nyilvántartásba kell vennünk és folyamatosan nyomon kell követnünk az eseményeket. Amennyiben a későbbiekben olyan körülmények jutnak a tudomásunkra, amely az érintettek jogaira és szabadságaira nézve kockázatot jelent (például mégis csak feltörhető az általunk feltörhetetlennek ismert védelmi rendszer), meg kell tennünk a szükséges intézkedéseket (hatósághoz bejelentés, érintettek értesítése stb.)*

Mentesülhetünk az érintettek tájékoztatásának kötelezettsége alól, ha az adatvédelmi incidenst követően olyan intézkedéseket tettünk, amelyek biztosítják, hogy az érintettek jogaira és szabadságaira jelentett veszély a továbbiakban ne valósuljon meg.

[478] AP (The Netherlands) – Transavia Airlines C.V. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_transavia.pdf, utolsó letöltés: 2022. 07. 31.

Példa

- ✓ *szervezetünk által használt jelszó kompromittálódott, ám még a jogosulatlan használat előtt meg tudtuk azt változtatni;*
- ✓ *az ellopott készüléken lévő adatokat még annak feltörése előtt távoli hozzáféréssel visszaállíthatatlanul le tudtuk törölni (és volt biztonsági másolatunk)*

Kockázatminimalizálási technikák

Adatkezelőként különféle megoldásokhoz folyamodhatunk annak érdekében, hogy csökkentsük az adatkezeléseinkkel járó kockázatokat, ilyen lehet például:

- ✓ az álnevesítés;
- ✓ az anonimizálás;
- ✓ a titkosítás; és a
- ✓ szabályzatok, protokollok.

Az EDPB kiadott egy iránymutatást,[479] amely segítséget tud nyújtani az adatvédelmi incidens kezeléséhez, felügyeleti hatósághoz bejelentéséhez, az érintettek értesítéséhez, illetve a korrekciós intézkedések kiválasztásához és megtételéhez.

Álnevesítés

Az adatkezelők egyik leggyakoribb hibája, hogy összekeverik az álnevesítést és az anonimizálást, ami igen súlyos hibának számít, mivel az anonimizált adatokkal ellentétben az álnevesített személyes adatokra a GDPR szabályai továbbra is vonatkoznak:

- ✓ az anonimizálás azt jelenti, hogy az egyének nem azonosíthatók, és nem azonosíthatók újra semmilyen észszerűen felhasználható eszközzel, azaz az újraazonosítás kockázata kellően alacsony. Az anonim adat nem személyes adat.
- ✓ az álnevesítés azt jelenti, hogy az egyének nem azonosíthatók magából az adatkészletből, de más, külön tárolt információkra való hivatkozással azonosíthatók. Az álnevesített adatok személyes adatok, például az eredeti adatok egy algoritmus segítségével visszaállíthatóak, és a „helyreállított" adatok alapján a személyek egyértelműen azonosíthatóak.

Milyen előnyei lehetnek az álnevesítésnek?

- ✓ *jobban meg tudunk felelni a célhoz kötöttség elvének;*
- ✓ *jelentősen csökkenteni tudjuk az érintetteket érő kockázatokat;*
- ✓ *könnyebb megvalósítanunk a beépített adatvédelem elvárásait;*
- ✓ *az álnevesítés egyben biztonsági intézkedés is (például jelentősen csökkentheti az adatvédelmi incidens esetén az érintettek jogait és szabadságait érő kockázatokat amennyiben a fordítókulcs nem kompromittálódik);*

[479] Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, Adopted on 14 December 2021 Version 2.0. https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf, utolsó letöltés 2022. 08. 20.

- ✓ *az érintettek bizonyos adatkezelésekben szívesebben vesznek részt, ha nem a saját nevükön (mindenki által azonosíthatóan) hanem álnevet megadva jelentkezhetnek (például marketing célú nyereményjáték nyerteseinek nyilvánosságra hozatala stb.).*

Hogyan tudunk álnevesíteni?

A kezelésünkben lévő személyes adataink olyan jellemzőket tartalmaznak, amelyek alkalmasak arra, hogy azonosítsák az adatkezelésünkben érintett természetes személyeket (például név, lakcím stb.), az álnevesítés során ezeket a jellemzőket cseréljük ki álnevekre.

Példa

- ✓ *amennyiben (ipari) kémkedés szempontjából kulcsembereinket nem a születési nevükön tartjuk nyilván, hanem álneveken, akkor ezzel biztosítjuk, hogy a valódi neveket csak a fordítókulcshoz hozzáférő személyek ismerhetik meg, ezzel minimalizálva a nagyon érzékeny és különösen fontos személyes adatok kompromittálódásának kockázatát. Vajon hányan tudják, mi James Bond valódi neve?*
- ✓ *klubtagjaink azonosító számot kapnak, majd a későbbiekben bármilyen listát is készítünk (rendezvényen részt vevők, tagdíjat be nem fizetők stb.), azokon mindig csak ez az azonosító szám szerepel, nem pedig a nevük;*
- ✓ *amennyiben gyermekek számára rendezünk matematika (vagy bármilyen más versenyt), nem biztos, hogy minden szülő szeretné a neten látni, hogy a gyermeke milyen eredményt ért el (utolsónak is kell lenni valakinek). Amennyiben lehetővé tesszük, hogy a gyerekek (illetve a szüleik) a nevezés során álnevet adhassanak meg, ezzel kiiktathatjuk ezt a problémát, a szülők pedig bármikor feloldhatják az álnevesítést és kérhetik azt, hogy a gyermekük a valódi nevén szerepeljen a dicsőséglistában.*

Az álnevesítés esetén tehát a személyes adatokat olyan módon kezeljük, amelynek következtében további információk (például „fordítókulcs") felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tároljuk és technikai, valamint szervezési intézkedések megtételével biztosítjuk, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet hozzákapcsolni. Ilyen intézkedés például az, amikor a fordítókulcsot elszeparálva tároljuk egy olyan biztonsági zónában, amelyet csak korlátozott számú személy tud kinyitni a szervezetünk berkein belül.

Az olasz adatvédelmi hatóság (Garante) gyakorlatából

A Garante engedélyezte az Istat számára a népszámláláshoz szükséges személyes adatok kezelését, kiemelve a problémákat és utasításokat adva azok megoldása érdekében. A Garante szerint az Istat által azon javasolt eljárás, amely minden egyes természetes személyhez egyedi kód hozzárendelésén alapul, és amelyet az intézmény valamennyi adatbázisára és az adatmegőrzési időszakra (akár 120 évre) is alkalmazhat, kockázatos, mivel a népszámlálás célja szempontjából irreleváns és felesleges adatok feldolgozására kerülhet sor.

A Garante előírta az Istatnak, hogy

- ✓ *alkalmazzon álnevesítési intézkedéseket, például a kódok hierarchikus szétválasztásának rendszerét különböző álneves kódok hozzárendelésével, amelyek mindegyike a céltól függően korlátozott érvényességgel rendelkezik;*
- ✓ *az általános népszámlálási tervbe bele kell foglalni a népszámlálás során gyűjtött információknak az önkormányzatokhoz összesített formában történő átadására szolgáló módszerek megjelölését;*
- ✓ *az állandó népszámlálás létrehozásával kapcsolatos statisztikai munkákhoz kapcsolódó személyes adatok védelmére vonatkozó hatásvizsgálatot integrálni kell az érdekelt felek újbóli azonosításának valószínűségére vonatkozó, konkrét mérőszámok segítségével történő jelzéssel;*
- ✓ *a határozat közlésétől számított 120 napon belül közölje az Istat, hogy milyen kezdeményezéseket tett vagy szándékozik tenni a határozatban megjelölt előírások végrehajtása érdekében, különösen az álnevesítés technikái tekintetében; a visszajelzés elmaradása a közigazgatási bírság alkalmazását vonhatja maga után.*[480]

A német bírósági gyakorlatból

A megfelelő technikai és szervezési biztosítékok – például az álnevesítés – alkalmazásának kérdése csak akkor merül fel, ha előbb az adatkezelő megerősíti az adatkezelési művelet szükségességét és megállapítja, hogy nem áll fenn összeütközés az érintett védendő érdekeivel.[481]

Anonimizálás

„a személyazonosításra alkalmatlan adat nem áll a személyes adatok védelméhez való jog illetve az információs önrendelkezési jog védelme alatt, s mivel „személytelen", ezért az alapjogvédelem körén kívül esik általában is (bármilyen individuális jogról is van szó). Mivel az anonimizált adatok esetén nem állapítható meg az alapjog védendő alanya, ezért sem az információs önrendelkezéshez való joggal, sem más alapjoggal nem hozhatók összefüggésbe (...)"[482]

Az anonimizálás során a személyes adatállományokból úgy szűrjük ki az összes azonosító elemet, hogy az érintettek többé ne legyenek azonosíthatóak – azaz az adatok anonimizálása után nem maradhat olyan elem az információban, amely a továbbiakban – észszerű erőfeszítés mellett – lehetővé tehetné az érintettek azonosítását.

[480] Provvedimento del 23 gennaio 2020 [9261093], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9261093, utolsó letöltés 2022. 08. 01.
[481] 10 Sa 2130/19, https://gesetze.berlin.de/bsbe/document/JURE200011045, utolsó letöltés: 2022. 08. 01.
[482] 67/2011. (VIII. 31.) AB határozat, https://net.jogtar.hu/jogszabaly?docid=A11H0067.AB&txtreferer=99700047.TV, utolsó letöltés 2022. 08. 27.

Az anonimizálás előnyei:

- ✓ *korlátozza az adatvédelmi kockázatainkat (például adatvédelmi incidens lehetősége, érintettek jogainak és szabadságainak sérelme stb.);*
- ✓ *csökkenti a hírnevünk sérülését okozó kockázatokat;*
- ✓ *lehetővé teheti, hogy a rendelkezésünkre álló információt más szervezetek vagy a nyilvánosság számára hozzáférhetővé tegyük akár ellenérték fejében is;*
- ✓ *támogatja az adatminimalizálás és a célhoz kötöttség elvét, valamint jobban meg tudunk felelni a beépített adatvédelem követelményeinek;*
- ✓ *általában könnyebb anonim információkat megosztanunk, illetve közzé tennünk, mint a személyes adatokat, mivel kevesebb jogi korlátozás vonatkozik rájuk.*

Adatkezelőként nem szabad elfelejtenünk, hogy az anonimizálás első lépéseként mindig – szükségszerűen – van személyes adat a kezelésünkben.

Az anonimizálás legnagyobb kockázata az érintettek újra azonosíthatósága.

„Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell. (…) Valamely természetes személy azonosíthatóságának meghatározásakor minden olyan módszert figyelembe kell venni – ideértve például a megjelölést –, amelyről észszerűen feltételezhető, hogy az adatkezelő vagy más személy a természetes személy közvetlen vagy közvetett azonosítására felhasználhatja. Annak meghatározásakor, hogy mely eszközökről feltételezhető észszerűen, hogy egy adott természetes személy azonosítására fogják felhasználni, az összes objektív tényezőt figyelembe kell venni, így például az azonosítás költségeit és időigényét, számításba véve az adatkezeléskor rendelkezésre álló technológiákat, és a technológia fejlődését. Az adatvédelem elveit ennek megfelelően az anonim információkra nem kell alkalmazni, nevezetesen olyan információkra, amelyek nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható.”[483]

Az újbóli azonosítás kockázatát úgy tudjuk felmérni, ha figyelembe vesszük az ehhez szükséges időt, erőfeszítést, illetve erőforrást figyelemmel az adatok jellegére, felhasználásuk összefüggéseire, az újbóli azonosításhoz rendelkezésre álló technológiákra és a kapcsolódó költségekre.

[483] GDRP (26) preambulumbekezdés

Mikor lehet szükségünk anonim adatokra? Például

- ✓ *jogszabály kötelez minket anonim információk közzétételére, például pályázatok eredményének kihirdetése stb.;*
- ✓ *az adatokat új és innovatív módon kívánjuk felhasználni, például szolgáltatásunk minőségét akarjuk javítani, új terméket tervezünk stb.;*
- ✓ *mesterséges intelligencia tanítására kívánjuk felhasználni az adatokat;*
- ✓ *információszabadsággal kapcsolatos kérelmeket kell teljesítenünk;*
- ✓ *tevékenységünket átláthatóbbá kívánjuk tenni;*
- ✓ *kutatási vagy statisztikai célokra használunk fel adatokat;*
- ✓ *meg kívánjuk osztani az általunk gyűjtött adatokat szélesebb körű társadalmi előnyök elérése érdekében (például geolokációs adatokat) stb.*

Az adatokat akkor tekinthetjük ténylegesen anonimizáltnak, ha:

- ✓ nem vonatkoznak azonosított vagy azonosítható személyre, vagy
- ✓ olyan módon anonimizáltuk azokat, hogy az egyének nem, vagy már nem azonosíthatóak.

A dán adatvédelmi hatóság (Datatilsynet) gyakorlatából

A dán adatvédelmi hatóság megrovásban részesítette a dán pénzügyi felügyeleti hatóságot (FSA), amiért az megsértette a GDPR 32. cikkének (1) bekezdését, amikor a visszaélésbejelentőkről szóló információkat továbbította egy újságírónak. A hatóság megállapítása szerint az FSA nem hozott megfelelő szervezeti és technikai intézkedéseket az adatkezeléssel járó kockázatoknak megfelelő biztonsági szint biztosítása érdekében.

A közzététel egy nem megfelelő anonimizálási technika miatt történt, amikor e-mail címek még mindig felfedhetők voltak a szerkesztett pdf dokumentumokban.

Az FSA egy újságírótól kapott kérelmet a visszaélésbejelentő rendszerén keresztül gyűjtött információkkal kapcsolatban. Az FSA eleget tett a kérelemnek, miután eltávolította a bejelentő személyekre vonatkozó azonosítható személyes adatokat. Ezt követően az egyik bejelentő panaszt tett az FSA-nál, hogy az újságíró e-mailben felvette vele a kapcsolatot. Az FSA kivizsgálta az ügyet és kiderült, hogy egy szoftverfunkciónak köszönhetően lehetséges volt a pdf-ben befeketített részek eltávolítása és az FSA szándékai szerint anonimizált információk visszaállítása.

Az adatvédelmi hatóság álláspontja szerint

- ✓ *a visszaélésbejelentő rendszeren keresztül kapott információk esetében megfelelő biztonsági intézkedésnek biztosítania kell, hogy az újságírónak továbbított anyag ne tartalmazzon olyan személyes adatokat, amelyek felfedhetik a bejelentők személyazonosságát. Az FSA-nak olyan anonimizálási módszert kellett volna választania, amely nem hagy nyomot az eltávolított személyes adatokról még a metaadatokban sem, és amelynek eredményeképpen szabványosított eszközökkel nem lehet könnyen megkerülni a törlést.*
- ✓ *az FSA belső irányelvei nem voltak elég világosak és pontosak ahhoz, hogy az ügyintézők megfelelően tudják anonimizálni a személyes adatokat.*
- ✓ *a munkatársak képzése nem volt megfelelő;*

- ✓ *az FSA nem rendelkezett a szükséges ismeretekkel arról, hogy milyen módszereket kell alkalmaznia az információknak a dokumentumokból való eltávolítására, beleértve a metaadatokat is annak érdekében, hogy az információk többé ne legyenek visszaállíthatóak.* [484]

Az anonimizált adatok nem tartoznak a GDPR hatálya alá, ám attól még más jogszabályok vonatkozhatnak rájuk (például az ePrivacy irányelv), illetve, ha rossz módszerrel anonimizáltunk csak hisszük, hogy az adott adatokra már nem vonatkozik a GDPR, miközben igen.

Nem szabad azonban hátradőlnünk, anonimizáltunk, tehát nincs további teendőnk, ugyanis minden alkalommal, amikor az érintett abból a célból, hogy gyakorolja az adathozzáféréshez, helyesbítéshez, törléshez, az adatkezelés korlátozásához és/vagy az adatok hordozhatóságához való jogát és számunkra az azonosítását lehetővé tevő kiegészítő információt nyújt, a korábban már anonimizált adatok újból személyes adatokká válhatnak.

Fontos

- ✓ *azért, mert titkosítunk egy adatot, attól az még nem lesz anonim;*
- ✓ *az anonimizálás nem jelenti egyben azt is, hogy az adat használhatatlanná (értéktelenné válik);*
- ✓ *nem minden adatot lehet anonimizálni, illetve az anonimizálást nem lehet minden esetben automatizálni (ilyen például a klasszikus fekete csíkkal kitakart szöveg megoldás);*
- ✓ *azért, mert más szervezetnél bevált egy anonimizálási eljárás még nem biztos, hogy nálunk is bevált;*
- ✓ *a rendelkezésre álló technológiák fejlődése az anonimizált adatokat újra személyes adatokká varázsolhatja (az anonimizálás nem szünteti meg az érintettek jogait és szabadságait érintő kockázatokat csak jelentősen csökkenti azokat);*
- ✓ *az újraazonosított adatok komoly problémákat okozhatnak mind nekünk (adatkezelőnek), mind az érintetteknek (adatvédelmi incidens stb.);*
- ✓ *a Big Data és a mesterséges intelligencia használata új lehetőségeket nyit az újraazonosítás terén.*

Az azonosíthatóság kockázata

Az anonimizálás relatív – ugyanaz az információ lehet személyes adat a mi számunkra, míg egy másik adatkezelő kezében ugyanez az információ anonim információ. Az, hogy egy adott információ anonim-e, nagyban függ a körülményektől, például a nyilvánosságra hozatal helyétől, módjától és a befogadók ismereteitől.

Azt, hogy egy adott információ anonim-e, úgy kell eldöntenünk, hogy figyelembe kell vennünk minden olyan eszközt, amelyet akár mi, akár egy harmadik fél észszerűen valószínűsíthetően felhasználhat azon személynek az azonosítására, akire az adott

[484] Journalnummer: 2020-442-8099, https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/apr/datatilsynet-udtaler-alvorlig-kritik-af-finanstilsynets-behandling-af-personoplysninger, 2022. 08. 01.

információ vonatkozik („észszerűen valószínű" teszt). Mit érdemes figyelembe vennünk?

Célszerű számba vennünk minden objektív tényezőt:

- ✓ ha vannak olyan eszközök, amelyek „észszerűen valószínűsíthetően" alkalmasak egy személy azonosítására, akkor az információt személyes adatnak kell tekintenünk,
- ✓ ha pedig „észszerűen valószínűsíthetően" nem használnak ilyen eszközt, akkor az információt ténylegesen anonimizáltnak tekinthetjük; az azonosíthatóság kockázatának azonban az adatkezeléssel való összefüggésében kellően távolinak kell lennie.

Az Európai Adatvédelmi Biztos (EDPS) példái a nem megfelelő anonimizálásra

„2006-ban (...) egy filmstreaming-szolgáltatás közzétett egy adathalmazt, amely 500 ezer ügyfél 10 millió filmes rangsorolását tartalmazta, azt állítva, hogy az anonim, de később kiderült, hogy egy ellenséges félnek elég volt egy kis ismeret az előfizetőről ahhoz, hogy azonosítani tudja az előfizető bejegyzését az adathalmazban. Egy másik példa a hiányos anonimizálásra: 2013-ban a New York-i Taxi és Limuzin Bizottság közzétett egy adatlapot, amely több mint 173 millió egyéni taxifuvarról tartalmazta a be- és kiszállás helyét, időpontját és az állítólag anonimizált engedélyszámokat. Az adatállományt nem megfelelően anonimizálták, és az eredeti engedélyszámokat, sőt, még a taxik egyes sofőrjeit is azonosítani lehetett."[485]

A körülmények azonban változnak, különösen igaz ez az egyének azonosítására rendelkezésre álló eszközök megvalósíthatóságára és költséghatékonyságára. Elmondhatjuk, általában minél megvalósíthatóbbá és költséghatékonyabbá válik egy módszer, annál valószínűbb, hogy észszerűen használható eszköz lesz. Ráadásul ezen eszközök észszerűvé minősítése függ attól, mennyire értékes az adott információ – amennyiben például közszereplőről van szó, valószínűleg lesznek olyanok, akik hajlandóak többet is áldozni az anonimizálás visszafordítására.

Célszerű már az anonimizálási folyamatunk legkorábbi szakaszában mérlegelnünk az észszerűen valószínűsíthetően használt eszközöket, különösen a nyilvánosságra hozás (meghatározott csoportok számára történő közzététel) esetén. Az azonosíthatóság értékelésénél minden esetben figyelembe kell vennünk:

- ✓ létezik-e olyan kiegészítő információ, amely lehetővé teszi az azonosítást;
- ✓ vannak-e olyan technikák, amelyek lehetővé teszik az azonosítást a szóban forgó információk alapján; és
- ✓ milyen mértékben valószínű, hogy a kiegészítő információk, illetve technikák észszerűen hozzáférhetők és felhasználhatók az eredeti információ érintettjének azonosítására.

[485] 10 MISUNDERSTANDINGS RELATED TO ANONYMISATION, https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf, utolsó letöltés: 2022. 09. 03.

A spanyol adatvédelmi hatóság (AEPD) gyakorlatából

2018. december 12-én a VOX spanyol politikai párt weboldalát kibertámadás érte, amelyben érintett volt a párt hírlevelére feliratkozók adatbázisa is. A mintegy 30 ezer feliratkozó nevét és vezetéknevét a későbbiekben egy Twitter-fiókban részben anonimizált módon tették közzé. Az AEPD megrovásban részesített a VOX-ot a biztonsági intézkedésekkel kapcsolatos gondatlansága miatt.

Ezen túlmenően az AEPD úgy vélte, hogy a kiszivárgott adatok nem tekinthetők a személyes adatok különleges kategóriájába tartozó adatoknak. Megállapította azonban, hogy a kiszivárgott adatok és az internetes kereséses eredmények kombinációja olyan politikai nézet nyilvánosságra hozatalát eredményezheti, amelyhez az érintett nem járult hozzá. Ez lehetőség olyan kockázatra, amelyet az adatkezelőnek értékelnie kell, amikor ilyen jellemzőkkel rendelkező adatokat kezel, és a védelmi szintjét ezen értékelés eredménye alapján szükséges növelnie.[486]

Az azonosíthatóság kockázatát növeli az, ha:

- ✓ az anonimizált adatok nyilvánosan elférhető információkkal kombinálva az érintett újra azonosíthatóvá válik, vagy
- ✓ statisztikai módszerekkel a különböző információkat úgy össze lehet kapcsolni, hogy az érintett újra azonosítható válik, vagy
- ✓ motivált illetéktelen személy várhatóan kísérletet tesz az újra azonosításra.

Ki számít motivált illetéktelen személynek? Az, akit előzetes ismeretek nélkül azonosítani kíván egy olyan személyt, akinek a személyes adataiból az anonim információ származik. Azonban minél értékesebb információk vannak a birtokunkban, annál motiváltabb illetéktelen személyekkel kell számolnunk, olyanokkal, akik drágább, fejlettebb eszközöket is tudnak alkalmazni, valamint adott esetben bűncselekmény elkövetésére is hajlandóak.

A magyar adatvédelmi hatóság (NAIH) gyakorlata

„A Kérelmezett anonimizálási/törlési módszertanának, továbbá az általa alkalmazott banki rendszerek nevének közzétételét sem az általános adatvédelmi rendelet, sem az ágazati jogszabályok nem írják elő, ezért emiatt a Kérelmezett ezt a saját döntése alapján üzletei titokként kezelheti (…)”[487]

A NAIH anonimizálási útmutatója[488] a buktatókat bemutatva nyújt segítséget abban, hogy – szükség esetén – mind az információszabadság (közérdekből nyilvános adatokkal kapcsolatos szabályok), mind a GDPR elvárásainak képesek legyünk megfelelni.

[486] Procedimiento Nº: PS/00254/2019, https://www.aepd.es/es/documento/ps-00254-2019.pdf, utolsó letöltés: 2022. 09. 04.
[487] NAIH-3145-5/2021
[488] NAIH-1938-2/2013/T. https://naih.hu/files/2014_02_03_anonimizalas_gyak_utm.pdf, utolsó letöltés: 2022. 08. 01.

„1. tanács: az anonimizált kivonat elkészítése nem pusztán ügyviteli feladat. Az adatkezelőnek felelősségteljes döntést kell hoznia arról, hogy melyek a védendő adatok, amelyeket a kivonat nem tartalmazhat. A védendő adatok meghatározására csak olyasvalaki alkalmas, aki jól ismeri a kivonat alapjául szolgáló irat tartalmát, valamint az iratban lévő adatok védelmére, illetve nyilvánosságára vonatkozó jogszabályi előírásokat.

2. tanács: a kivonat készítése során csak a törvény alapján védendő információkat szabad a szövegből törölni. Az adatkezelő nem zárhat el önkényesen olyan információkat a nyilvánosság elől, amelyek bizalmaságát, védelmét jogszabály nem írja elő.
3. tanács: a kivonatot úgy kell elkészíteni, hogy a szöveg belső összefüggései lehetőleg fennmaradjanak, mert egyébként az eredmény használhatatlan szóhalmaz lesz. A bemutatott szöveg elektronikus formában rendelkezésre áll, anonimizálása helyesen úgy történhet, hogy a szereplők azonosító adatait pszeudonim kódokra cserélik.

4. tanács: Egyértelműen jelezni kell, hogy honnan töröltek adatot, mert a védett adat észrevétlen, nyomtalan törlése éppúgy meghamisíthatja a szöveg értelmét, mint egy adat meghamisítása, vagy valótlan adat betoldása.

5. tanács: a szöveg arányai is információt hordoznak. A kivonat felhasználói nem jogosultak a védett adatokat megismerni, azonban az nem titkolható el előlük, hogy valahonnan egy szót, egy sort, egy bekezdést, vagy egy oldalt töröltek. Ezért törekedni kell arra, hogy a kivonat megőrizze az eredeti szöveg arányait.

6. tanács: Elektronikus közzététel esetén célszerű informatikus szakértővel előzetesen megvizsgáltatni, hogy tartalmaz-e az elektronikus dokumentum védett adatot nem megjelenített kísérőinformációként. Kétség esetén az is megoldás lehet, ha a kivonatot tartalmazó elektronikus dokumentumot kinyomtatják. Ha a kivonatra elektronikus formában van szükség, akkor a nemkívánatos kísérőinformációktól megtisztított, kinyomtatott lapok utólag beszkennelhetők.

7. tanács: a teljes és végleges adattörlést akár papír alapú iraton, akár elektronikus dokumentumban minden esetben úgy kell végrehajtani, hogy a kivonat még elfedve, vagy DRM segítségével hozzáférhetetlenné téve se tartalmazza a védett adatokat."[489]

Az újraazonosítás kockázata

Lehet olyan illetéktelen személy („támadó"), aki – akár úgy is, hogy nincs előzetes ismerete – be kívánja azonosítani azt a személyt, akinek a személyes adataiból származtattuk anonim információkat. Adatkezelőként a mi feladatunk annak vizsgálata, vajon ez a „támadó" sikerrel járhat-e. Mit kell ilyenkor feltételeznünk? Többek között azt, hogy

[489] NAIH-1938-2/2013/T. https://naih.hu/files/2014_02_03_anonimizalas_gyak_utm.pdf, utolsó letöltés: 2022. 08. 01.

- ✓ valamiért akarja az újraazonosítást (van motivációja, például anyagi haszonszerzés, szakmai dicsőség, oknyomozás stb.);
- ✓ valamilyen szinten ért ahhoz, amit tenni akar (de nincsenek mélyreható ismeretei);
- ✓ hozzáfér megfelelő erőforrásokhoz és használja is azokat (pl. internet, nyilvános dokumentumok stb.), ám nem fér hozzá speciális eszközhöz;
- ✓ akár alapvető nyomozati technikákat is képes alkalmazni (pl. HUMINT stb.), de bűncselekmény elkövetésére azért nem szánja el magát annak érdekében, hogy hozzáférjen a biztonságosan tárolt adatokhoz (pl. betörés);
- ✓ a végeredményt pedig valamilyen módon fel kívánja használni, azaz a tevékenysége mindenképpen kockázatot jelent számunkra.

„Tizenöt hónapnyi mobilitási adatot vizsgáltunk másfél millió személyről, és azt találtuk, hogy az emberi mobilitás nyomai rendkívül egyediek. Valójában egy olyan adathalmazban, ahol az egyén helyét óránként határozzák meg, és ahol a térbeli felbontás megegyezik a szolgáltató antennáinak felbontásával, négy tér-időbeli pont elegendő az egyének 95%-ának egyedi azonosításához.(…)

Az egyszerűen anonimizált adatkészlet nem tartalmaz nevet, lakcímet, telefonszámot vagy más nyilvánvaló azonosítót. Ha azonban az egyén mintái elég egyediek, a külső információk felhasználhatók az adatok egyénhez való visszakapcsolására. Egy tanulmányban például egy orvosi adatbázist sikeresen kombináltak egy választói listával, hogy kiderítsék Massachusetts állam kormányzójának egészségügyi adatait. Egy másikban a felhasználók legfőbb tartózkodási helyének felhasználásával mobiltelefon-adatokat azonosítottak újra. Végül a Netflix adatállományának egy részét az Internet Movie Database külső információinak felhasználásával azonosították újra.”[490]

Ilyen motivált személy lehet például ipari kém, oknyomozó újságíró, zaklató, de akár féltékeny élettárs is – éppen a potenciális „támadók” sokfélesége és eltérő motivációi miatt lehet a valószínű „támadó” profilja nagyon eltérő:

- ✓ pénzügyi, illetve bizalmas adatoknál számolnunk kell a rutinosabb „támadóval”, olyan személlyel, aki jobban felszerelt technikai eszközökkel;
- ✓ állami szereplők nagyobb számítási teljesítményt, illetve szakértelmet tudnak bevonni a támadásba;
- ✓ olyan személy is lehet, akinek ugyan engedélyeztük a hozzáférést, de akár szándékosan, akár véletlenül azonosít egy vagy több személyt.

Az, hogy mennyire kell felkészülnünk az ilyen, újraazonosításra koncentráló támadásra függ attól, hogy

- ✓ milyen adatokat kezelünk (jelleg, mennyiség, típus stb.);
- ✓ annak a valószínűsége, hogy az újraazonosításra valakinek szüksége van (számára értékes az információ);

[490] Yves-Alexandre de Montjoye, Ce´sar A. Hidalgo, Michel Verleysen & Vincent D. Blondel: Unique in the Crowd: The privacy bounds of human mobility, SCIENTIFIC REPORTS | 3 : 1376 | DOI: 10.1038/srep01376, https://www.nature.com/articles/srep01376.pdf, utolsó letöltés: 2022. 08. 16.

- ✓ a várható támadó mennyire lesz képzett (az általunk kezelt anonimizált adatra egy elhagyott élettárs vagy egy harmadik ország titkosszolgálata kíváncsi) és milyen olyan előzetes információ birtokában lehet, amely segítheti az újraazonosítást;
- ✓ milyen már meglévő biztonsági intézkedéseink vannak, amelyek már eleve csökkenthetik a támadási kedvet.

Egyes adatkategóriák vonzhatják a támadókat (azaz ilyen esetekben fokozott figyelmet kell tanúsítanunk), például

- ✓ olyan személyes adatok, amelyeket fel lehet használni anyagi haszonszerzésre vagy más módon károkozásra (pl. rágalmazás stb.);
- ✓ az adatok bizonyos személyek megszégyenítésére, diszkriminációjára alkalmasak;
- ✓ az adatok közszereplőkkel vagy celebekkel kapcsolatosak;
- ✓ az adatok felhasználhatóak politikai kampányokban;
- ✓ az információ jelentős értékkel bírhat a bulvársajtó számára (kihez törtek be, kinek a rokonát gyilkolták meg stb.);
- ✓ az újraazonosítás a támadó kvalifikáltságát is jelenti egyben (jelentős szakmai kihívás az újraazonosítás).

Az újraazonosítás kockázatát növeli az is, hogy hogyan és mily módon hozzuk nyilvánosságra az adatokat – minél nagyobb a nyilvánosság, annál nagyobb a kockázat, illetve a széles közönség elé tárt adatok esetében a későbbiekben szinte lehetetlen azok visszahívása, ha kiderül, hogy nagyon nagy a visszaazonosítás kockázata. A legkörültekintőbben akkor járhatunk el, ha a kockázatértékelésünk során

- ✓ a nyilvános közzététel / adatkiadás esetén az újbóli azonosítás maximális kockázatát vesszük figyelembe az adatállomány összes eleme tekintetében, illetve
- ✓ nem nyilvános adatmegosztás esetén szerződéses kikötésekkel szabályozzuk az adatokhoz hozzáférést, a felhasználást és a megsemmisítést.

Titkosítás

A biztonság fenntartása és a GDPR rendelkezéseit sértő adatkezelés megelőzése érdekében értékelnünk kell az adatkezelés természetéből fakadó kockázatokat, és az e kockázatok csökkentésére szolgáló intézkedéseket, például titkosítást kell alkalmaznunk. Ezek az intézkedések biztosítják a megfelelő szintű biztonságot – ideértve a bizalmas kezelést is –, figyelembe véve a tudomány és a technológia állását, valamint a végrehajtás kockázatokkal és a védelmet igénylő személyes adatok jellegével összefüggő költségeit.

A dán adatvédelmi hatóság gyakorlatából

Az adatvédelmi hatóság megállapította, hogy a dán Igazságügyi Minisztérium egyik szerve megsértette a GDPR rendelkezéseit, mivel nem titkosította a személyes adatokat tartalmazó USB flash meghajtót, valamint az USB flash meghajtó elvesztését követően nem jelentette az adatvédelmi incidenst.

Az incidensben érintett szervezet feladata a jogállamiság alapelveinek biztosítása (például a bűncselekmények áldozatainak kártérítés nyújtásával, valamint az igazságszolgáltatáshoz való hozzáférés támogatásával) és munkájának jellegéből adódóan nagy mennyiségű, az eljárásban részt vevő felekre vonatkozó érzékeny és bizalmas információ kezelése.

A szervezet egy több mint 800 oldalnyi személyes adatot tartalmazó USB flash meghajtót küldött el egy érintett képviselőjének, az azonban ismeretlen körülmények között elveszett. Az USB flash meghajtó nem volt titkosítva, és a szervezetben az ügyintézők nem rendelkeztek semmilyen iránymutatással sem az eltávolítható tárolóeszközök és hordozható adathordozók kezelésére vonatkozóan. A szervezet nem jelentette az adatvédelmi incidenst a felügyeleti hatóságnak.

A hatóság megállapította, hogy

- ✓ *az eltávolítható tárolóeszközök (beleértve az USB flash meghajtókat) nagyobb kockázatot jelentenek az érintettekre, ugyanakkor a titkosítás viszonylag könnyen megvalósítható biztonsági intézkedés az adatkezelő számára, ezért a titkosítást szükséges és előírt biztonsági intézkedésnek kell tekinteni;*
- ✓ *amennyiben egy adatkezelő nagy mennyiségű érzékeny és bizalmas adatot kezel, az USB flash meghajtók használatára megfelelő iránymutatásokat kell biztosítani azok számára, akik azokat kezelik, ebben az esetben azonban az adatkezelőnek ilyenje nem volt;*
- ✓ *az adatvédelmi incidenst nem jelentette a szervezet, miután tudomást szerzett arról.* [491]

Megjegyzés: a Budapesti Rendőrfőkapitányság[492] *hasonló adatvédelmi incidensbe keveredett.*

A GDPR többször megemlíti a titkosítást (általában az álnevesítéssel együtt), így

- ✓ amennyiben például az adatgyűjtés céljától eltérő célból történő adatkezelés nem az érintett hozzájárulásán vagy valamely olyan uniós vagy tagállami jogon alapul, amely szükséges és arányos intézkedésnek minősül egy demokratikus társadalomban a 23. cikk (1) bekezdésében rögzített célok eléréséhez, annak megállapításához, hogy az eltérő célú adatkezelés összeegyeztethető-e azzal a céllal, amelyből a személyes adatokat eredetileg gyűjtöttük – többek között – figyelembe kell vennünk megfelelő garanciák meglétét is, ami jelenthet titkosítást vagy álnevesítést is.
- ✓ a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket kell végrehajtanunk annak érdekében, hogy a kockázat

[491] Civilstyrelsen indstilles til bøde, https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/maj/civilstyrelsen-indstilles-til-boede, utolsó letöltés: 2022. 08. 01.
[492] Lásd megtörtént adatvédelmi incidensek (melléklet, Budapesti Rendőrfőkapitányság adatvédelmi incidense)

mértékének megfelelő szintű adatbiztonságot garantáljuk, ideértve, többek között, adott esetben a személyes adatok álnevesítését és titkosítását is.

- ✓ amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, indokolatlan késedelem nélkül tájékoztatnunk kell az érintettet az adatvédelmi incidensről, kivéve ha megfelelő technikai és szervezési védelmi intézkedéseket hajtottunk végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmaztuk, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat.

A dán adatvédelmi hatóság gyakorlatából

A hatóság megrovásban részesített egy önkormányzatot, amiért az nem használ végponttól végpontig terjedő titkosítást az e-mailben küldött érzékeny tartalmak esetében, valamint a protokoll jól ismert biztonsági hibái ellenére továbbra is a TLS 1.1-et használta.

Egy önkormányzat – emberi hiba miatt – a tartalom megfelelő titkosítása nélkül küldte el egy tanácsadó ügynökségnek a 12.916 állami iskolába járó gyermek adatait.

A dán adatvédelmi hatóság megállapította, hogy

- ✓ *nem rendelkezett elegendő bizonyítékkal annak megállapításához, hogy a TLS 1.1-et használták a szállítási rétegben, amikor ezt a konkrét e-mailt elküldték a tanácsadó cégnek;*
- ✓ *a szállítási réteg titkosítása nem elegendő, ha az e-mail érzékeny jellegű, vagy különleges személyes adatokat tartalmaz; ilyen esetekben a végponttól végpontig terjedő titkosítás megfelelőbb biztonsági intézkedés;*
- ✓ *a TLS 1.1 jól ismert biztonsági problémákkal küzd, ezért a protokoll nem alkalmas a szállítási réteg titkosítására;*
- ✓ *az adatkezelő nem teljesítette a kockázatnak megfelelő biztonsági szintet biztosító technikai és szervezési intézkedések végrehajtására vonatkozó kötelezettségét.*[493]

A titkosítás hamis biztonságérzetet is kelthet bennünk – ha titkosak az adataink, azzal már egy hekker sem tud mit kezdeni, védve vagyunk, és ha adatvédelmi incidens történik, akkor sem kell aggódnunk, hiszen nem történik az érintettek jogai és szabadságai vonatkozásában olyan kockázat, amely miatt a felügyeleti hatóságot értesítenünk kellene.

Napjainkban azonban számos, széles körben elterjedt kulcskezelési gyakorlat sem elég biztonságos ahhoz, hogy maximálisan biztosak legyünk abban, ha az ily módon titkosított adatainkhoz illetéktelen személy hozzáfér, azokat nem tudja visszafejteni,

[493] Journalnummer: 2021-442-11601. https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/nov/foelsomme-oplysninger-i-ukrypteret-mail-fra-silkeborg-kommune, utolsó letöltés: 2022. 08. 01.

így megismerni és felhasználni sem. Az is előfordulhat, adatvédelmi incidens esetén, hogy szakértő vizsgálja meg a titkosítási rendszerünket és a bevezetett kulcskezelési gyakorlatainkat, és ő állapítja meg, hogy jogosan hivatkoztunk-e a titkosítási mentességre (azaz az adataink titkosak voltak, ezért nem jelentettük az incidenst), vagy visszaélés szerűen alkalmaztuk ezt a mentességet, mert valójában a titkosításunk mértéke messze nem felelt meg a hatóság által elvárt színvonalnak.

Szabályzatok, protokollok

„Az első: soha ne bízz az emberi tényezőben. Ez egy kicsit keménynek tűnhet, és hogy igazságosak legyünk, a legtöbb ember jót akar. De bárki, aki nyomon követi az informatikai híreket, tudja, hogy vannak fenyegetések és rossz szereplők. Tehát akár a játéktervezésről, akár a kiberbiztonságról van szó, az egyik kérdés, amit általában felteszek magamnak, az az, hogy „hogyan használnám ki vagy rombolnám le?".

A második a kudarcra való felkészülés. Valószínű, hogy a kudarc bekövetkezik. Az igazi trükk az, hogy a lehető legkevesebbre csökkentsük ezt a hatást, és készen álljunk a reagálásra. Ehhez pedig fel kell készülnünk arra, hogy amikor valami bekövetkezik, már rendelkezzünk tervekkel, ellenőrző listákkal, biztonsági mentésekkel és az izommemóriánkkal, hogy a lehető leggyorsabban enyhíthessük a helyzetet, és a szervezetet újra működésbe hozhassuk." [Sean (Spiceworks) játéktervező][494]

Kockázatunkat jelentősen csökkenthetjük azzal, ha megfelelő adminisztratív intézkedéseket hozunk annak érdekében, hogy mindenki tudja a szervezetünkben, mi is a dolga. Komoly rendszerszintű problémákat előzhetünk meg azzal, ha vannak jogszerű eljárásrendjeink és nemcsak kialakítottuk ezeket, hanem megismertettük az alkalmazottjainkkal és be is tartatjuk velük. Bármilyen szabályzat, protokoll csak annyit ér amennyit betartunk belőle – később, például egy adatvédelmi incidens vizsgálata során csak enyhe vígaszt jelenthet számunkra, hogy aki hibázott az akár jól, előírásoknak megfelelően is végezhette volna a munkáját és akkor nem történt volna meg a baj.

Milyen szabályzatok segíthetnek a kockázatok csökkentésében? Például azok, amelyek folyamatszinten szabályozzák a lépéseket:

- iratkezelési és selejtezési szabályzat (például a szervezetünkhöz érkező iratok iktatása, szervezeten belüli mozgása, irattározása, selejtezése, szervezeten kívülre iratok küldése stb.);
- adatvédelmi és adatbiztonsági szabályzat (például okmánymásolatok készítése, erkölcsi bizonyítványokkal kapcsolatos tennivalók, adatok tárolásának rendje, ellenőrzések szabályai, kötelező nyilvántartások használatának módja, tudnivalók a szabályos adattovábbításról stb.);

[494] What are your Five Laws of Cybersecurity?, Posted by Sean (Spiceworks) on Aug 2nd, 2022, https://community.spiceworks.com/topic/2458776-what-are-your-five-laws-of-cybersecurity, utolsó letöltés: 2022. 08. 29.

- információbiztonsági szabályzat (IT rendszerrel kapcsolatos követelmények, jogosultságmenedzsment, jelszóval kapcsolatos követelmények, internet és e-mail fiókok használata, IT védelem követelményei stb.);
- speciális szabályzatokban rögzített adatkezelési követelmények, például hozzáférési, tárolási, archiválási, másolatkészítési és megsemmisítési szabályok (kamera működtetésre, beléptetésre, munkára alkalmasság ellenőrzésére, biometrikus azonosításra stb. vonatkozó szabályzatok);
- „to do" listák, például
    - mit tegyünk akkor, ha a kapuban/portánkon megjelenik egy önmagát hatósági személynek állító valaki és személyes adatokat kér? Vagy ugyanezt teszi, csak nem személyesen, hanem telefonon?
    - szerződéskötés folyamatának szabályozása a szervezetünkön belül annak érdekében, hogy minden szempont (kereskedelmi, biztonsági, IT, adatvédelmi stb.) figyelembe legyen véve stb.

A dán adatvédelmi hatóság (Datatilsynet) gyakorlatából

A Datatilsynet megrovásban részesített egy nagy fogyasztási cikkeket forgalmazó kiskereskedőt, amiért nem alakított ki megfelelő hozzáférés-ellenőrzési gyakorlatot a vállalat alkalmazottjaira vonatkozó és a közös meghajtón tárolt személyes adatokhoz.

A Coop Danmark A/S („vállalat") egy új szkennelő tesztelése során szerzett tudomást arról, hogy a vállalat megosztott meghajtóján megfelelő hozzáférés-ellenőrzés nélkül személyes adatokat tárolt. Ezek az információk összesen 477 alkalmazottra és külső tanácsadóra vonatkoztak és – többek között – egészségügyi, pénzügyi és társadalombiztosítási adatokat tartalmaztak.

Az információk egy részét maguk az érintettek helyezték el a mappákban, míg más információkat az adatkezelő a foglalkoztatási folyamatok részeként mentett ide. A személyes adatok a 2013-tól 2017-ig tartó időszakra vonatkoztak, amikor még nem volt a vállalatnál a hozzáférés menedzsment tekintetében megfelelő szabályzás.
2021. június 12-én a vállalat adatvédelmi incidensről értesítette a felügyeleti hatóságot, három hónap elteltével pedig kezdeményezte az incidensben érintettek értesítését. Ezzel egyidejűleg a vállalat megkezdte az adatok áthelyezését egy biztonságosabb, jobb felhasználókezelést és naplózást biztosító tárhelyre (a vállalat megtisztította a fájlokat, és azokat egy olyan mappába helyezte át, ahol csak olyan munkavállalók fértek hozzá az információkhoz, akiknek erre a munkavégzésükkel kapcsolatban volt szükség).

A Datatilsynet véleménye szerint

- ✓ *a sok felhasználóra vonatkozó, nagy mennyiségű érzékeny információt tartalmazó rendszerek esetében az adatkezelőknek szigorúbb intézkedésekkel kell biztosítaniuk, hogy csak az arra jogosult személyek férjenek hozzá az adatokhoz.*
- ✓ *egy olyan méretű adatkezelőnek, mint a Coop Danmark A/S, már korábban is tisztában kellett volna lennie azzal, hogy az alkalmazottak tévesen*

személyes adatokat helyezhettek el a vállalat közös meghajtóján és megfelelő biztonsági intézkedéseket kellett volna bevezetnie. [495]

A kockázatok csökkentésére készítenünk kell olyan eljárásrendeket, amelyeknek az a célja, hogy a már megtörtént események kockázatát próbáljuk csökkenteni (adatvédelmi incidens esetén vizsgálóbizottság felállítása, a bizottság feladatai, reagálási terv készítése stb.).

GDPR

- ✓ Az álnevesítés fogalma [GDPR 4. cikk 5. pont]
- ✓ Az adatvédelmi incidens fogalma [GDPR 4. cikk 12. pont]
- ✓ Azonosítást nem igénylő adatkezelés [GDPR 11. cikk, (57) és (64) preambulumbekezdések]
- ✓ Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak [GDPR 33. cikk, (75), (85) és (87)-(88) preambulumbekezdések]
- ✓ Az érintett tájékoztatása az adatvédelmi incidensről [GDPR 34. cikk, (86)-(88) preambulumbekezdések]
- ✓ Adatvédelmi hatásvizsgálat [GDPR 35. cikk, (75), (84) és (89)-(93) preambulumbekezdések]
- ✓ Előzetes konzultáció [GDPR 36. cikk, (94)-(96) preambulumbekezdések]

Iránymutatások

- ✓ NAIH: Gyakorlati útmutató védett adatot nem tartalmazó kivonat készítéséhez[496]
- ✓ A 29. cikk alapján létrehozott adatvédelmi munkacsoport: Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e, WP 248 rev.01. Az elfogadás időpontja: 2017. április 4. A legutóbbi felülvizsgálat és elfogadás időpontja: 2017. október 4. https://naih.hu/files/WP248_rev01_hu.pdf
- ✓ A 29. cikk alapján létrehozott adatvédelmi munkacsoport: Iránymutatás az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről, WP250rev.01. Elfogadás időpontja: 2017. október 3. A legutóbbi felülvizsgálat és elfogadás időpontja: 2018. február 6. kedd, https://naih.hu/files/wp250rev01_hu.pdf

[495] Alvorlig kritik af Coop Danmark A/S' behandling af oplysninger på virksomhedens fællesdrev, https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/nov/alvorlig-kritik-af-coop-danmark-as%e2%80%99-behandling-af-oplysninger-paa-virksomhedens-faellesdrev-, utolsó letöltés 2022. 08. 29.
[496] NAIH-1938-2/2013/T. https://naih.hu/files/2014_02_03_anonimizalas_gyak_utm.pdf, utolsó letöltés: 2022. 08. 01.

ADATTOVÁBBÍTÁS (ADATMEGOSZTÁS)

A magyar Alkotmánybíróság gyakorlatából

„Az adattovábbítás szűkebb értelme az, hogy az adatot az adatfeldolgozó meghatározott harmadik személy számára hozzáférhetővé teszi. Az adat nyilvánosságra hozása azt jelenti, hogy az adatot bármely harmadik személy megismerheti. (…) Személyes adatot az érintetten és az eredeti adatfeldolgozón kívüli harmadik személy számára hozzáférhetővé tenni – s eszerint adatfeldolgozási rendszereket egymással összekapcsolni – csak akkor szabad, ha minden egyes adat vonatkozásában az adattovábbítást megengedő összes feltétel teljesült."[497]

Az adatvédelmi szabályok alapján adattovábbítás az, amikor harmadik személy számára hozzáférhetővé tesszük az adatot. Ez a harmadik személy bárki lehet, de nem lehet azonos

- ✓ az érintettel,
- ✓ az adatkezelővel,
- ✓ az adatfeldolgozóval,
- ✓ vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt személyes adatok kezelését végzik.

Példa

- ✓ *adatkezelőként egy másik adatkezelőnek adunk át adatot, ez adattovábbítás (például az alkalmazottakra csoportos biztosítást kötünk, és a kárrendezés érdekében átadunk a biztosítónak személyes adatokat);*
- ✓ *ha adatkezelőként a könyvelőnknek adjuk át az aktuális bevallásokhoz szükséges személyes adatokat, ez nem adattovábbítás;*
- ✓ *vállalatcsoportokon belüli adatátadások adattovábbításnak számítanak, hiszen jogilag elkülönült szervezetek között történik az adatmegosztás még akkor is, ha a cégháló anyája (tévesen) azt hiszi, hogy az összes lányával együtt ő egy és oszthatatlan.*

Az adattovábbítás (megosztás)

Az adattovábbítás mellett miért beszéljünk az adatmegosztásról is?

A GDPR adattovábbításról beszél, ám gyakran az adattovábbítás valójában úgy történik, hogy nem történik tényleges továbbítás, csak megosztás. Az adatmegosztás azonban nem jelent minden esetben adattovábbítást.

Hogyan tudjuk nyomon követni az adatmegosztásokat? Legegyszerűbben az érintettek szempontjából – az érintettek egy adott adatkezelőnek adták oda az adataikat, és ha azok egy harmadik személyhez kerülnek (harmadik személy tudomására jutnak), az bizony adatmegosztás, bármilyen úton-módon is került arra sor ténylegesen.

[497] 15/1991. (IV. 13.) AB határozat. A határozat esetében az „adatfeldolgozás" alatt a jelenlegi adatvédelmi jogban adatkezelést kell érteni.

Az adatmegosztás lehet – többek között –

- ✓ *egyirányú vagy kölcsönös. Tipikus egyirányú adatmegosztás, amikor a sok-sok személyes adatot tartalmazó bevallást benyújtjuk az adóhatóság felé;*
- ✓ *az, amikor adatkezelőként hozzáférést biztosítunk az informatikai rendszerünkben bizonyos adatokhoz egy másik adatkezelőnek;*
- ✓ *adatkezelőként mi, vagy több adatkezelővel együttműködve adunk adatokat harmadik félnek/feleknek (például adatbankot üzemeltetünk);*
- ✓ *amikor több adatkezelővel együtt létesítünk adatbankot és elérhetővé tesszük az adatokat egymás számára („data pooling"), de akár harmadik félnek is elérhetővé tehetjük a személyes adatokat vagy azok egy részét;*
- ✓ *rendszeresen és tervezetten osztunk meg adatokat egy adott cél érdekében (például diákszövetkezettel, munkaerő kölcsönzővel, könyvvizsgálóval, flottakezelővel stb.);*
- ✓ *egyszeri adatmegosztást hajtunk végre (például munkaügyi ellenőrzés során az ellenőrzés alá vont személyek adatait átadjuk az ellenőrnek);*
- ✓ *egyszeri adatmegosztást hajtunk végre sürgősségi helyzetben (például üzemi baleset esetén a katasztrófavédelemnek átadjuk a még elő nem került, gyaníthatóan a baleset helyszínén tartózkodó munkavállalóink fényképét és egyéb adatait annak érdekében, hogy megkönnyítsük a keresést).*

Előfordulhat, hogy az adatmegosztás akkora kockázatot hordoz, hogy adatvédelmi hatásvizsgálatot kell lefolytatnunk, ilyen lehet például az, amikor különleges adatok kategóriájába tartozó adatot osztunk meg.

Az adatok átadásakor

- ✓ mindig meg kell felelnünk a GDPR alapelveinek (például az elszámoltathatóság, adatbiztonság stb.);
- ✓ fokozott figyelmet kell fordítanunk azokra az esetekre, amikor az érintettekkel egyenlőtlenek az erőviszonyaink (például a munkavállalók, mint kiszolgáltatott réteg);
- ✓ minden esetben figyelembe kell vennünk az érintettek jogait és szabadságait (Alapjogi Chartában és az Alaptörvényben rögzített alapjogok, a Polgári törvénykönyvben foglalt személyiségi jogok stb.);
- ✓ ügyelnünk kell az adatbiztonság követelményeire; és
- ✓ nem árt, ha az etikai kérdéseket is szem előtt tartjuk, mert hiába jogszerű egy adatmegosztás, attól még ez tartozhat a tisztességtelen kategóriába.

Az adatok átadásakor tisztáznunk kell az átadás kereteit (közös adatkezelés, adatfeldolgozás vagy egymástól elkülönült adatkezelők együttműködése), illetve jogszerűen tudnunk kell hivatkozni a megfelelő jogalapra.

Átadhatjuk (megoszthatjuk) az adatokat például

- ✓ hozzájárulás alapján. Szükséges feltétel: hozzájárulás megléte.

Példa

- ✓ *munkáltatóként támogatjuk, hogy alkalmazottjaink részt vegyenek egy jótékonysági futóversenyen, a nevezéshez pedig el kell küldenünk az adatokat a szervezőnek;*
- ✓ *matematikaversenyt szervezünk és a nyertes kisiskolások szülei hozzájárulnak, hogy a verseny közösségi médiás oldalán a helyezettek fotóit nyilvánosságra hozzuk.*

✓ szerződés alapján. Szükséges feltétel: szerződés előkészítéséhez szükséges dokumentáció / szerződés / szerződés teljesítésének dokumentációja.

Példa

- ✓ *a külföldi utazást szervező utazási irodának az utas adatait át kell adnia a szállodának foglalás céljából;*
  Szükséges feltétel: az utassal kötött szerződés teljesítéséhez szükséges legyen az adatátadás, azaz csak úgy tud szállást foglalni az utas számára az iroda, ha az adatokat átadja a szállodának.

✓ jogi kötelezettség alapján. Szükséges feltétel: jogszabályi hely korrekt megjelölése.

Példa

- ✓ *munkáltatóként meg kell küldenünk a munkavállalóink adatait az illetékes munkavédelmi hatóságnak egy munkahelyi balesettel kapcsolatban.*

✓ létfontosságú (vitális) érdek alapján. Szükséges feltétel: szükségesség-arányosság és adatkezelőként nem tudunk másik jogalapra hivatkozni.

Példa

- ✓ *balesetben megsérülünk, és öntudatlan állapotban nem tudjuk adatainkat megadni a mentőknek és ezt helyettünk – életünk megmentése céljából – más teszi meg.*

✓ Közérdek / közfeladat ellátása alapján. Szükséges feltétel: jogszabályi előírás vagy szükségességi-arányossági teszt.

Példa

- ✓ *fenntartóként óvodát üzemeltetünk és átadjuk a gyermekek adatait az illetékes kormányhivatalnak.*

✓ jogos érdek alapján. Szükséges feltétel: érdekmérlegelési teszt.

Példa

- ✓ *az üzleti partnerünk képviselőjének az adatait átadjuk az irodaház portaszolgálatának annak érdekében, hogy tárgyalópartnerünk képviselője részt tudjon venni a mi irodánkban tartandó megbeszélésen (azaz beléphessen az épületbe).*

Különleges adatok, illetve bűnügyi adatok esetében a GDPR 9. és 10. cikkben foglaltakat is teljesíteni kell tudnunk adatkezelőként, hiszen

- ✓ ezek kezelése alapvetően tilos,
- ✓ kivéve, ha a 9. cikk (2) bekezdésében felsorolt tíz feltétel egyikét teljesíteni tudjuk.

Példa

- ✓ *a munkavállalóink üzemi balesetével kapcsolatban azokat az adatokat (például a sérüléssel kapcsolatos egészségügyi adatokat) adhatjuk át a foglalkoztatást szabályozó jogi kötelezettségre hivatkozva, amelyek átadásra az adott adatkategória tekintetében jogszabály kötelez minket.*

Adatkezelőként mindig el kell tudnunk számolnunk az érintettek felé azzal, hogy kivel osztottuk meg a személyes adataikat (akár rendszeres, akár eseti jelleggel) és nem oszthatjuk meg úgy az adatokat, hogy arra az érintettek nem számíthatnak.

Példa

- ✓ *munkáltatóként nem adhatjuk át biztosításokat közvetítő alkuszcégnek a munkavállalóink személyes adatait arra gondolva, hogy biztos szükségük van valamilyen biztosításra és örülni fognak, ha az alkusz felkeresi őket.*

Milyen szempontokat kell követnünk az adatmegosztásunk során? Íme néhány kérdés, amit mindenképpen tudnunk kell válaszolnunk:

- ✓ mi a célunk az adatmegosztással? Ez a cél fogja meghatározni azt, hogy kivel és milyen adatokat oszthatunk meg.
- ✓ milyen adatokat szükséges megosztanunk? Csak azokat, amelyek a célunk eléréséhez feltétlenül szükségesek. A „biztos jó lesz valamire” adatokat nemcsak kezelnünk, de megosztanunk is kifejezetten tilos.
- ✓ az adatok megosztása nélkül el tudjuk érni az adott célunkat?

Példa

Ha az irodaház üzemeltetőjének nem adjuk oda a munkavállalóink adatait, akkor vajon azok hogyan tudnak belépni az általunk bérelt irodákba?

- ✓ *Ha kapunk x darab belépőkártyát („személyi kártyát”), amelyeket mi osztunk ki a saját munkavállalóinknak és azzal be tudnak lépni az épületbe a kollégák, akkor nem szükséges leadnunk a neveket az üzemeltetőnek, csak nekünk, mint bérlőnek kell nyilvántartanunk, pontosan melyik azonosítási számú kártyát kinek adtuk ki használatra.*
- ✓ *Ha az irodaház mélygarázsába szeretne beállni a munkavállalónk a saját autójával, abban az esetben az irodaház adatkezelési folyamataitól függően*
  - o *a munkavállalónk gépjárművének rendszámát le kell adnunk, mint beléptetéshez szükséges adatot (rendszámfelismerő rendszer alkalmazása esetén). Amennyiben az adott munkavállaló több járművet is használhat, abban az esetben minden rendszámot le kell adni.*

- *a belépő kártyához van rendelve olyan lehetőség, hogy az illető behajthat gépjárművel a területre (a beléptető kapunál a kártyát kell megmutatni); ez esetben nem szükséges a rendszámot leadni, illetve ugyanaz a munkavállaló több járművet is használhat anélkül, hogy fennakadás lenne a rendszerben.*

Az irodaház üzemeltetője dönt abban a kérdésben, hogy milyen beléptető rendszereket alkalmaz és azokkal kapcsolatban mennyi személyes adatot kíván kezelni.

Amennyiben lehetséges, alkalmaznunk kell olyan garanciális megoldásokat, mint például az álnevesítés és az anonimizálás.

- ✓ milyen kockázatokkal jár az adatmegosztásunk az érintettekre? Ez a kockázat lehet például fizikai, érzelmi, gazdaság, szociális kár stb.
- ✓ Valószínű, hogy az érintettek tiltakozni fognak az adatátadásunk ellen? Alááshatja az érintettek belénk, azaz az adataik kezelőjébe vetett bizalmát az adatátadásunk?

A spanyol adatvédelmi hatóság (AEPD) gyakorlatából

Az AEPD úgy ítélte meg, hogy a személyes adatokat tartalmazó dokumentumok bíróságokkal és más érintett felekkel való megosztása a bírósági eljárások keretében nem sérti az adatvédelemhez való jogot, mivel a tisztességes eljáráshoz és a jogi védelemhez való joggal szemben egyensúlyt kell teremteni.

Egy érintett panaszt nyújtott be az AEPD-hez, mivel egy ellene indított jogi eljárásban az egyik részt vevő fél megosztott egy másik, ugyanabban a jogi eljárásban részt vevő másik féllel egy olyan jogi dokumentumot, amely az érintett személyes adatait tartalmazta.
Az AEPD a spanyol alkotmánybíróság ítélkezési gyakorlata alapján úgy ítélte meg, hogy egy olyan bírósági eljárás keretében, amelyben az érintett fél, nem szükséges az érintett hozzájárulását kérni ahhoz, hogy a bírósággal és az eljárásban részt vevő többi féllel megosszák a perben bizonyítékként használt dokumentumokat.

Az AEPD a határozata nem elemezte részletesen a GDPR rendelkezéseit, hanem általános mérlegelést végzett az adatvédelemhez való jog, a tisztességes eljáráshoz való jog és a jogi védelemhez való jog között és arra a következtetésre jutott, hogy az egyének nem használhatják fel az adatvédelmi jogot arra, hogy elkerüljék a bírósági eljárás szempontjából releváns személyes adatok nyilvánosságra hozatalát.[498]

[498] Procedimiento Nº: E/01090/2021, https://www.aepd.es/es/documento/e-01090-2021.pdf, utolsó letöltés: 2022. 08. 09.

- ✓ a leginkább megfelelő módot választottuk az adatátadásra? A kérdés megválaszolása során olyan szempontokat kell figyelembe vennünk, mint például a kockázat mértéke, etikai megfontolások stb.
- ✓ mit eredményez az, ha nem osztjuk meg az adatokat?

Példa

- ✓ *amennyiben az adóhivatallal nem osztjuk meg a jogszabályban előírt adatokat, akkor vizsgálatot és büntetést kapunk a nyakunkba;*
- ✓ *ha nem adjuk át a képviselőnk adatát az üzleti partnerünknek, ezzel lehetetlenné tesszük a korrekt és gördülékeny kommunikációt;*
- ✓ *ha nem adjuk át a kötelező továbbképzést végző cégnek a munkavállalóink adatait, azok nem fogják tudni leoktatni a munkavállalóinkat és nem tudnak számukra olyan bizonyítványt (igazolást) kiállítani, amely szükséges a munkakörük további betöltéséhez;*
- ✓ *amennyiben a cégünket képviselő ügyvédnek nem adjuk át a képviseletünkhöz szükséges személyes adatokat, abban az esetben nem tudja ellátni megfelelően a szerepét a peres eljárásunkban,*

- ✓ jogosultak vagyunk megosztani a személyes adatokat?

Példa

- ✓ *csak olyan dolgozónkat nevezzünk jótékonysági futóversenyre, aki a nevezéshez (az adatainak a szervezők számára átadásához) hozzájárult*

- ✓ kinek szükséges, hogy hozzáférése legyen a megosztott adatokhoz? Ügyelnünk kell a „need to know” elv alkalmazására, ezért célszerű mindig kikötnünk az adatmegosztásra vonatkozó megállapodásban, hogy csak az arra jogosultsággal rendelkező személyek férhessenek hozzá az átadott adatokhoz, akkor is csak a munkakörükből/megbízásukból fakadó szükségesség erejéig.
- ✓ mikor kell megosztanunk az adatokat? (esetenként vagy rendszeresen)
- ✓ hogyan osztjuk meg az adatokat?

Példa

- ✓ *a hatóságnak e-mailben elküldhetjük a kért tájékoztatást (személyes adatot)*
- ✓ *a tanulmányi kirándulás szervezőjének e-mailhez csatolt fájlként küldjük el a diákok adatait*
- ✓ *az érintettnek az érintetti kérelmére a választ levélben postán küldjük ki (azért, mert így kérte)*
- ✓ *fejvadász cégként hozzáférést adtunk az adatbázisunkhoz a velünk szerződés keretében együttműködő partnerünknek*

- ✓ hogyan ellenőrizhetjük, hogy az adatmegosztásunk teljesítette a célját?

Példa

- ✓ *az adóhivatal visszaigazolja a munkavállalóink személyes adatait tartalmazó havi bevallásunk beérkezését*
- ✓ *a tanulmányi kirándulás szervezőjétől visszaigazolást kapunk a busz- és szállásfoglalásról*
- ✓ *az érintetti kérelemre válasz esetén visszaérkezik a levél átvételének igazolása*
- ✓ *az adatbázisunk naplóadataiból látjuk, hogy partnerünk mikor lépett be az adatbázisunkba és pontosan mely álláskeresők profilját nézte meg*

✓ folytattunk le az adatmegosztásunkkal kapcsolatban hatásvizsgálatot? Ha igen, milyen megállapításokra jutottunk a kockázatok tekintetében és mikor kell azt felülvizsgálnunk? Ha nem volt kötelező hatásvizsgálatot lefolytatnunk, de új technológiára kívánunk áttérni, akkor – ezen új körülmények figyelembevételével – kell ilyet lefolytatnunk?

Példa

- ✓ *rendszeres, kis mennyiségű adatot érintő adatmegosztást eddig titkosított e-mailes formában végeztünk, ám most áttérünk az adatbázisunkhoz közvetlen hozzáférés biztosításával történő adatmegosztásra és ezzel egyidejűleg a megosztott adatok mennyisége is jelentősen nő;*
- ✓ *az eddigi rendszeres papír alapú adatmegosztásunkat digitális transzformáció keretében átalakítjuk és IoT-eszközök segítségével közvetlen adatáramlást biztosítunk,*

Adatmegosztás közös adatkezelés keretében

Amennyiben az adatmegosztásra más adatkezelőkkel közös adatkezelés keretében kerül sor, az erről szóló megállapodásban feltétlen rendeznünk kell az alábbiakat:

✓ mely szervezetek (adatkezelők) tagjai az adatmegosztásnak?

Például

- ✓ *egy multinacionális vállalatcsoport esetében mely leányvállalatok használják közösen ugyanazt az alkalmazást a munkavállalók adatainak kezelésére?*

✓ a közös adatkezelésben részt vevő adatkezelők mely más adatkezelőkkel osztják meg az adatokat?

Példa

- ✓ *a leányok milyen adatfeldolgozókat vesznek igénybe a munkavállalók adatainak kezelése során (például bérszámfejtő alvállalkozó számára adatátadás stb.)?*

✓ hogyan biztosítjuk a közös adatkezelés keretében végzett adatkezelések során az érintettek jogait? Hogyan gyakorolhatják az érintettek a hozzáférési jogukat?

A közös adatkezelés esetén az érintettek bármelyik adatkezelőhöz fordulhatnak akkor is, ha a közös adatkezelők kijelöltek kapcsolattartó szervezetet.

- ✓ a közös adatkezelés során milyen adatkategóriákat osztunk meg és kivel? Rendelkeznünk kell a jogosultságról stb.
- ✓ milyen jogalapra hivatkozunk a közös adatkezelés során?
- ✓ érint a közös adatkezelésünk keretében történő adatmegosztásunk az adatok különleges kategóriájába tartozó vagy bűnügyi adatokat?

Példa

- ✓ *egy fogorvosi rendelőben több önálló fogorvos is dolgozik (nem munkavállalóként), miközben ugyanazt a szoftvert és adatbázist használják a betegek ellátása során.*

- ✓ milyen információkezelési intézkedésekre van szükségünk? A megállapodásban rendelkeznünk kell olyanokról, mint például az adatmegőrzés egyeztetett időtartama, adattörlés és a hibás adatok javításának módja, jogosultság kiosztása, információbiztonsági intézkedések, érintetti kérelmek teljesítése, adatvédelmi incidens kezelése stb.;
- ✓ a közös adatkezelésről szóló megállapodás felülvizsgálatának módja, időszakossága;
- ✓ egyéb olyan kérdések, amelyeket rendezni kívánunk a megállapodásban, például a tevékenységre irányadó jogszabályok megnevezése, az adatkezelés során használt egységesített nyomtatványok stb.

A norvég adatvédelmi hatóság gyakorlatából

2020-ban a Norvég Fogyasztói Tanács panaszt nyújtott be a Grindr ellen miszerint az a személyes adatokat marketingcélokból jogellenesen osztja meg harmadik felekkel. A megosztott adatok: lokációs adatok, IP-cím, hirdetési azonosító, életkor, a nem és az a tény, hogy az adott felhasználó a Grindr-en van. A megosztott adatok alapján a felhasználók azonosíthatóak voltak és a címzettek potenciálisan tovább oszthatták az adatokat.

A hatóság megállapította, hogy a Grindr jogalap (érvényes hozzájárulás) nélkül adta át a felhasználói adatait harmadik feleknek viselkedésalapú reklámozás céljából. A Hatóság továbbá arra a következtetésre jutott, hogy ebben az esetben a hozzájárulás volt az alkalmazandó jogalap, de a Grindr által a személyes adatok hirdetési partnerekkel való megosztásához gyűjtött állítólagos hozzájárulások nem voltak érvényesek.

A Hatóság véleménye szerint azok az adatok, amelyekből kiderül, hogy valaki Grindr-felhasználó, erősen utalnak arra, hogy szexuális kisebbséghez tartozik, azaz az átadott adatok az érintettek szexuális irányultságára vonatkozó adatok különleges kategóriába tartozó adatoknak minősülnek, amelyek a GDPR

értelmében különleges védelmet érdemelnek, ezért a hatóság 6,5 millió eurós közigazgatási bírságot szabott ki.[499]

Felelősségünk a velünk megosztott adatokkal kapcsolatban

Amennyiben kellő gondossággal kívánunk eljárni adatkezelőként

- ✓ meg kell erősítenünk az adatok forrását;

Példa

- ✓ *igazolnunk kell, hogy tényleg onnan kaptuk az adatokat ahonnan kell, nem pedig közbeékelődéses („man in the middle") támadás áldozatai vagyunk. A közbeékelődéses támadás során az adatokat átadó és az adatokat átvevő szereplők közötti kommunikációt kompromittálja a támadó oly módon, hogy a kommunikációs csatornát (például az e-mailt) eltérítve mindkét fél számára a másik félnek adja ki magát.*

- ✓ meg kell állapítanunk, jogszerűen szereztük-e meg az adatokat;
- ✓ le kell ellenőriznünk, hogy az érintett milyen tájékoztatást kapott az adatkezeléssel kapcsolatban;
- ✓ le kell ellenőriznünk az adatok kezdeti gyűjtésének módját és idejét;
- ✓ meg kell győződnünk a hozzájárulás érvényességéről (amennyiben hozzájárulásra hivatkozva kezeljük az adatokat);
- ✓ le kell ellenőriznünk, hogy az érintettek milyen információkat kaptak az adatkezelésről amennyiben az adatok nem az érintettektől származnak;
- ✓ meg kell vizsgálnunk az adatok pontosságát és naprakészségét;
- ✓ ügyelnünk kell arra, hogy a kapott adatok ne legyenek túlzottak vagy irrelevánsok, figyelembe véve az igényeinket (adattakarékosság, illetve célhoz kötöttség elve);
- ✓ tájékoztatnunk kell az érintetteket (egy hónapon belül, illetve ennél korábban, ha felvettük velük a kapcsolatot, lásd GDPR 14. cikke).

Nyilvánosságra hozatal, publikáció

Az adat nyilvánosságra hozása azt jelenti, hogy az adatot bármely harmadik személy megismerheti.[500] Amennyiben személyes adatot hozunk nyilvánosságra (osztunk meg), meg kell bizonyosodnunk arról, hogy

- ✓ ezt jogi kötelezettség alapján tesszük-e (pl. közérdekből nyilvános adatokat hozunk nyilvánosságra);
- ✓ az információ nyilvánvalóan nem tolakodó (azaz nem hatolunk be túlságosan az érintett privát szférájába);
- ✓ amennyiben ez szükséges, az érintett hozzájárult a nyilvánosságra hozatalhoz;
- ✓ az információ olyan formában kerül nyilvánosságra, hogy az érintett nem azonosítható.

[499] The NO DPA imposes fine against Grindr LLC, https://www.datatilsynet.no/en/regulations-and-tools/regulations/avgjorelser-fra-datatilsynet/2021/gebyr-til-grindr/
[500] 15/1991. (IV. 13.) AB határozat

Példa

- ✓ *a köznevelési intézmény nyilvánosságra hozza azokat a személyes adatokat, amelyeket jogszabály (információszabadság) alapján nyilvánosságra kell hoznia;*
- ✓ *állatorvosként a négylábú páciensünk gazdája hozzájárult, hogy a praxisunk honlapján az ő fényképükkel reklámozzuk a rendelőnket;*
- ✓ *a zárt közösségi médiás csoport is nyilvánosságra hozatalnak számít, így a zárt Facebook csoportban sem tehetjük közzé, hogy abban az óvodában, ahova gyermekünk jár, melyik csoportban pontosan melyik gyermeknek az anyukája covidos.*

Minden esetben egyensúlyt kell teremtenünk a publikálás előnyei és az érintettek (például a munkavállalók, szerződéses partnerek) privát szférájuk tiszteletben tartásával kapcsolatos észszerű elvárásai között.

Az osztrák adatvédelmi hatóság (Datenschutzbehörde – DSB) gyakorlatából

A DSB 600 eurós bírsággal sújtott egy orvost, mert az 2020 februárja és júniusa között a Facebook-oldalán információkat, köztük egészségügyi adatokat tett közzé betegeiről.

A közzé tett adatok között volt – többek között – a betegek neve és társadalombiztosítási száma, orvosi feljegyzések és protokollok, orvosi diagnózisok, gyógyszerezési adatok, kórházi felvételekre és elbocsátásokra vonatkozó adatok, valamint a betegeket kezelő más orvosok neve.

A DSB megállapította, hogy a betegek nem adták kifejezett hozzájárulásukat az adataiknak online közzétételéhez, és az adatkezelésnek nem volt más jogalapja, ezért az orvost a GDPR több rendelkezésének megsértéséért pénzbírsággal sújtotta [GDPR 5. cikke (1) bekezdés a) pont, illetve a 9. cikk (1) és (2) bekezdés].[501]

Nemzetközi adattovábbítás – biztosítékok, garanciák

A GDPR deklarált célja, hogy az érintettek jogai és szabadságai egyenszilárdságú védelmet élvezzenek szerte az Unió területén és azon kívül is, amennyiben ez lehetséges – a GDPR hatálya alá tartozó adatkezelőknek és adatfeldolgozóknak pedig kötelezettségük ezt a védelmet biztosítani. Az egyenszilárdságú védelem biztosítása érdekében felhasználható eszközöket a GDPR V. fejezete sorolja fel tételesen, ha ezen garanciák egyikét sem tudjuk felmutatni, akkor az adattovábbítás tilos.

Az EGT-tagállamok a GDPR szempontjából belföldnek számítanak, tehát az V. fejezet szerinti plusz garanciát nem kell felmutatnunk ezen tagállamok közötti adatáramlások (adattovábbítások) esetén.

[501] GZ: 2020-0.111.488 vom 19. Oktober 2020 (Verfahrenszahl: DSB-D550.279), https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20201019_2020_0_111_488_00/DSBT_20201019_2020_0_111_488_00.pdf, utolsó letöltés: 2022. 08. 09.

Az alábbi országok tagjai az Európai Gazdasági Térségnek (EGT)

- ✓ *Az Európai Unió tagállamai: Ausztria, Belgium, Bulgária, Ciprus, Csehország, Dánia, Észtország, Finnország, Franciaország, Görögország, Hollandia, Horvátország, Írország, Lengyelország, Lettország, Litvánia, Luxemburg, Magyarország, Málta, Németország, Olaszország, Portugália, Románia, Spanyolország, Svédország, Szlovákia, Szlovénia*
- ✓ *az Európai Gazdasági Térségről szóló megállapodásban részes más államok: Izland, Liechtenstein, Norvégia*

Mi számít nemzetközi adattovábbításnak?

A GDPR nem határozza meg a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbításának fogalmát. Ezt a hiányosságot pótolva az EDPB iránymutatásában[502] három kumulatív kritériumot határozott meg, amelyek alapján az adatkezelés harmadik országba adattovábbításnak minősül:

a) az adatkezelő vagy az adatfeldolgozó az adott adatkezelés tekintetében a GDPR hatálya alá tartozik.
b) Ez az adatkezelő vagy adatfeldolgozó („exportőr") továbbítás útján vagy más módon az adott adatkezelés tárgyát képező személyes adatokat egy másik adatkezelő, közös adatkezelő vagy adatfeldolgozó („importőr") rendelkezésére bocsátja. Az ugyanazon vállalatcsoport részét képező szervezetek külön adatkezelőnek vagy adatfeldolgozónak minősül(het)nek, azaz az ugyanazon vállalatcsoporthoz tartozó szervezetek közötti adatközlések (csoporton belüli adatközlések) személyes adatok továbbításának minősül(het)nek.
c) Az importőr harmadik országban található vagy nemzetközi szervezet, függetlenül attól, hogy ez az importőr a GDPR 3. cikk szerint az adott adatkezelés tekintetében a GDPR hatálya alá tartozik-e vagy sem.

Amennyiben az adattovábbításunk esetében három kritérium teljesül, abban az esetben harmadik országnak vagy nemzetközi szervezetnek történő átadásról van szó. Ez konkrétan azt jelenti, hogy a személyes adatokat exportőrként egy harmadik országbeli másik adatkezelő vagy adatfeldolgozó (importőr) részére megküldjük vagy bocsátjuk rendelkezésre, függetlenül attól, hogy ez az importőr az adott adatkezelés tekintetében a GDPR hatálya alá tartozik-e vagy sem.

Ha ebben a helyzetben vagyunk, meg kell felelnünk a GDPR V. fejezetében foglalt feltételeknek, és az adattovábbítás során olyan eszközöket kell alkalmaznunk, amelyek célja a személyes adatok védelme a harmadik országba vagy nemzetközi szervezethez történő továbbítást követően.

Melyek ezek az eszközök?

[502] Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international
transfers as per Chapter V of the GDPR Adopted on 18 November 2021, https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf, utolsó letöltés 2022. 08. 30.

Ezek az eszközök magukban foglalják annak elismerését, hogy

- ✓ abban a harmadik országban vagy nemzetközi szervezetben, ahová a személyes adatokat továbbítjuk, ezen adatok tekintetében megfelelő szintű védelem áll fenn (GDPR 45. cikk), vagy – ilyen megfelelő szintű védelem hiányában –
- ✓ exportőrként a GDPR 46. cikkben előírt megfelelő garanciák valamelyikét hajtjuk végre.

Amennyiben ezen, feltételeknek nem tudunk megfelelni, a GDPR 49. cikk tartalmazza azokat a kivételes helyzeteket, amely meghatározott helyzetekben és feltételek mellett a személyes adatokat továbbíthatjuk harmadik országba vagy nemzetközi szervezetnek megfelelő szintű védelem vagy megfelelő garanciák végrehajtása nélkül.

Megfelelő garanciák alapján történő adattovábbítások (GDPR 46. cikk)

Megfelelőségi határozat

Az Európai Bizottság megfelelőségi határozata által „adekvát" államoknak minősített országokban ugyan nem hatályos a GDPR, azonban az érintettek jogai és szabadságai legalább ugyanolyan védelmet élveznek, mint az EGT-tagállamok területén.

Az Európai Bizottság eddig az alábbi államokat ismerte el megfelelő védelmet nyújtónak: Andorra, Argentína, Kanada (kereskedelmi szervezetek), a Feröer-szigetek, Guernsey, Izrael, Man-sziget, Japán, Dél-Korea, Jersey, Új-Zéland, Svájc, Uruguay és az Egyesült Királyság.[503]

Ez nem azt jelenti, hogy ezek a harmadik országok ugyanazokat a jogi eszközöket alkalmazzák, mint a GDPR – a védelmi eszközeik eltérőek is lehetnek, a lényeg az, hogy az Unió elvárt védelmi szintet biztosítsák. Ehhez a Bizottság olyan területeket vizsgál meg, mint az adott ország nemzeti jogszabályai, az alkalmazandó nemzetközi kötelezettségei, részvétele többoldalú vagy regionális rendszerekben, különös tekintettel a személyes adatok védelmét illetően.

Egyéb garanciák

Megfelelőségi határozat hiányában adatot továbbítani olyan megfelelő feltételeket biztosító garanciák nyújtásával tudunk, amelyek az érintettek számára elérhetővé teszik az érvényesíthető jogokat és a hatékony jogorvoslati lehetőségeket. Ilyen megfelelő garancia lehet többek között:

- ✓ vállalkozáscsoportok vagy közös gazdasági tevékenységben részt vevő vállalatcsoportok esetében a vállalatok a személyes adatokat az úgynevezett kötelező erejű vállalati szabályok (BCRs)
- ✓ szerződéses megállapodások a személyes adatok címzettjével, például az Európai Bizottság által jóváhagyott általános szerződési feltételek felhasználásával (SCCs)[504]

[503] az USA történetét lásd a „Adattovábbítás az Amerikai Egyesült Államokba" fejezetben.
[504] az Európai Bizottság által az EGT-n belüli adatkezelők vagy adatfeldolgozók és az EGT-n kívüli adatkezelők vagy adatfeldolgozók közötti személyesadat-továbbításra vonatkozóan

- ✓ magatartási kódex vagy tanúsítási mechanizmus betartása, valamint
- ✓ a címzett jogilag kötelező erejű, kikényszeríthető jogi kötelezettségvállalásának megszerzése a továbbított adatok védelmét biztosító megfelelő garanciák alkalmazása érdekében.

Az adattovábbítás kockázatai tekintetében kockázatértékelést (hatásvizsgálatot) kell végeznünk.

A biztosítékok tartalmát a helyzettől függően kell testre szabnunk – például adatkezelőként más garanciákat kell nyújtanunk, mint adatfeldolgozóként. Éppen ezért a megfelelő adattovábbítási eszközök, azaz a szabványos szerződéses záradékok (SCCs) vagy ad hoc szerződéses záradékok kidolgozásakor figyelembe kell vennünk azt, hogy ezek ne a GDPR szerinti kötelezettségeink megkettőzése, hanem hiányzó garanciák pótlásai legyenek (például a harmadik országban a GDPR rendelkezéseivel ellentétes nemzeti jogszabályok vagy a kormányzati hozzáférés miatt, illetve a jogérvényesítés és jogorvoslat nehézségei miatt szükséges hiányosságok pótlása érdekében).

Soha nem szabad szem elől tévesztenünk, hogy adatkezelőként felelősek vagyunk minden általunk ellenőrzött adatkezelésért, függetlenül attól, hogy az hol történik. Ráadásul a harmadik országokban történő adatkezelés olyan kockázatokat rejthet magában, amelyeket azonosítanunk és kezelnünk kell annak érdekében, hogy a GDPR értelmében jogszerűen járjunk el.

A személyes adatok EGT-n belüli és EGT-n kívüli, közhatalmi vagy egyéb, közfeladatot ellátó szervek közötti továbbításáról az EDPB külön iránymutatást adott ki.[505]

Mely intézkedésekkel csökkenthetjük az adattovábbítás kockázatait?

Az EDPB ajánlást[506] bocsátott ki azon intézkedésekről, amelyek kiegészítik az adattovábbítási eszközöket a személyes adatok uniós védelmi szintjének való megfelelés biztosítása érdekében.

elfogadott általános adatvédelmi kikötések (vagy „általános szerződési feltételek"). Az Európai Bizottság által elfogadott általános szerződési feltételek az általános adatvédelmi rendelet 46. cikk (2) bekezdés c) pontja és (5) bekezdése értelmében a GDPR szerinti adattovábbítási eszköznek minősülnek.

[505] 2/2020. számú iránymutatás az (EU) 2016/679 rendeletnek a személyes adatok EGT-n belüli és EGT-n kívüli, közhatalmi vagy egyéb, közfeladatot ellátó szervek közötti továbbításáról szóló 46. cikke (2) bekezdésének a) pontjáról és 46. cikke (3) bekezdésének b) pontjáról, 2.0 változat, https://edpb.europa.eu/system/files/2021-05/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_hu.pdf, utolsó letöltés: 2022. 08. 30.

[506] 01/2020. számú ajánlás azon intézkedésekről, amelyek kiegészítik az adattovábbítási eszközöket a személyes adatok uniós védelmi szintjének való megfelelés biztosítása érdekében 2.0. változat Elfogadás időpontja: 2021. június 18. https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_hu_0.pdf, utolsó letöltés: 2022. 08. 30.

Az EDPB határozottan állást foglal atekintetben, hogy a személyes adatok harmadik országokba történő továbbítását nem alkalmazhatjuk az EGT-ben biztosított védelem aláásásának vagy gyengítésének eszközeként – azaz a harmadik országokban biztosított védelmi szintnek, nem azonosnak, hanem lényegében azonosnak kell lennie az EGT-ben biztosított védelmi szinttel. Adatexportőrként eljárva a mi feladatunk, hogy esetről esetre és adott esetben a harmadik országbeli adatimportőrrel együttműködve ellenőrizzük, hogy a harmadik ország joga vagy gyakorlata hatással van-e az általunk használt garanciák megfelelő hatékonyságára. Ha igen, olyan kiegészítő intézkedéseket kell végrehajtanunk, amelyek pótolják a védelem ezen hiányosságait.

Az EDPB hatlépéses vizsgálatot javasol:

Első lépés: ismerjük meg az adattovábbításainkat és legyen tisztában azzal, hogy az általunk továbbított adatok az adatkezelési célunk szempontjából megfelelőek és relevánsak-e, valamint a szükségességre korlátozódnak-e, illetve hova, milyen védelmi szintű helyre kerülnek.

Második lépés: ellenőrizzük, hogy a GDPR V. fejezetében felsoroltak közül melyik adattovábbítási eszközön alapul az adattovábbításunk.

- Ha megfelelőségi határozat megfelelőnek nyilvánította azt az országot, régiót vagy ágazatot, amelybe az adatokat továbbítjuk, akkor mindaddig, amíg a határozat hatályban van, nem kell további lépéseket tennünk azon kívül, hogy figyelemmel kísérjük a megfelelőségi határozat érvényességét.
- Megfelelőségi határozat hiányában a GDPR 46. cikkében felsorolt adattovábbítási eszközök valamelyikét kell igénybe vennünk.
- A GDPR 49. cikkében meghatározott eltérésekre csak néhány esetben hivatkozhatunk és csak akkor, ha teljesítjük az abban foglalt feltételeket. Fontos, a kivételes helyzet az kivételes helyzet, azaz nem alkalmazhatjuk főszabályként.

Harmadik lépés: értékeljük, hogy a harmadik országban fennálló jogi helyzet és/vagy gyakorlat bármilyen módon hatást gyakorolhat-e azon adattovábbítási eszközök megfelelő garanciáinak hatékonyságára, amelyeket az adott adattovábbítással összefüggésben igénybe veszünk. Az értékelés során az adattovábbítási eszköz szempontjából releváns harmadik országbeli jogszabályokra kell összpontosítanunk, illetve a harmadik ország hatóságainak gyakorlatait megvizsgálva ellenőrizhetjük, hogy az adattovábbítási eszközben foglalt garanciák képesek-e biztosítani a gyakorlatban is a továbbított személyes adatok hatékony védelmét. Amennyiben:

a) a harmadik ország uniós előírásoknak formálisan megfelelő jogszabályait a gyakorlatban nyilvánvalóan nem alkalmazzák/nem tartják be;
b) léteznek olyan gyakorlatok, amelyek összeegyeztethetetlenek az adattovábbítási eszköz kötelezettségvállalásaival, amennyiben a harmadik országban hiányoznak a vonatkozó jogszabályok;
c) az általunk továbbított adatok és/vagy az adatimportőr problematikus jogszabályok hatálya alá tartoznak vagy tartozhatnak. Ebben az esetben az adattovábbítási eszközben foglalt szerződéses garanciában foglaltak megkérdőjeleződnek és az nem felel meg a GDPR követelményeinek.

Az első két esetben fel kell függesztenünk az adattovábbítást, vagy megfelelő kiegészítő intézkedéseket kell végrehajtanunk, ha folytatni kívánjuk azt, a harmadik esetben a bizonytalanságokra tekintettel

- vagy felfüggesztjük az adattovábbítást és további kiegészítő intézkedéseket hajtunk végre az adattovábbítás folytatása érdekében,
- vagy kiegészítő intézkedések végrehajtása nélkül folytatjuk az adattovábbítást. Ezt csak abban az esetben érdemes megtennünk, ha úgy ítéljük meg, és képesek vagyunk bizonyítani és dokumentálni, hogy nincs okunk azt feltételezni, hogy a vonatkozó és problematikus jogszabályokat a gyakorlatban úgy értelmezik és/vagy alkalmazzák majd, hogy azok hatálya kiterjedjen az általunk továbbított adatokra és az adatimportőrre.

Ezt az értékelést úgy hajtsuk végre, hogy az illetékes felügyeleti és/vagy igazságügyi hatóságok kérhetik ezt tőlünk és elszámoltathatnak minket bármely döntésünkért, amit ez alapján az értékelés alapján hoztunk.

A belga bírósági gyakorlatból

Az Államtanács felfüggesztett egy amerikai vállalat kiválasztásáról szóló közbeszerzési döntést, mivel nem lett megfelelően megvizsgálva, hogy a vállalat megfelel-e a GDPR követelményeinek, különösen az adattovábbításra és a további feldolgozásra vonatkozó rendelkezéseknek.

A VIVALIA (kórházak állami hálózata) nyilvános pályázatot írt ki a kórházak betegadatainak statisztikai célú feldolgozására. A megbízást a 3M amerikai vállalat kapta, amely már korábban is szerepelt a hírekben azzal kapcsolatban, hogy megfelelő biztosítékok nélkül továbbított adatokat az Egyesült Államokba és Oroszországba. Ennek alapján egy harmadik fél, amely szintén részt vett a közbeszerzési eljárásban, megtámadta a VIVALIA döntését.

Az Államtanács úgy ítélte meg, hogy a közbeszerzési eljárás lezárása előtt a VIVALIA-nak – a közbeszerzési eljárásokra vonatkozó szabályokat figyelembe véve – vizsgálnia kellett volna, hogy a 3M mennyiben felel meg a GDPR nemzetközi adattovábbításra vonatkozó rendelkezéseinek. Tekintettel arra, hogy a VIVALIA e tekintetben nem végzett elemzést, az Államtanács felfüggesztette a 3M-et szerződő félként kiválasztó döntést.[507]

Negyedik lépés: azonosítsuk és fogadjuk el azon kiegészítő intézkedéseket, amelyek szükségesek ahhoz, hogy az általunk továbbított adatok védelmének szintje megfeleljen a lényegi azonosság uniós követelményének. Erre a lépésre csak akkor van szükségünk, ha az értékelésünk szerint a harmadik ország jogszabályai és/vagy gyakorlatai hatással vannak az adattovábbításunkkal összefüggésben igénybe vett vagy igénybe venni kívánt adattovábbítási eszköz hatékonyságára. A kiegészítő

[507] nº 253.677 du 6 mai 2022, http://www.raadvst-consetat.be/Arrets/253000/600/253677.pdf#xml=http://www.raadvst-consetat.be/apps/dtsearch/getpdf.asp?DocId=40765&Index=c%253a%255csoftware%255cdtsearch%255cindex%255carrets_fr%255c&HitCount=2&hits=1e+1f+&065529202251, utolsó letöltés: 2022. 08. 30.

intézkedéseket esetről esetre kell megválasztanunk, azok egyes országokban hatékonyak lehetnek, másokban azonban nem feltétlen. Az általunk választott kiegészítő intézkedéseket értékelnünk és dokumentálnunk kell. Az ajánlás 2. sz. melléklete esettanulmányok keretében tartalmaz példákat a kiegészítő intézkedésekre.

A belga bírósági gyakorlatból

Az Államtanács (Conseil d'Etat/ Raad van State) megerősítette a flamand hatóságok azon döntését, miszerint egy, az AWS felhőszolgáltatásait használó amerikai vállalat uniós fióktelepével történő szerződéskötés nem sérti a GDPR rendelkezéseit. Az Államtanács többek között az EDPB[508] és a Flamand Felügyeleti Bizottság iránymutatásaira hivatkozott, amelyek az USA-ba irányuló adattovábbítás esetén lehetséges kiegészítő intézkedésként említik a titkosítást.

A flamand hatóságok odaítéltek egy tendert egy AWS felhőszolgáltatásokat használó amerikai vállalat uniós székhelyű vállalkozásának. Egy holland vállalat, amelyet a flamand hatóságok a pályázati eljárás során nem választottak ki, megtámadta ezt a határozatot a következőkre hivatkozva:

- ✓ *a GDPR adattovábbításra vonatkozó rendelkezéseinek megsértése, mivel az Egyesült Államokban nem biztosított a személyes adatok megfelelő védelme. A holland vállalat különösen a flamand felügyeleti bizottság ("Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens") véleményére hivatkozott, amely szerint az AWS használata nem lehetett összhangban a Schrems II. határozattal és a GDPR rendelkezéseivel;*
- ✓ *a GDPR 28. cikkének megsértése, mivel az adatfeldolgozó kiválasztása nem nyújt elegendő garanciát;*
- ✓ *a GDPR 32. cikkének megsértése a megfelelő technikai és szervezési intézkedések hiánya miatt;*
- ✓ *a pályázat odaítéléséről szóló döntés indokoltságának hiánya.*

Az Államtanács megállapította, hogy:

- ✓ *az EDPB és a Flamand Felügyeleti Bizottság nem ellenezte a titkosítás használatát, és az ilyen eszköz használata bizonyos körülmények között megfelelő kiegészítő intézkedés lehet az általános szerződéses kikötések (SCCs) alkalmazása mellett;*
- ✓ *az adatfeldolgozó kiválasztása nem sértette a GDPR 28. cikket, ugyanis a felperes nem tudta bizonyítani, hogy az adatkezelő és az adatfeldolgozó nem hajtotta végre a szükséges technikai és szervezési intézkedéseket;*
- ✓ *a döntés kellően indokolt volt.[509]*

[508] 01/2020. számú ajánlás azon intézkedésekről, amelyek kiegészítik az adattovábbítási eszközöket a személyes adatok uniós védelmi szintjének való megfelelés biztosítása érdekében 2.0. változat Elfogadás időpontja: 2021. június 18. https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_hu_0.pdf, utolsó letöltés: 2022. 08. 30.

[509] JUDGMENT no. 251.378 of 19 August 2021 in case A. 234.221/X11-9119, https://gdprhub.eu/index.php?title=Council_of_State_-_251.378, utolsó letöltés: 2022.08.30

Ötödik lépés: minden olyan hivatalos eljárási lépés megtétele, amelyre az általunk választott kiegészítő intézkedésének elfogadásához szükség lehet.

Hatodik lépés: megfelelő időközönként újra kell értékelnünk az általunk harmadik országokba továbbított személyes adatok védelmi szintjének újraértékelését.

Adattovábbítás az Amerikai Egyesült Államokba

2020. nyaráig az Adatvédelmi pajzs („Privacy Shield") rendezte az Európa Unió és az Egyesült Államok közötti adatáramlást, mely alapján az Adatvédelmi pajzshoz csatlakozó szervezetek esetében adatkezelőként vélelmezhetjük, hogy a tevékenység során biztosítják az érintettek számára a GDPR által megkövetelt „egyenszilárdságú" védelmet.

„A Bíróság érvénytelennek nyilvánítja az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről szóló 2016/1250 határozatot

> *Ezzel szemben a Bíróság úgy ítéli meg, hogy a személyes adatoknak harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló 2010/87 bizottsági határozat érvényes*

(...)

Maximillian Schrems, Ausztriában lakóhellyel rendelkező osztrák állampolgár 2008 óta a Facebook felhasználója. Az Unió területén lakó többi felhasználóhoz hasonlóan M. Schrems személyes adatait a Facebook Ireland részben vagy egészben a Facebook Inc. Egyesült Államokban található szervereire továbbítja, és azokat ott kezelik. M. Schrems panaszt nyújtott be az ír felügyeleti hatósághoz, amely lényegében arra irányul, hogy utóbbi tiltsa meg ezen adattovábbításokat. Arra hivatkozott, hogy az Egyesült Államok joga és gyakorlatai nem biztosítanak elégséges védelmet azzal szemben, hogy az ezen országba továbbított adatokhoz a hatóságok hozzáférjenek. Ezt a panaszt többek között azzal az indokkal utasították el, hogy a Bizottság a 2000/520 határozatában[510] (az úgynevezett „biztonságos kikötőről" szóló határozat) megállapította, hogy az Egyesült Államok megfelelő védelmi szintet biztosít. 2015. október 6-án hozott ítéletében a Bíróság, amely a High Court (felsőbíróság, Írország) által előzetes döntéshozatal céljából előterjesztett kérdés alapján járt el, e határozatot érvénytelennek nyilvánította (a továbbiakban: Schrems I ítélet).[511]

A Schrems I ítélet nyomán, és azt követően, hogy az ír bíróság ez alapján megsemmisítette az e panaszt elutasító határozatot, az ír felügyeleti hatóság felhívta

[510] A 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott „biztonságos kikötő" adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről szóló, 2000. július 26-i 2000/520/EK bizottsági határozat

[511] A Bíróság 2015. október 6-i C-362/14. sz. Schrems-ügyben hozott ítélete, sajtóközlemény: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117hu.pdf

M. Schremset, hogy fogalmazza újra a panaszát (...). Az újrafogalmazott panaszában M. Schrems fenntartja, hogy az Egyesült Államok nem nyújt elégséges védelmet az ezen országba továbbított adatok számára. Kéri, hogy a jövőre nézve függesszék fel vagy tiltsák meg a személyes adatainak az Unióból az Egyesült Államokba történő továbbítását, amelyet a Facebook Ireland immár a 2010/87 határozat[512] mellékletében szereplő általános adatvédelmi kikötések alapján végez. Mivel az ír felügyeleti hatóság úgy vélte, hogy M. Schrems panaszának kezelése többek között a 2010/87 határozat érvényességétől függ, eljárást indított a High Court (felsőbíróság) előtt annak érdekében, hogy ez utóbbi előzetes döntéshozatal iránti kérelmet nyújtson be a Bírósághoz. Ezen eljárás megindítását követően a Bizottság elfogadta az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről szóló 2016/1250 határozatot[513] (az úgynevezett „adatvédelmi pajzsról" szóló határozat). (...)

A mai napon[514] kihirdetett ítéletében a Bíróság megállapítja, hogy 2010/87 határozatnak az Alapjogi Chartára tekintettel történő vizsgálata nem tárt fel olyan tényezőt, amely e határozat érvényességét érintené. Ezzel szemben a Bíróság érvénytelennek nyilvánítja a 2016/1250 határozatot.

A Bíróság mindenekelőtt úgy ítéli meg, hogy az uniós jog és különösen a GDPR alkalmazandó a személyes adatoknak a valamely tagállamban letelepedett gazdasági szereplő által valamely harmadik országban letelepedett másik gazdasági szereplő részére kereskedelmi célból végzett továbbítására, még abban az esetben is, ha ezeket az adatokat e továbbítás során vagy azt követően az érintett harmadik ország hatóságai közbiztonsági, honvédelmi és nemzetbiztonsági célból kezelhetik. A Bíróság pontosítja, hogy a valamely harmadik ország hatóságai általi adatkezelés e típusa nem zárhatja ki az ilyen továbbítást a rendelet hatálya alól.

Az ilyen továbbítás keretében megkövetelt védelmi szint tekintetében a Bíróság úgy ítéli meg, hogy a GDPR rendelkezései által e célból előírt követelményeket, amelyek a megfelelő garanciákra, az érvényesíthető jogokra és a hatékony jogorvoslati lehetőségekre vonatkoznak, úgy kell értelmezni, hogy azon személyeknek, akiknek a személyes adatait az általános adatvédelmi kikötések alapján továbbítják harmadik országba, olyan védelmi szinttel kell rendelkezniük, amely lényegében azonos a Charta fényében értelmezett e rendelet által az Unióban biztosított védelmi szinttel. Ezzel összefüggésben a Bíróság kimondja, hogy e védelmi szint értékelésének figyelembe kell vennie mind az Unióban letelepedett adatkezelő és a továbbításnak az érintett harmadik országban letelepedett címzettje között létrejött szerződéses

[512] A 2016. december 16-i (EU) 2016/2297 bizottsági végrehajtási határozattal módosított, a 95/46 irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló, 2010. február 5-i 2010/87/EU bizottsági határozat

[513] A 95/46 irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről szóló, 2016. július 12-i (EU) 2016/1250 bizottsági végrehajtási határozat

[514] Az Európai Unió Bírósága 91/20. sz. SAJTÓKÖZLEMÉNY Luxembourg, 2020. július 16. A C-311/18. sz. ügyben hozott ítélet Data Protection Commissioner kontra Facebook Ireland és Schrems, https://naih.hu/kozlemenyek/EUB_sajtokozlemeny_cp200091hu.pdf, utolsó letöltés: 2022. 08. 30.

kikötéseket, mind pedig – e harmadik ország hatóságainak az így továbbított adatokhoz való esetleges hozzáférését illetően – az ezen ország jogrendszerének releváns elemeit.

Az ilyen továbbítással összefüggésben a felügyeleti hatóságokra háruló kötelezettségek kapcsán a Bíróság úgy ítéli meg, hogy e hatóságok – feltéve, hogy nem létezik a Bizottság által érvényesen elfogadott megfelelőségi határozat – többek között kötelesek felfüggeszteni vagy megtiltani a személyes adatok harmadik országba irányuló továbbítását, ha úgy vélik e továbbítás sajátos körülményeire tekintettel, hogy az általános adatvédelmi kikötéseket ebben az országban nem tartják be, vagy azokat ott nem lehet tiszteletben tartani, és hogy a továbbított adatok védelme, amelyet az uniós jog megkövetel, más eszközzel nem biztosítható, amennyiben az Unióban letelepedett adatkezelő maga nem függesztette fel vagy fejezte be az ilyen továbbítást.

A Bíróság ezt követően a 2010/87 határozat érvényességét vizsgálja. A Bíróság szerint e határozat érvényességét nem kérdőjelezi meg önmagában az, hogy az e határozatban szereplő általános adatvédelmi kikötések szerződéses jellegük miatt nem kötik azon harmadik ország hatóságait, amelybe az adatokat továbbíthatják. Ezzel szemben a Bíróság kimondja, hogy ez az érvényesség attól függ, hogy az említett határozat tartalmaz-e olyan hatékony mechanizmusokat, amelyek a gyakorlatban lehetővé teszik annak biztosítását, hogy az uniós jog által megkövetelt védelmi szintet tiszteletben tartsák, és hogy a személyes adatok ilyen kikötéseken alapuló továbbítását az e kikötések megsértése, illetve tiszteletben tartásuk lehetetlensége esetén felfüggesszék vagy megtiltsák. A Bíróság megállapítja, hogy a 2010/87 határozat ilyen mechanizmusokat alakít ki. E tekintetben többek között azt hangsúlyozza, hogy e határozat bevezeti az adatkezelő és az adattovábbítás címzettje azon kötelezettségét, hogy előzetesen ellenőrizzék, hogy az érintett harmadik országban tiszteletben tartják-e ezen védelmi szintet, és e címzettet arra kötelezi, hogy tájékoztassa az adatátadót arról, ha esetleg nem képes eleget tenni az általános adatvédelmi kikötéseknek, ez utóbbi pedig köteles felfüggeszteni az adattovábbítást és/vagy az előbbivel kötött szerződéstől elállni.

A Bíróság végül a 2016/1250 határozat érvényességét vizsgálja azokra a követelményekre tekintettel, amelyek a GDPR-ből következnek, utóbbit a Chartának a magán- és családi élet tiszteletben tartására, a személyes adatok védelmére és a hatékony bírói jogvédelemre vonatkozó rendelkezései fényében értelmezve. E tekintetben a Bíróság megállapítja, hogy e határozat a 2000/520 határozathoz hasonlóan a nemzetbiztonság, a közérdek és a bűnüldözés követelményeinek elsőbbségét fejezi ki, amely így lehetővé teszi a beavatkozást azon személyek alapvető jogaiba, akiknek az adatait az Unióból e harmadik országba továbbítják. A Bíróság szerint a személyes adatok védelmének korlátozásai, amelyek az Egyesült Államok azon belső szabályozásából erednek, amelyek az amerikai hatóságok által az Unióból e harmadik országba továbbított ilyen adatokhoz való hozzáférésre és azok felhasználására vonatkoznak, és amely korlátozásokat a Bizottság a 2016/1250 határozatban értékelt, nem úgy lettek szabályozva, hogy megfeleljenek az uniós jogban az arányosság elve által megkövetelt követelményekkel lényegében azonos követelményeknek, amennyiben az e szabályozáson alapuló megfigyelési programok nem a feltétlenül szükséges mértékre korlátozódnak. Az e határozatban

szereplő megállapítások alapján a Bíróság kimondja, hogy egyes megfigyelési programok esetében az említett szabályozásból semmilyen módon nem következik, hogy létezne az abban foglalt, e programok végrehajtására vonatkozó felhatalmazás korlátozása, sem pedig az, hogy fennállnának az esetlegesen érintett, nem amerikai személyek számára szóló garanciák. A Bíróság hozzáteszi, hogy bár ugyanez a szabályozás tartalmaz olyan követelményeket, amelyeket be kell tartaniuk az amerikai hatóságoknak az érintett megfigyelési programok végrehajtása során, nem biztosít az érintett személyek számára az amerikai hatóságokkal szemben a bíróságok előtt érvényesíthető jogokat.

A bírói jogvédelem létezése kapcsán a Bíróság úgy ítéli meg, hogy ellentétben azzal, amit a Bizottság a 2016/1250 határozatban megállapított, az e határozatban szereplő ombudsmani mechanizmus nem biztosít e személyek számára jogorvoslati lehetőséget olyan szerv előtt, amely az uniós jogban megkövetelt garanciákkal lényegében azonos garanciákat nyújtana, amelyek biztosíthatnák mind az e mechanizmus által előírt ombudsman függetlenségét, mind pedig az olyan normák meglétét, amelyek felhatalmazzák az említett ombudsmant arra, hogy az amerikai hírszerzési szervezetekkel szemben kötelező erejű határozatokat hozzon. Mindezen indokok alapján a Bíróság megállapítja a 2016/1250 érvénytelenségét."[515]

A bírósági ítélet után az EDPB kibocsátott egy iránymutatást,[516] mely a GDPR V. fejezete szerinti adattovábbításokkal kapcsolatos. Ezen iránymutatás leszögezi, hogy az V. fejezet rendelkezéseinek célja az, hogy a személyes adatok folyamatos védelme biztosítva legyen azt követően is, hogy azokat harmadik országba vagy nemzetközi szervezetnek továbbították. Amennyiben a személyes adatokat az EU területén kezelik, azokat nemcsak a GDPR védi, hanem más, uniós és tagállami szabályok is, amelyeknek összhangban kell lenniük a GDPR rendelkezéseivel (beleértve az abban foglalt esetleges eltéréseket) és végső soron az Európa Unió Alapjogi Chartájával is. Amikor azonban a személyes adatokat az Unió területén kívüli adatkezelők vagy adatfeldolgozók számára továbbítjuk és hozzáférhetővé tesszük, akkor az Unión belül biztosított jogszabályi környezet már nem alkalmazandó.

A francia adatvédelmi hatóság (CNIL) gyakorlatából:

2020 augusztusában a CNIL-hez panasz érkezett a panaszos személyes adatainak az Egyesült Államokba történő továbbításával kapcsolatban, amelyeket a bepanaszolt online kiskereskedelmi vállalat (kiskereskedő) weboldalának látogatása során gyűjtöttek.

[515] Az Európai Unió Bírósága 91/20. sz. SAJTÓKÖZLEMÉNY Luxembourg, 2020. július 16. A C-311/18. sz. ügyben hozott ítélet Data Protection Commissioner kontra Facebook Ireland és Schrems, https://naih.hu/kozlemenyek/EUB_sajtokozlemeny_cp200091hu.pdf, utolsó letöltés: 2022. 08. 30.

[516] Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international
transfers as per Chapter V of the GDPR Adopted on 18 November 2021, https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf, utolsó letöltés 2022. 08. 30.

A CNIL kérdőívet és kiegészítő információkérést küldött a kiskereskedőnek, amely a Google Analytics funkciót integráló, a kiskereskedő weboldalának francia nyelvű változatát látogatóktól származó adatok továbbításával volt kapcsolatos. A válasz szerint e szolgáltatáson keresztül szerzett statisztikák több tagállamban élő személyekre vonatkoznak, így ez az adatkezelés határokon átnyúló jellegű.

A CNIL az alábbiakat állapította meg:

- ✓ *az adatkezelés tartalma a kiskereskedő weboldalán a Google Analytics funkció integrálása a médiakampányok közönségének és teljesítményének mérése céljából. Ez a szolgáltatás lehetővé teszi a felhasználók nyomon követését azáltal, hogy egyedi azonosítójukat összekapcsolja az eszközükről indított munkamenetből származó adatokkal. Ezen információkat az Egyesült Államokban található Google Analytics szerverekre továbbítják.*
- ✓ *a kiskereskedő adatkezelőnek minősült ezen adatkezelés tekintetében, mivel ő határozta meg a Google Analytics weboldalán történő integrálása révén szerzett adatok gyűjtésének és kezelésének módját és célját.*
- ✓ *a kiskereskedő és a Google LLC között létrejött SCCs („általános szerződéses feltételek") nem nyújtanak megfelelő szintű védelmet, mivel:*
  - ✓ *a Google LLC [az 50 U.S. Code § 1881(b)(4) bekezdése szerint] „elektronikus hírközlési szolgáltatónak" minősül, és ezért az amerikai hírszerző szolgálatok megfigyelő tevékenységének ki van szolgáltatva, és*
  - ✓ *a Google által az SCCs kiegészítésére bevezetett szerződéses, szervezeti és technikai intézkedések nem megfelelőek, mivel nem tudják megakadályozni, hogy az amerikai hírszerző szolgálatok hozzáférjenek az érintett személyes adataihoz.*
  - ✓ *A CNIL elutasította a Google azon érvelését, miszerint a Google Analytics adatait álnevesítik, kiemelve, hogy az univerzális egyedi azonosítók nem felelnek meg a GDPR 4. cikkének (5) bekezdése szerinti álnevesítés fogalmának, mivel egyedüli céljuk a felhasználók azonosítása.*
- ✓ *a kiskereskedő nem hivatkozhat a GDPR V. fejezete szerinti egyéb továbbítási mechanizmusokra.*

Mindezek alapján a francia adatvédelmi hatóság úgy ítélte meg, hogy a kiskereskedő nem biztosított megfelelő szintű védelmet az általa kezelt személyes adatok nemzetközi továbbítása tekintetében és egy hónapot adott neki arra, hogy az adatkezelését összhangba hozza a GDPR-ral, szükség esetén a személyes adatoknak a Google Analytics jelenlegi verziója szerinti kezelésének megszüntetésével.[517]

Miután a CNIL benyújtotta a határozattervezetet az érintett hatóságoknak (GDPR 60. cikk), egyikük sem emelt indokolással ellátott kifogást. Ez azt jelezheti, hogy

[517] https://www.cnil.fr/sites/default/files/atoms/files/med_google_analytics_anonymisee.pdf, utolsó letöltés: 2022.

várhatóan a jövőben a hasonló ügyek hasonló kimenetelűek lesznek, példa erre az osztrák adatvédelmi hatóság hasonló határozata.[518]

Mindezeket figyelembe véve biztosítanunk kell, hogy az átadott személyes adatokat más módon védjék, például az Európai Bizottság megfelelőségi határozatával összefüggésben történő továbbítással vagy a GDPR V. fejezetével összhangban megfelelő garanciák nyújtásával.

Ha a GDPR 46. cikkében felsorolt adattovábbítási eszközök valamelyikére támaszkodunk, abban az esetben meg kell vizsgálnunk, hogy szükséges-e kiegészítő intézkedések végrehajtása annak érdekében, hogy az átadott adatok védelmi szintje elérje az alapvető egyenértékűség uniós szabványát. Ez az eset állhat fenn például akkor, amikor harmadik ország személyes adatokhoz való kormányzati hozzáférésre vonatkozó szabályai túlmutatnak azon, ami egy demokratikus társadalomban szükséges és arányos – a GDPR V. fejezet rendelkezései ezt a kockázatot hivatottak ellensúlyozni.

A bajor adatvédelmi hatóság („Bayrisches Landesamt für Datenschutzaufsicht" – BayLDA) gyakorlatából

A BayLDA úgy ítélte meg, hogy egy német vállalat részéről a Mailchimp hírlevél-eszköz használata jogellenes volt, mivel a Mailchimp megkapja a hírlevélre feliratkozók e-mail címeit, miközben a Mailchimp az amerikai felügyeleti jog szerint „elektronikus hírközlési szolgáltatónak" minősülhet.

A panaszos panasza szerint a német vállalat hírlevelére feliratkozók e-mail címeinek a Mailchimp szolgáltatójának (The Rocket Science Group LLC, USA) történő átadása a GDPR 44. és azt követő cikkek alapján jogellenes volt.

A BayLDA megállapította, hogy a Mailchimp használata és így az e-mail címek átadása a Mailchimp szolgáltatójának jogellenes volt, mivel

- ✓ *az adattovábbítás az uniós szabványos adatvédelmi záradékokon (Standard Contractual Clauses – SCC) alapult;*
- ✓ *vannak arra utaló jelek, hogy a Mailchimp szolgáltatója az amerikai megfigyelési törvény [FISA702 (50 U.S.C. § 1881)] szerint „elektronikus hírközlési szolgáltatónak" minősül, ez pedig az átadott e-mail címeket veszélyeztetheti, mivel az amerikai hírszerző szolgálatok hozzáférhetnek;*
- ✓ *az EUB „Schrems II" (C-311/18) határozatára figyelemmel az alperes elmulasztotta felmérni, hogy szükségesek-e további intézkedések annak biztosítására, hogy az átadott adatok védve legyenek az amerikai megfigyeléssel szemben.*

Mivel a bepanaszolt vállalat kijelentette, hogy azonnali hatállyal tartózkodik a Mailchimp használatától, a BayLDA nem szabott ki bírságot.[519]

[518] DSB (Austria) – 2021-0.586.257 (D155.027) https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk_0.pdf. Utolsó letöltés 2022. 08. 09.
[519] LDA-1085.1-12159/20-IDV, BayLDA 15 March 2021

Harmadik országba adattovábbítás – különös helyzetek

Előfordulhat, hogy a személyes adatok harmadik országba továbbítására úgy van szükségünk**,** hogy nem áll rendelkezésünkre se megfelelőségi határozat se megfelelő garancia. Az ilyen esetekre ad kivételes lehetőséget a GDPR 49. cikke „különös helyzetekben biztosított eltérések" formájában. Ez alapján továbbíthatjuk a személyes adatot például akkor, amikor

- ✓ az érintett kifejezetten hozzájárulását adja a tervezett továbbításhoz azt követően, hogy tájékoztattuk az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról;
- ✓ az adattovábbítás köztünk és az érintett közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, a szerződést megelőző intézkedések végrehajtásához szükséges;
- ✓ az adattovábbítás az adatkezelő és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;
- ✓ az adattovábbítás fontos közérdekből szükséges;
- ✓ az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;
- ✓ az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására;
- ✓ a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja, és amely vagy általában a nyilvánosság, vagy az ezzel kapcsolatos jogos érdekét igazoló bármely személy számára betekintés céljából hozzáférhető, de csak ha az uniós vagy tagállami jog által a betekintésre megállapított feltételek az adott különleges esetben teljesülnek.

Ha az adattovábbítás nem alapulhat a már említett megfelelőségi határozaton vagy garanciákon, illetve az egyedi helyzetekre vonatkozó eltérések egyike sem alkalmazható, harmadik országok és nemzetközi szervezetek részére történő adattovábbítást csak akkor végezhetünk, ha az adattovábbítás

- ✓ nem ismétlődő,
- ✓ csak korlátozott számú érintettre vonatkozik,
- ✓ adatkezelőként olyan kényszerítő erejű jogos érdekünkben szükséges, amely érdekhez képest nem élveznek elsőbbséget az érintett érdekei, jogai és szabadságai, és
- ✓ az adattovábbítás minden körülményét megvizsgáltuk, és e vizsgálat alapján megfelelő garanciákat nyújtottunk a személyes adatok védelme tekintetében.

Ebben az esetben tájékoztatnunk kell a felügyeleti hatóságot az adattovábbításról és tájékoztatnunk kell az érintetteket is az adattovábbításról, valamint a kényszerítő erejű jogos érdekünkről.

A kivételes eset tényleg csak kivételes lehet, azaz nem használhatjuk a kivételes helyzetet visszatérő jelleggel (sorozatosan).

A harmadik fél részére továbbított adat (függetlenül attól, hogy GDPR hatálya vonatkozik-e rá) mindig kiemelt kockázatot jelent. Erre jelenleg a legjobb példa az orosz-ukrán válság során felmerült adatbiztonsági incidens lehetősége – a személyes adatok nagyméretű gyűjtésének kérdése több esetben is megjelent, többek között sajtóinformációk szerint a Sberbanktól is kerültek ki személyes adatok a konfliktus kitörését követő időszakban. A médiában megjelent információk alapján a Google engedélyezte egy szankcionált orosz reklámcégnek, hogy hónapokig gyűjtsön felhasználói adatokat. A Google a Sberbank tulajdonában lévő RuTargetet egyedi mobiltelefon-azonosítókkal, IP-címekkel, helyadatokkal, valamint a felhasználók érdeklődési köréről és online tevékenységéről információkkal látta el (feltehetően 2022. június 23-án osztotta meg ezeket a potenciálisan érzékeny felhasználói adatokat a szankcionált orosz reklámtechnológiai vállalattal). Kockázati tényezőként a következő azonosítható:

- ✓ *a felhasználók személyes adatai (név, cím, pénzügyi adatok, keresési előzmények, érdeklődési kör stb.) kiszivárogtak és ismeretlen felhasználókhoz kerültek;*
- ✓ *a reklámcég a személyes adatokat továbbította a Sberbank rendszerébe és onnan kiegészítve a banki adatokkal esetleg orosz kormányzati rendszerbe került az információ.*

GDPR

- ✓ A személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása [GDPR V. fejezet]

ADATVÉDELEM ÉS ADATBIZTONSÁG – TECHNIKAI ÉS SZERVEZETI INTÉZKEDÉSEK, ESZKÖZÖK

A kiberbiztonság öt törvénye

1. Ha van egy sebezhetőség, azt ki fogják használni	*1. Kezelj mindent úgy, mintha sebezhető lenne*
2. Minden sebezhető valamilyen módon	*2. Feltételezd, hogy az emberek nem fogják betartani a szabályokat*
3. Az emberek akkor is bíznak, amikor nem kellene	*3, Ha nincs rá szükséged, szabadulj meg tőle*
4. Az innovációval együtt jár a kihasználhatóság lehetősége is	*4. Mindent dokumentálj és rendszeresen auditálj*
5. Ha kétségeid vannak, lásd az 1. pontot	*5. Tervezz kudarc esetére*
Nick Espinosa (2018)[520]	*Martin Banks (2021)*[521]

Adatbiztonság – a CIA-elv

Az adatbiztonság az információs rendszer olyan kedvező állapota, amelyben a kezelt adatok bizalmassága (**C**onfidentiality), sértetlensége (**I**ntegrity) és rendelkezésre állása (**A**vailability) biztosított (**CIA-elv**), valamint a rendszer elemeinek biztonsága szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

Az adatbiztonság követelményei:

- ✓ **bizalmasság**: egy adott információt (adatot) csak az arra jogosultak tudhatnak meg. A gyakorlatban ez azt az elvárást jelenti, miszerint illetéktelen személy csak irreálisan nagy erőbefektetéssel, költséggel, vagy irreálisan kis valószínűséggel legyen képes az adott információhoz hozzájutni. A bizalmasság biztosítása érdekében például olyan hozzáférés-védelmi rendszereket (beléptető rendszer, jogosultság szabályzás, fizikai akadályok stb.) és/vagy rejtjelezési eljárásokat vethetünk be, amelyek gyakorlatilag kizárják az illetéktelen személy hozzáférését az adott információhoz, legyen az akár üzleti titok, akár védendő személyes adat. A bizalmasság kérdése megosztja a szakértőket, a jogászokat és a műszaki szakembereket, mivel egyes technológiai ágazatoknál a rendszerekben kezelt személyes adatok bizalmassága nem élvez prioritást, míg más adatok bizalmassága fontosabb. Azonban vannak olyan ágazatok, mint például az egészségügy, ahol a személyes és különleges személyes adatok kezelése elsődleges.
- ✓ **sértetlenség:** egy adott információt (adatot) vagy rendszert csak az arra jogosultak változtathatnak meg. Mivel az elektronikus adatok módosításának teljeskörű megakadályozása gyakorlati nehézségekbe ütközhet, adatkezelőként a hangsúly a sértetlenség tekintetében a módosítás észlelésére, detektálására is helyezhetjük.

[520] The Five Laws Of Cybersecurity, https://www.forbes.com/sites/forbestechcouncil/2018/01/19/the-five-laws-of-cybersecurity/?sh=e0583c02265a, utolsó letöltés: 2022. 08. 29.
[521] A Closer Look at the 5 Laws of Cybersecurity, https://cybersecuritymagazine.com/a-closer-look-at-the-5-laws-of-cybersecurity/, utolsó letöltés: 2022. 08. 29.

A sértetlenség követelményéhez szorosan kapcsolódik az adat-konzisztencia, a hitelesség és letagadhatatlanság is. A Stuxnet támadása után megváltozott a világ, kételyek merültek fel azzal kapcsolatban, hogy a SCADA rendszerben tárolt adatok valósnak és hitelesnek tekinthetőek-e. Az ICS[522] és ICT[523] rendszerek esetén is megnőtt a sértetlenség fontossága, bár mind a mai napig vannak, akik ezt a kérdést nem kezelik súlyának megfelelően. Az ICT rendszerek esetében ez kiemelt prioritással bír, hiszen ezekben a rendszerekben személyes adatok nagy mennyiségét kezelik.

- ✓ **rendelkezésre állás**: egy adott rendszernek az elvárt megbízhatósággal kell ellátnia a feladatát. Ennek mérésére objektív statisztikai jellemzőket használhatunk, mint például üzemidő, rendelkezésre-állási tényező és sebezhetőségi ablak. Adatkezelőként lehetnek olyan rendszereink, amelyek kiesése még rövid időtartamra is nagy kockázattal jár (például egy kórház informatikai rendszere), míg más rendszerek esetében hosszabb kihagyás sem okozhat jelentős problémát. Fontos az is, hogy ez ágazatonként is eltér, azaz például ICS rendszerek esetében ez a legfontosabb szempont.

A CIA követelmények teljesítése érdekében három nagy területen tehetünk biztonsági intézkedéseket

- ✓ *fizikai (mechanikai védelem, elektronikai jelzőrendszer, élőerős védelem, beléptető rendszer, biztonsági kamera rendszer, villám és túlfeszültség védelem, tűzvédelem),*
- ✓ *logikai (azonosítás és a hitelesítés, hozzáférés-védelmi rendszer stb.) és*
- ✓ *adminisztratív (szervezési, szabályozási, ellenőrzési intézkedések, védelemre vonatkozó oktatás stb.).*

A biztonsági intézkedések megléte, illetve hiánya különösen akkor kap nagy hangsúlyt, ha adatvédelmi incidens történik.

A lengyel adatvédelmi hatóság (UODO) gyakorlatából

Az UODO a Fortum Marketing Sales Polska S.A.-t („Fortum”) mint adatkezelőt és a PIKA Spółka z o.o.-t („PIKA) mint adatfeldolgozót mintegy 1 millió euró, illetve 53 ezer euró összegű közigazgatási bírsággal sújtotta az adatok bizalmas kezelésének megsértése és a megfelelő biztonsági intézkedések hiánya miatt.

A Fortum villamosenergiával és üzemanyaggal kereskedik, beleértve a végfelhasználóknak történő értékesítést, mind az üzleti szektor, mind a háztartások számára, mely során együttműködik az archiválási szolgáltatásokat (beleértve a digitális archívumot is) nyújtó PIKA-val. A két cég között 2016-tól tárolási (dokumentumarchívum) megállapodás van, 2018-tól adatfeldolgozási megállapodás is hatályban van.

[522] Industrial Control System
[523] Information Communication Systems

A Fortum adatvédelmi incidensről értesítette az UODO-t, amelyben a cég bejelentése alapján 137 314 ügyfél adatait másolták le. Az egy újonnan létrehozott adatbázist érintett, amelytöbbek között olyan ügyfél-adatokat tartalmazott, mint a név és vezetéknév, lakóhely vagy tartózkodási cím, személyazonosító okmány adatai, e-mail cím, telefonszám, valamint szerződéses adatok.

A Fortum nem értesítette az érintetteket az adatvédelmi incidensről, mivel értékelése szerint az incidens nem járt valószínűsíthetően magas kockázattal a természetes személyek jogaira és szabadságaira nézve.

Az eljárás során kiderült, hogy a PIKA, mint adatfeldolgozó szintén érintett az adatvédelmi incidensben. A PIKA elmondta, hogy a rendszerek módosítása esetén az informatikai részlegének egyes területei kötelesek a rendszerekben végrehajtott változtatásokat a belső projektmenedzsment-támogató és ellenőrző rendszereikben rögzíteni. A rendszer módosításakor a Fortum ügyfeleinek tényleges személyes adatait használták fel és az alkalmazott biztonsági funkciók hatékonyságát nem ellenőrizték, mielőtt a rendszer módosításait a Fortumhoz továbbították volna a teljesítményprobléma megoldása érdekében.

Az UODO véleménye szerint:

- ✓ *az EN ISO/IEC 27002:2017-06 szabvány szerint ajánlott elkerülni a személyes vagy egyéb érzékeny adatok tesztadatként való felhasználását. Ha személyes adatokat használnak a tesztelés során, ajánlott az összes érzékeny adatot és kontextust törléssel vagy módosítással védeni. Amennyiben valós adatokat használnak tesztelési célokra, a tesztelt alkalmazásokban ugyanazokat a hozzáférés-ellenőrzési eljárásokat kell alkalmazni, mint a valós rendszerekben.*
- ✓ *a PIKA az adatfeldolgozási megállapodásban foglaltakkal ellentétesen járt el, amely többek között előírta az adatok álnevesítésének végrehajtását. A PIKA a személyes adatok védelme érdekében alkalmazandó biztonsági intézkedések meghatározásakor nem alkalmazott olyan intézkedéseket, amelyek az aktuális biztonsági szabványokat tükrözik.*
- ✓ *az adatfeldolgozó alkalmazása nem mentesíti a Fortumot a kötelezettségei tekintetében. Jelen esetben a Fortum számára fontosabb volt a rendszer kapacitásának mielőbbi növelése, mint az e rendszer segítségével kezelt személyes adatok megfelelő szintű biztonságának biztosítása, ez pedig a bizalmasság és az integritás elvének a megsértéséhez vezetett.*
- ✓ *a GDPR adatfeldolgozásra vonatkozó rendelkezései szerint az adatkezelő csak olyan adatfeldolgozók szolgáltatásait veheti igénybe, akik megfelelő garanciákat nyújtanak a megfelelő technikai és szervezési intézkedések végrehajtására annak érdekében, hogy az adatkezelés megfeleljen a GDPR követelményeinek és védje az érintettek jogait. Jelen esetben a Fortum nem ellenőrizte a PIKA-t az adatfeldolgozásra vonatkozó megállapodás megkötése előtt. A Fortum elmondta, hogy évek óta együttműködik a PIKA-val, és eddig nem történt biztonsági incidens, valamint a PIKA piacvezető az általa nyújtott szolgáltatások tekintetében, és magas színvonalat képvisel az archiválás és a digitalizálás terén. A fentiekre tekintettel a Fortum elegendőnek tartotta az adatfeldolgozási megállapodás aláírását a megállapodás függelékében feltüntetett rendelkezésekkel együtt.*

- ✓ *a Fortum nem gyakorolta a GDPR által biztosított ellenőrzési jogát a PIKA biztonsági intézkedéseivel kapcsolatban.*
- ✓ *mivel az adatkezelés az adatkezelő nevében történt, az adatkezelő csak olyan adatfeldolgozó szolgáltatásait vehette volna igénybe, aki megfelelő garanciákat nyújt a megfelelő technikai és szervezési intézkedések végrehajtására vonatkozóan. A felek olyan hosszú távú együttműködése, amelyet nem támasztanak alá rendszeres auditok vagy ellenőrzések, nem garantálja, hogy az adatfeldolgozó megfelelően látja el a feladatait. A múltban pozitívan értékelt együttműködés csak kiindulópont lehet annak ellenőrzésénél, hogy az adatfeldolgozó elegendő garanciát nyújt-e a megfelelő technikai és szervezési intézkedések végrehajtására. A személyes adatok feldolgozására vonatkozó megállapodás puszta aláírása az adatfeldolgozó megfelelő értékelése nélkül nem tekinthető az adatfeldolgozónak a GDPR követelményeinek való megfelelésére vonatkozó ellenőrzési eljárás lefolytatására vonatkozó kötelezettség teljesítésének. Egy adott adatfeldolgozóval 2018. május 25. előtt, azaz a GDPR alkalmazása előttre visszanyúló hosszútávú együttműködés szintén nem mentesíti az adatkezelőt az ilyen értékelés elvégzésének kötelezettsége alól.*
- ✓ *a Fortum jelen esetben nem végzett ilyen ellenőrzést, hanem megelégedett a korábbi együttműködésből származó pozitív értékeléssel („nem történt biztonsági incidens”).* [524]

A OUDO azt ajánlja, hogy adatkezelőként – mielőtt a nekünk szolgáltatást végzőkre bíznánk feldolgozás céljára a személyes adatokat – fordítsunk különös figyelmet az ellenőrzésükre, valamint az együttműködés során is folyamatosan ellenőrizzük az adatfeldolgozás megfelelőségét.

Adatbiztonság – intézkedések

Adatkezelőként a GDPR elvárása alapján megfelelő technikai és szervezési intézkedéseket kell tennünk annak érdekében, hogy a kockázat mértékének megfelelő adatbiztonságot garantáljuk. A megfelelő adatbiztonság kialakítása során figyelemmel kell lennünk a tudomány és technológia állására és a megvalósítás költségeire, továbbá az adatkezelés jellegére, hatókörére, körülményeire és céljaira, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatokra.

Adatbiztonsági intézkedés lehet például

- ✓ *a személyes adatok álnevesítése és titkosítása,*
- ✓ *a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének, integritása, rendelkezésre állása és ellenálló képessége biztosítása,*
- ✓ *fizikai incidens esetén az arra való képesség, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza*

[524] DKN.5130.2215.2020, https://www.uodo.gov.pl/decyzje/DKN.5130.2215.2020, utolsó letöltés: 2022. 08. 09.

lehessen állítani, vagy redundáns rendszereket biztosítsunk a személyes adatok védelme tekintetében,

- ✓ *az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárás, valamint visszacsatolás a mért eredmények és a rendszerfejlesztések között, azaz a mért eredmények szolgáljanak alapul a jövőbeni fejlesztésekhez.*

A GDPR nem fogadja el azt a kifogást, hogy nem volt pénzügyi fedezet a biztonsági intézkedésekre, hanem elvárja, hogy adatkezelőként üzleti költségként tekintsünk az adatvédelem és az adatbiztonság költségeire.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„Adatbiztonsági szempontból a Hatóság nem tartja megfelelő gyakorlatnak, ha a jelszavakat a felhasználók nem egy előre meghatározott olyan magasabb biztonsági követelményeket felállító szabályrendszer szerint kötelesek kitalálni, amelyet az adott rendszer ki is kényszerít a jelszó megadása során (pl. jelszó kötelező hossza, kötelezően megadandó különleges karakterek stb.). Ennek oka, hogy nem megfelelően erős jelszóvalidálási rendszer esetén a felhasználók jellemzően minél egyszerűbb és rövidebb jelszavakat fognak használni. Az egyszerűbb jelszavakat azonban könnyebben tudja egy külső támadó visszafejteni, vagy kikövetkeztetni.”[525]

Adatkezelőként a biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell vennünk az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok

- ✓ véletlen vagy jogellenes megsemmisítéséből,
- ✓ elvesztéséből,
- ✓ megváltoztatásából,
- ✓ jogosulatlan nyilvánosságra hozatalából, vagy
- ✓ az azokhoz való jogosulatlan hozzáférésből erednek.

Ezen kívül intézkedéseket kell hoznunk annak biztosítására, hogy az irányításunk alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag a mi utasításainknak megfelelően kezelhessék az adatokat.

Dán felügyeleti hatóság (Datatilsynet) gyakorlatából

A dán adatvédelmi hatóság 6 700 eurós bírságot javasolt egy önkormányzat ellen, mert az nem akadályozta meg, hogy alkalmazottjai manuálisan letiltsák a polgárok személyes adatait tartalmazó mobiltelefonjaik hozzáférési kódjait, és ezzel szükségtelen kockázatnak tették ki az érintetteket.

Az adatvédelmi hatóság azután szerzett tudomást az ügyről, hogy az önkormányzat bejelentést tett, amikor egy alkalmazottnak ellopták a munkahelyi telefonját. A telefon nem volt hozzáférési kóddal védve, mivel azt a munkavállaló kézzel kikapcsolta, és így hozzáférhettek a munkavállaló munkahelyi e-mail fiókjához,

[525] NAIH/2019/2668/2

amely több polgár nevére, társadalombiztosítási számára, egészségügyi adataira és kábítószerrel való visszaélésre vonatkozó információkat tartalmazott.

Az önkormányzat arról is tájékoztatta az adatvédelmi hatóságot, hogy az alkalmazottak több éven keresztül manuálisan letilthatták az egyébként kötelező hozzáférési kódot. Az incidenst követően az önkormányzat azonnal korrekciós intézkedéseket hozott a védelem érdekében.

A dán adatvédelmi hatóság megállapította, hogy

- ✓ *az önkormányzat személyes adatok kezeléséra vonatkozó eljárása megsértette a megfelelő biztonsági intézkedésekre vonatkozó szabályokat;*
- ✓ *az adatkezelőnek abból kell kiindulnia, hogy nem minden alkalmazott fogja betartani a vonatkozó belső szabályokat, ezért a valódi és hatékony védelem olyan biztonsági intézkedéseken múlik, amelyeket nem lehet megkerülni, ilyen például a hozzáférési kódok kényszerített használata;*
- ✓ *az önkormányzat felelőtlenül járt el, mivel a polgárok személyes adatait szükségtelen kockázatnak tette ki a készülékek elégtelen biztonsági intézkedései miatt.* [526]

Bármilyen fájdalmas a ráeszmélés, ki kell szakadnunk abból az illúzióból, hogy az adatbiztonság pusztán a megfelelő berendezések – hardver és szoftver – meglétével érhető el, ugyanis az adatbiztonsághoz (információvédelemhez) megfelelő belső szervezeti szabályok is szükségesek, illetve ezek következetes betartása és betartatása.

Példa

- ✓ *valamennyi munkavállalónkat rendszeres tájékoztatjuk az adatbiztonsági szabályokról, valamint a munkavállalóként az adatvédelmi jog alapján fennálló kötelezettségeikről, különösen a titoktartási kötelezettségről,*
- ✓ *megköveteljük a világos feladatkör-megosztást és a hatáskörök egyértelmű meghatározását adatkezelési kérdésekben, különösen a személyes adatok kezelésére és a harmadik személynek vagy érintetteknek történő továbbítására irányuló döntésekkel kapcsolatban,*
- ✓ *a személyes adatok kizárólag az általunk meghatározott illetékes személy utasításai vagy az általánosan elfogadott szabályok szerint használhatók fel,*
- ✓ *intézkedéseket teszünk a saját, illetve az adatfeldolgozóink hivatalos helyiségeihez, valamint hardvereihez és szoftvereihez való hozzáférés védelme érdekében, a hozzáférési engedélyek ellenőrzését is beleértve,*
- ✓ *leszabályozzuk, hogy a személyes adatokhoz való hozzáférési engedélyt mindig az általunk meghatározott illetékes személy adja ki, és az engedély megadásához megfelelő dokumentálást is előírjuk,*
- ✓ *lehetővé tesszük az automatizált protokollok rendszeres ellenőrzését,*

[526] Lolland Kommune indstilles til bøde, https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/aug/lolland-kommune-indstilles-til-boede, utolsó letöltés: 2022. 08. 18.

- ✓ *biztosítjuk, hogy az automatizált hozzáférésen kívüli más közlési formák alapos dokumentálása is kötelező legyen annak igazolására, hogy nem történt jogellenes adattovábbítás.*

A munkavállalók adatbiztonsággal kapcsolatos képzése szintén a hatékony biztonsági óvintézkedések egyik fontos eleme, és nemcsak oktatnunk, hanem ellenőrzési eljárásokat is alkalmaznunk kell annak biztosítására, hogy a megfelelő intézkedések ne csupán papíron létezzenek, hanem a nevünkben adatkezelést végzők a gyakorlatban is végrehajtsák azokat és azok ténylegesen is működjenek (pl. belső vagy külső ellenőrzések).

A kutatásunk bebizonyította, hogy a megkérdezettek egy jelentősebb része nincs tisztában saját munkakörnyezetében és a digitális térben az adatbiztonság fogalmával. A katonai szervezeteknél az is megállapítható, hogy a katonai vezetők tisztában vannak az adatbiztonság fogalmának tartalmával, fontosságával és bíznak a szervezetszerű adtavédelmi megoldásokban.

Az EDPB iránymutatásában[527] az alábbi intézkedéseket, jó gyakorlatokat javasolja az adatkezelők és adatfeldolgozók számára, figyelembe véve a GDPR 25. cikkében foglalt követelményeket:

- ✓ már az adatkezelési művelet tervezésének kezdeti szakaszaitól kezdve, még az adatkezelés módjának meghatározása előtt gondolnunk kell az adatvédelemre;
- ✓ amennyiben van adatvédelmi tisztviselőnk, érdemes aktív szerepet vállalnia a beépített és alapértelmezett adatvédelem beszerzési és fejlesztési folyamataiban, valamint az adatkezelés teljes életciklusába történő beépítésében;
- ✓ a 18 év alatti gyermekek és más kiszolgáltatott csoportok esetében külön védelmet kell biztosítanunk a beépített és alapértelmezett adatvédelemnek való megfelelés érdekében;
- ✓ nem választhatunk olyan szolgáltatókat vagy adatfeldolgozókat, amelyek nem kínálnak olyan rendszereket, amelyek lehetővé teszik vagy elősegítik számunkra a GDPR 25. cikkének való megfelelést, mivel felelősek vagyunk ezen cikk végrehajtásának elmulasztása miatt;
- ✓ a szolgáltatóknak és adatfeldolgozóknak aktív szerepet kell játszaniuk annak biztosításában, hogy „a tudomány és technológia állására" vonatkozó kritériumok teljesüljenek, és értesíteniük kell minket „a tudomány és technológia állásának" minden olyan változásáról, amely befolyásolhatja a meglévő intézkedéseink hatékonyságát. Ezt a követelményt szerződéses kikötésként is szerepeltetnünk kell a megállapodásainkban annak érdekében, hogy a naprakészségünk biztosítható legyen;
- ✓ tisztességesnek kell lenniünk az érintettekkel szemben, valamint átláthatónak azzal kapcsolatban, hogy milyen módon értékeljük és bizonyítjuk a beépített

[527] [527] 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről 2.0 változat, Elfogadás időpontja: 2020. október 20., https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_hu.pdf, utolsó letöltés 2022. 08. 01.

és alapértelmezett adatvédelem hatékony megvalósítását, ugyanúgy, ahogyan az elszámoltathatóság elve alapján igazoljuk az általános adatvédelmi rendeletnek való megfelelést;

- ✓ a magánélet védelmét erősítő, már kiforrott, korszerű technológiákat is alkalmazhatjuk a beépített és alapértelmezett adatvédelem követelményeinek való megfelelést szolgáló intézkedésként, amennyiben a kockázatalapú megközelítés szerint megfelelőnek bizonyulnak;
- ✓ a már meglévő korábbi rendszereinkre a beépített és alapértelmezett adatvédelem ugyanazon követelményei vonatkoznak, mint az új rendszereinkre. Ha egy korábbi rendszerünk még nem felel meg a beépített és alapértelmezett adatvédelem követelményének, és nem hajthatók végre a kötelezettségek teljesítését lehetővé tevő változtatások, a korábbi rendszer ebben az esetben nem felel meg az általános adatvédelmi rendelet szerinti követelményeknek, és így nem használható személyes adatok kezelésére;
- ✓ a GDPR 25. cikk nem állapít meg enyhébb követelményeket a kkv-k számára, nekik megoldás lehet például az igazolt referenciákkal rendelkező partnerekkel együttműködés, illetve az adatvédelmi hatósággal konzultáció.

GDPR

- ✓ Az adatkezelés biztonsága [GDPR 32. cikk (83) és (74)-(77) preambulumbekezdések]

SZANKCIÓK

Általános tapasztalat, hogy a szereplőket nehéz úgy jogkövető magatartásra bírni, hogy a jogalkotó nem helyez kilátásba szankciót a szabályok megsértése esetére. A GDPR esetén a büntetés alapja az adatkezelő, illetve adatfeldolgozó éves árbevétele, így a felügyeleti hatóság a bírság kiszabásánál maximális mértékben figyelembe tudják venni a jogszerűtlenül eljáró gazdasági súlyát, piaci dominanciáját.

Kutatásunk során bizonyítást nyert az a tény,[528] hogy a megkérdezettek alapvetően a retorziót említették, mint egyetlen olyan garanciát, amely biztosítja a személyes adataik megfelelő szintű védelmét, leginkább azért, mert jelenleg nincs lehetőségük arra, hogy az adatkezelőket ellenőrizni tudják (erre jelenleg megállapításunk szerint technológiai megoldás nem áll rendelkezésre).

A GDPR felhatalmazza a tagállamok felügyeleti hatóságait, hogy közigazgatási bírságot szabjanak ki, amelynek nagysága attól függ, hogy a rendelet mely cikkeit sértette meg az adatkezelő, illetve az adatfeldolgozó. A bírság összege legfeljebb 20 millió euró, illetve vállalkozások esetében azok teljes éves világpiaci forgalmának legfeljebb 4%-át kitevő összeg lehet attól függően, hogy melyik érték magasabb.[529]

A 29. cikk alapján létrehozott adatvédelmi munkacsoport gyakorlatából

„Végső soron a vállalatot vagy szervet kell felelősnek tekinteni az adatfeldolgozásért és az adatvédelmi jogszabályokból eredő kötelezettségekért, kivéve, ha egyértelmű elemek utalnak arra, hogy egy természetes személy a felelős. […] Azonban az ilyen esetekben is, amikor konkrét természetes személyt neveznek ki, hogy biztosítsa az adatvédelmi elvek betartását vagy hogy személyes adatokat dolgozzon fel, ez a személy nem lesz adatkezelő, hanem annak a jogi személynek (vállalatnak vagy köztestületnek) a nevében jár el, amely adatkezelői minőségében továbbra is felelős az alapelvek megsértése esetén."[530]

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A Hatóság álláspontja szerint az ügyintézői hibára vonatkozó érvelés nem mentesíti a Kérelmezettet az adatkezelői felelősség alól, tekintettel arra, hogy az általános adatvédelmi rendelet 4. cikk 7. pontja értelmében a Kérelmezett minősül adatkezelőnek és nem a munkavállalói. A Kérelmezett az, aki megszervezi az adatkezelés folyamatát és kialakítja annak körülményeit, nem pedig az ügyintézők. Az adatkezelő legfontosabb jellemzője az, hogy érdemi döntéshozatali jogkörrel rendelkezik, és felelősséggel tartozik az adatkezelés valamennyi, az általános adatvédelmi rendeletben rögzített kötelezettség teljesítéséért. (…) Az ügyintéző által

[528] a megkérdezettek több mint 90%, az 1/A és 1/B kérdőíveken.
[529] GDPR 83. cikk (5) bekezdés
[530] 1/2010. számú vélemény az „adatkezelő" és az „adatfeldolgozó" fogalmáról, 00264/10/HU WP 169, Elfogadás időpontja: 2010. február 16., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_hu.pdf, utolsó letöltés 2022. 07. 28.

végrehajtott téves adatrögzítés ténye tehát nem minősül kimentési oknak, ebben az esetben is az adatkezelő viseli a felelősséget."[531]

Ezzel, azaz az emelt mértékű bírsággal sújtható az adatkezelés elveinek, illetve a hozzájárulás feltételeinek, az érintettek jogainak, valamint a rendelet személyes adatok harmadik országbeli címzett részére történő továbbítására vonatkozó rendelkezéseinek megsértése. Egyéb, „kisebb" jogsértések esetén a felügyeleti hatóságok legfeljebb 10 millió euró vagy a vállalkozás esetén teljes éves világpiaci forgalmának legfeljebb 2%-át kitevő összeget szabhatnak ki attól függően, hogy melyik érték a magasabb.[532]

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

„A bírságkiszabással a Hatóság speciális prevenciós célja az, hogy ösztönözze a Kérelmezettet arra, hogy adatkezelési tevékenységét, tevékenységeit tudatosan folytassa, és az érintetteket ne tárgyként, hanem valóban jogosultként kezelje, biztosítva az ebből eredő jogaik, a személyes adataik kezelése feletti kontroll gyakorlásához szükséges információkat, egyéb feltételeket.

Általában pedig szükséges valamennyi hasonló helyzetben lévő adatkezelő számára világossá tenni, hogy a személyes adatok kezelése fokozott tudatosságot igényel, nem lehet e téren a józan belátásra hagyatkozva bármilyen proaktív intézkedések megtétele nélkül működni, gondatlanul bízva abban, hogy nem származik hátrány a személyes adatok ténylegesen kontrollálatlan kezeléséből. Az ilyen hanyag magatartás az érintettek jogait figyelmen kívül hagyja, és mint ilyen, nem maradhat szankcionálatlanul."[533]

A WP 29. cikk szerint adatvédelmi munkacsoport 2017-ben kiadott egy iránymutatást a közigazgatási bírság alkalmazásáról és megállapításáról,[534] ezen dokumentum kiegészítéséül – a büntetési gyakorlat harmonizálása érdekében – az EDPB 2022. májusában társadalmi egyeztetésre bocsátott egy újabb iránymutatást.[535]

Az új iránymutatás megerősíti, hogy a bírság összegének kiszámítása a felügyeleti hatóságok mérlegelési jogkörébe tartozik, a GDPR cikkeinek figyelembevételével:

- ✓ a bírság összegének minden egyes esetben hatékonynak, arányosnak és visszatartó erejűnek kell lennie [GDPR 83. cikk (1) bekezdés],

[531] NAIH-55-11/2022., https://naih.hu/hatarozatok-vegzesek/file/540-uzleti-titokra-valo-hivatkozassal-hanganyag-korlatozott-felhasznalhatosaggal-torteno-rendelkezesre-bocsatasa, utolsó letöltés: 2022. 07. 28.
[532] GDPR 83. cikk (4) bekezdés
[533] NAIH/2020/643/6, Budapest, 2020. július 17., https://www.naih.hu/files/NAIH-2020-643-hatarozat.pdf, utolsó letöltés: 2022. 07. 14.
[534] Iránymutatás a 2016/679 rendelet szerinti közigazgatási bírság alkalmazásáról és megállapításáról, https://ec.europa.eu/newsroom/article29/items/611237, utolsó letöltés: 2022. 09. 03.
[535] Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 1.0 Adopted on 12 May 2022, https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf, utolsó letöltés 2022. 09. 03.

- ✓ a bírság összegének megállapításakor a felügyeleti hatóságoknak kellően figyelembe kell venniük az elkövető és a jogsértés jellemzőit (súlyosságát) [GDPR 83. cikk (2) bekezdés], valamint
- ✓ a bírság összege nem haladhatja meg a GDPR 83. cikkének (4), (5) és (6) bekezdésében meghatározott maximális összegeket. A bírság összegének számszerűsítése egyedi értékelésen alapul, a GDPR által előírt határok figyelembevételével.

Az EDPB öt lépésből álló módszertant dolgozott ki a felügyeleti hatóságoknak a közigazgatási bírságok kiszámítására:

1. lépés: a hatóságnak azonosítania kell az adott esetben végzett adatkezelési műveleteket, és értékelnie kell a GDPR 83. cikke (3) bekezdésének alkalmazását.[536]

2. lépés: meg kell határoznia a bírság összegének további kiszámításához szükséges kiindulópontot

- ✓ a jogsértés GDPR szerinti minősítésének értékelésével,
- ✓ a jogsértés súlyosságának az eset körülményeire tekintettel történő értékelésével, valamint
- ✓ a vállalkozás forgalmának értékelésével.

3. lépés: a hatóságnak az adatkezelő/adatfeldolgozó múltbeli vagy jelenlegi magatartásával kapcsolatos súlyosbító és enyhítő körülményeket értékelnie kell, és ennek megfelelően a bírságot emelheti vagy csökkentheti.

4. lépés: a hatóságnak meg kell határoznia a különböző jogsértésekre vonatkozó jogi maximumokat (azonban az előző vagy a következő lépésekben alkalmazott emelések nem haladhatják meg ezt a maximális összeget).

5. lépés: a hatóságnak elemeznie kell, hogy a kiszámított végső összeg megfelel-e a hatékonyság, a visszatartó erő és az arányosság követelményeinek és szükség esetén módosítható, azonban nem haladhatja meg a felső határt.

Hazánkban, amennyiben az adatvédelmi hatósági eljárásban hozott határozatban kiszabott bírság megfizetésére kötelezett költségvetési szerv, abban az esetben a bírság mértéke százezertől húszmillió forintig terjedhet.[537]

A bírság kiszabásakor a felügyeleti hatóságok számos tényezőt vesznek figyelembe[538], például

- ✓ *mérlegelik a jogsértés jellegét, súlyosságát és időtartamát, az érintett adatkategóriákat és azt, hogy a jogsértést szándékosan vagy gondatlanságból követte-e el az adott adatkezelő vagy adatfeldolgozó;*
- ✓ *az adatkezelő vagy adatfeldolgozó milyen intézkedéseket tett az érintettek által elszenvedett károk enyhítése érdekében;*
- ✓ *a vizsgálat alá vont hogyan működött együtt a felügyeleti hatósággal a jogsértést követően, illetve a hatóság miként értesült a jogsértésről*

[536] GDPR 83. cikk (3) bekezdés: Ha egy adatkezelő vagy adatfeldolgozó egyazon adatkezelési művelet vagy egymáshoz kapcsolódó adatkezelési műveletek tekintetében – szándékosan vagy gondatlanságból – e rendelet több rendelkezését is megsérti, a bírság teljes összege nem haladhatja meg a legsúlyosabb jogsértés esetén meghatározott összeget.

[537] Infotv. 61.§ (4) bekezdés b) pont

[538] GDPR 83. cikk (2) bekezdés

(például kitől értesült az adatvédelmi incidens megtörténtéről, az adatkezelőtől/adatfeldolgozótól vagy pedig egyéb módon).

A hatóságok korrekciós hatáskörrel is rendelkeznek, például

- ✓ utasíthatják az adatkezelőket, illetve az adatfeldolgozókat,
- ✓ figyelmeztethetik vagy elmarasztalhatják őket, valamint
- ✓ átmenetileg vagy véglegesen megtilthatják az adatkezelési tevékenységeket.

A magyar adatvédelmi hatóság (NAIH) gyakorlatából

A NAIH a bírság kiszabása során az alábbi körülményeket jelentős súlyosbító körülményként vette figyelembe:

- ✓ *„az Ügyfél nem csak az ügy tárgyát képező incidenssel kapcsolatban nem tett eleget az általános adatvédelmi rendelet vonatkozó rendelkezéseinek, hanem egyáltalán nem rendelkezett az eset megtörténtekor belső incidenskezelési szabályzattal, amelynek a megléte azonban részéről elvárható.”*[539]
- ✓ *„Az adatvédelmi incidens kifejezetten magas kockázattal járt: politikai véleményre vonatkozó, különleges személyes adatokat érintett, nagy számú érintettre vonatkozott, az érintettek egyéni azonosítását is lehetővé tevő, rájuk nézve további incidensek kockázatát hordozó adatok váltak megismerhetővé.”*[540]
- ✓ *„a Kérelmezett szándékosan, egy hierarchikus viszonyban, munkáltatói helyzetével visszaélve követte el a jogsértést”*[541]
- ✓ *„Az Ügyfél tudomással bírt az incidensről, az érintett adatok különleges személyes adat jellege nyilvánvaló, mégsem tette meg a Hatóság részére a bejelentéssel, valamint az érintettek tájékoztatásával kapcsolatos intézkedéseket, így magatartása kifejezetten magas fokon felróható.”*[542]
- ✓ *„Az elavult titkosítási technológia az incidensnek az érintettek jogaira és szabadságaira nézve fennálló kockázatát kifejezetten megnövelte.”*[543]
- ✓ *„Az Ügyfél (…) az incidensről való tudomásszerzést követően, – annak ellenére, hogy az érintett adatok különleges személyes adat jellege nyilvánvaló, – nem tette meg a Hatóság részére a bejelentéssel, valamint az érintettek tájékoztatásával kapcsolatos intézkedéseket, így magatartása kifejezetten magas fokon felróható.”*[544]
- ✓ *„(…) egy alapvetően magas kockázatú, különleges adatokat is érintő adatkezelés tekintetében az Ügyfél a jogosulatlan hozzáférések kiküszöbölésére és kimutatására alkalmatlan, a kockázatokkal aránytalan adatbiztonsági intézkedéseket alkalmazott, amikor az egészségügyi és további személyes adatokhoz rendkívül könnyen hozzá lehetett kívülről férni, anélkül, hogy ezt az Ügyfél észlelte volna. Az ilyen adatok kezelésére való biztonsági felkészültség, az egészségügyi tevékenységet fő*

[539] NAIH/2019/2485/20
[540] NAIH/2019/2668/2
[541] NAIH/2020/643/6. (NAIH/2019/5963.)
[542] NAIH/2019/2668/2
[543] NAIH/2019/2668/2
[544] NAIH/2020/952/ NAIH/2019/5606

tevékenységként kifejtő, profit alapú vállalkozásoktól fokozottan elvárható."[545]

- ✓ *„Ügyfélnél az egészségügyi adatok nagy számban történő kezelése alaptevékenységéhez tartozik és ezzel kapcsolatban közfeladatot ellátó szervnek minősül. Fokozottan elvárható így tőle ezen adatok körültekintő és adatvédelmi szempontból is megfelelő kezelése, az adatkezeléshez kapcsolódó kockázatok felmérésének képessége."*[546]
- ✓ *„A természetes személyek alapvető jogainak, így személyes adataik védelme szempontjából a Covid-19 járvány miatti veszélyhelyzet nem adhat felmentést a megfelelő adatbiztonsági előírások betartása alól."*[547]
- ✓ *Az Importőr adatkezelésének kiterjedtsége és piaci pozíciója alapján elvárható lenne az Importőrtől, hogy ne kizárólag egyes ügyintézői egyedi és felügyelet nélküli döntésétől függjön az érintetti jogok gyakorolhatósága."*[548]
- ✓ *„a jogsértés több éven át fennálló, folyamatos gyakorlat eredménye, és ennek megtervezése – illetve az általános adatvédelmi rendeletnek megfelelő áttervezése – elvi szinten volt átgondolatlan."*[549]
- ✓ *„a Bank által elkövetett jogsértés súlyosan gondatlannak minősül, ugyanis – mivel a Kérelmező kifejezetten jelezte, hogy beadványa adatvédelmi tárgyú, amire a GDPR és az Infotv. rendelkezései alapján szeretne választ kapni – ha a Bank minimális odafigyelést tanúsított volna, meg tudta volna válaszolni az érintett hozzáférési, illetve tiltakozási kérelmét"*[550]
- ✓ *„a Kérelmezett számos adatvédelmi hatósági eljárást kezdeményezett érintettként a Hatóságnál, továbbá a Hatóság döntéseivel szemben több alkalommal is bírósági jogorvoslattal élt, azaz a Kérelmezettről elmondható, hogy adatvédelmi kérdésekben tudatos, ezért a tudatának át kellett volna fognia, hogy az e-mailek elküldésével jogsértést valósít meg, ezért a Hatóság álláspontja szerint megállapítható, hogy a Kérelmezett a jogsértést szándékosan követte el."*[551]

A NAIH a bírság kiszabásánál az alábbi körülményeket jelentős enyhítő körülményként vette figyelembe:

- ✓ *„A Kérelmező több összetett, nagyvonalakban ismétlődő, azonban kisebb részletekben eltérő érintetti joggyakorlásra irányuló kérelmet nyújtott be – és nyújt be folyamatosan – a Kérelmezetthez, szinte követhetetlenné téve, hogy melyik kérelme pontosan mire is irányult. Ezen kérelmek sorozatos előterjesztése nehezíti és lassítja a kérelmeinek pontos és megfelelő elbírálását, teljesítését a Kérelmezett részéről. Ezekkel a kérelmekkel összefüggésben a Hatóság előtt 48 db adatvédelmi hatósági és vizsgálatai eljárás indult a Kérelmező kérelmére, panasza alapján, mely szám jól*

[545] NAIH/2020/952/ NAIH/2019/5606
[546] NAIH-2894-3/2021
[547] NAIH-2894-3/2021
[548] NAIH-2857-20/2021
[549] NAIH-2857-20/2021
[550] NAIH-1763-4/2021
[551] NAIH- 2868-23/2021.

mutatja azt, hogy a Kérelmező a folyamatos érintetti kérelmeivel nagy munkaterhet ró a Kérelmezettre." [552]

- ✓ *„az eljárás során a Hatóságnak nem jutott tudomására olyan információ, amely arra utalna, hogy az érintetteket a jogsértés nyomán kár érte volna"*[553]
- ✓ *„A Hatóság az incidenst kiváltó adatbiztonsági hiányosságot nem tekintette rendszerszintű problémának, mivel az csupán egy egyszeri adattovábbításhoz kapcsolódott és egyszeri kapkodásra, hanyagságra vezethető vissza."*[554]
- ✓ *„a jogsértés gondatlan jellegű, nem irányult az érintettek megkárosítására vagy jogellenes haszonszerzésre, és a megjelölt érdek adott esetben megállhat jogos érdekként, ha az adatkezelés feltételeit megfelelően hozzáigazítják az általános adatvédelmi rendelet indokolásban kifejtett rendelkezéseihez."*[555]
- ✓ *„a GDPR 6. cikk (1) bekezdés e) pont szerinti jogalap esetén a jogalkotó feladata, hogy jogszabályban meghatározza – többek között – a kezelendő adatok fajtáit és az adatkezelés célját és feltételeit; amennyiben e fő szempontok a jogszabályban nem jelennek meg, úgy a jogalkalmazóra hárul a felelősség annak mérlegelése során, hogy egy közérdekű feladat kezelése céljából milyen adatkör lehet szükséges"*[556]

Az is előfordul a NAIH gyakorlatában, hogy a hatóság kifejezetten enyhítő körülményként egyetlen tényezőt sem vesz figyelembe.[557]

GDPR

- ✓ A közigazgatási bírságok kiszabására vonatkozó általános feltételek [GDPR 83. cikk (148) és (150)-(151) preambulumbekezdések]
- ✓ Szankciók [GDPR 84. cikk (149) és (152) preambulumbekezdések]

Infotv.

- ✓ Infotv. 61.§ (4) bekezdés b) pont

[552] NAIH-3145-5/2021
[553] NAIH/2020/952/ NAIH/2019/5606
[554] NAIH-2894-3/2021
[555] NAIH-2857-20/2021
[556] NAIH/2020/54/4.
[557] NAIH-1763-4/2021

VÉGSZÓ

Az adatvédelemre odafigyelés soha nem volt fontosabb, mint napjainkban, amikor az adatok hatalma és jelentősége folyamatosan növekszik. Ez a könyv azzal a céllal született, hogy azoknak segítsen megérteni és megvalósítani az adatvédelmi gyakorlatokat, akik mindennapi munkájuk során adatok kezelésével foglalkoznak.

Az adatvédelem azonban nem csupán egy jó, vagy kevésbé jól sikerült szabályzat, netalán kötelezettség, hanem olyan alapvető jog és felelősség, amellyel mindannyian rendelkezünk. Ahogy a technológia fejlődik, és az adatok, és a mögöttük álló személyek egyre sebezhetőbbé válnak, kulcsfontosságú, hogy mindannyian tisztában legyünk az adatok védelmének és a biztonságuk legjobb gyakorlataival.

Ez a könyv éppen ezért átfogó képet nyújt az adatvédelem alapvető fogalmairól, módszereiről és eszközeiről olyanok számára, akik nem szakértői a területnek. Megismerteti az olvasót az adatvédelmi jogszabályokkal, a személyes adatok kezelésének alapelveivel és a legalapvetőbb adatbiztonsági követelményekkel, valamint számtalan példát is bemutat annak érdekében, hogy ez a „száraz” téma könnyebben befogadható és megérthető legyen.

Elmondhatjuk, az adatvédelem az egyén és a társadalom jövője szempontjából kulcsfontosságú tényező. Bízunk benne, hogy ez a könyv ösztönző erőt ad az olvasóknak az adatvédelem iránti elkötelezettségük megerősítéséhez, és segít nekik kialakítani a biztonságos és etikus adatkezelés kultúráját a mindennapi munkájuk során, ezzel is hozzájárulva egy biztonságosabb és felelősebb digitális világ kialakításához.

Az adatvédelem azonban nem csupán a szervezetek, és a szervezetek nevében adatokat kezelők felelőssége, hanem mindannyiunké. A tudatosság és a proaktív megközelítés a kulcs ahhoz, hogy megvédjük adatainkat és tiszteletben tartsuk mások magánszféráját – ezt támasztja alá az adatvédelmi tudatossággal kapcsolatos kutatásunk eredménye is:

- az iskolai végzettség tekintetében elmondható, hogy jellemzően a magasabban végzetséggel rendelkező személyek ismerték az általános adatvédelmi rendeletet, míg az alacsonyabb végzettséggel rendelkezők nagyobb számban válaszoltak nemmel. Ebből az eredményből az következik, hogy az adatvédelemmel, kiemelten a személyes adatok védelmével kapcsolatos oktatást (ismeretterjesztést) már általános iskolai szinten meg kell kezdeni. Emellett a magasabb iskolai végzettséggel rendelkező személyek jellemzően érdeklődnek, vagy rendelkeznek alapismeretekkel az adatvédelemről. Ennek oka feltételezhetően az, hogy a felsőoktatásban több esetben találkoznak adatvédelmi kérdésekkel, valamint tanulmányaik során rálátást szereznek arra, hogy a személyes adatok védelme kiemelt prioritással bír.
- bebizonyosodott, hogy a felhasználók kevesebb, mint fele rendelkezik ismeretekkel a GDPR-ról. Emellett a felhasználók vagy nem értik vagy el sem olvassák az adatvédelmi tájékoztatókat.
- a kutatás során vizsgáltuk, hogy a megkérdezettek a rendelet szabályait az adatkezelési tájékoztatókban tudják-e értelmezni. A 141 fő válaszadó

közül 41 fő válaszolt „igen-nel”, 56 fő pedig „nem-el”, 44 fő pedig saját bevallása szerint nem olvassa el ezeket a tájékoztatókat. Az arányokból arra lehet következtetni, hogy a megkérdezettek közel 29%-a tudja csak értelmezni az adatvédelmi tájékoztatókban foglaltakat, közel 40% pedig nem érti ezeket a szabályokat, 31% pedig el sem olvassa azokat.

- jellemzően probléma, hogy az érintett által szolgáltatott adatok gyakorlati felhasználását nem tudja követni az érintett, valamint nem rendelkezik információval azokról adatvédelmi, kibervédelmi és informatikai megoldásokról, amelyekkel a gyakorlatban az adatkezelők véd(het)ik a kezelésükben lévő személyes adatokat. A megkérdezettek egy része azt is elmondta, hogy elgondolásuk szerint az adatkezelők feleslegesen kérnek be, illetve tárolnak olyan személyes adatokat, amelyek valószínűleg nem is szükségesek a tényleges adatkezelésekhez.

Az adatvédelemnek minden szinten prioritást kell élveznie, legyen szó vállalati szintű irányításról, állami szabályozásról vagy egyéni magatartásról, és együtt tehetünk azért, hogy az adatok védelme ne csak egy szakmai feladat legyen, hanem egy társadalmi elkötelezettség és érték is.

Záró gondolatként szeretnénk köszönetet mondani mindazoknak, akik részt vesznek az adatvédelem terén folytatott erőfeszítésekben, és az olvasóknak, akik elkötelezték magukat abban, hogy ismereteket szerezzenek az adatvédelem területén.

Bízunk benne, hogy ez a könyv hozzájárul az adatvédelem fontosságának megértéséhez és az adatvédelmi gyakorlatok megvalósításához, és egyre többen válunk az adatvédelem elkötelezett híveivé, így járulva hozzá egy biztonságosabb digitális jövőhöz.

dr. Albert Ágota LL.M adatbiztonsági és adatvédelmi szakjogász, mesterséges intelligencia és technológiai jogi szakjogász, adatvédelmi tisztviselő

Üveges András József őrnagy, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola Doktorandusz, Nemzeti Közszolgálati Egyetem Katonai Nemzetbiztonsági Tanszék tudományos segédmunkatárs

ADATVÉDELMI INCIDENSEK (MEGTÖRTÉNT ESETEK)

Kórház adatvédelmi incidense

(a Kórház által az adatvédelmi incidens bekövetkezéséről kiadott tájékoztatás alapján)

„(…) 2019. május 6-án egy magánszemély telefonon tájékoztatta a Kórházat arról, hogy a (…) piacon vásárolt egy használt számítógépet (PC). Az eszköz installálása közben észlelte, hogy a számítógépen a Kórház szövettani, kórbonctani leletei, valamint boncolási jegyzőkönyvek és azok hanganyagai találhatóak. (…)

A lefolytatott vizsgálat a következő megállapításokat tette.

2019. március 08-án sor került a (…) Pathológiai Osztályok régi, elavult PC-inek a cseréjére.

A selejtezésre került IT eszközök elszállítására és megsemmisítésére a Kórház egy külső céggel áll szerződéses jogviszonyban. Viszont mielőtt a külső cégnek az IT eszközök átadásra kerültek volna megsemmisítésre, ismeretlen személyek eltulajdonították azokat a selejtezett IT eszközök gyűjtésére rendszeresített konténerből.

Az adatok törlése a szerződött szolgáltatóval történt megállapodás szerint a szállítást követően történt volna meg, azonban a PC eszközök eltulajdonítása miatt a törlés elvégzésére már nem volt lehetőség. (…)

Az Intézménynek az érintettek felé tájékoztatási kötelezettsége van, tekintettel azonban arra, hogy az incidens körülményeit fgyelembe véve az érintetteket és az incidenssel érintett személyes adatok körét nem lehetséges egyértelműen és pontosan megállapítani, és emiatt az érintettek egyenkénti tájékoztatása nem lehetséges, ezért az Intézmény az érintettek tájékoztatását nyilvánosan közzétett információk útján teszi meg.

Jelen tájékoztatásunk célja, hogy biztosítsa az érintettek hatékony és megfelelő tájékoztatását, továbbá felhívja az érintettek fgyelmét az incidenssel kapcsolatosan a személyes adataikat érintő kockázatokról.

A Kórház vezetése fenti eset kapcsán szeretné közölni a tisztelt nyilvánossággal, hogy habár a selejtezésre váró számítógépek a selejtezés során eltűntek, és ez a Kórház felelősségi körén kívül esik, de mélységesen együtt érez az érintettekkel, és a Kórház vezetése és dolgozói sajnálatukat fejezik ki, hogy a Kórház területéről olyan PC eszközök tűnhettek el, amelyek számos érintett egészségügyi szenzitív adatait tartalmazták. A Kórház vezetése ezen, cselekményt maximálisan elítéli, és a mindennapi munkája során a kórházi vezetőség és a dolgozók is arra törekednek, hogy az érintettek személyes adatai minden esetben jogszabályi előírásoknak megfelelő védettséget élvezzenek.

(…), 2019. augusztus 14.
(…) főigazgató sk.”

Megjegyzések (figyelemmel a közleményben foglaltakra):

- ✓ az IT eszközök még a külsős cégnek átadás előtt tűntek el, teljes adattartalommal;
- ✓ március 8 és május 6 között senkinek sem tűnt fel, hogy az eszközök eltűntek a konténerből;
- ✓ az adatkezelő úgy selejtezte le az eszközöket, hogy fogalma sem volt, azokon milyen adat van (átadás előtt a tartalom nem került átnézésre, archiválásra, törlésre stb.);
- ✓ a kórház nem érzi úgy, hogy bármilyen felelőssége is lenne az IT eszközök eltűnésével kapcsolatban (azok a kórház területén lévő konténerből, még az átadás előtt, teljes adattartalommal tűntek el);
- ✓ a kórház az érintettek tájékoztatására szolgáló dokumentumot a NAIH erre vonatkozó kötelezése után tette ki a honlapjára;[558]
- ✓ a kórház az incidens után (új) adatvédelmi szabályzatot készített, mely az incidensről szóló közlemény utáni napon lépett hatályba.

Az adatvédelmi incidens elkerülhető lett volna, illetve az érintettek jogait és szabadságait érintő kockázatok mérsékelhetőek lehettek volna:

- ✓ selejtezés menetének korrekt szabályozásával és a szabályozás betartásának megkövetelésével, különös tekintettel az információbiztonsági előírásokra (pl. IT eszköz csak úgy kerülhessen a konténerbe, hogy az ne tartalmazhasson adatokat stb.);
- ✓ vagyonbiztonsági követelmények előírása és azoknak megfelelés az IT eszközök tárolására szolgáló konténer esetén (pl. zárhatóság, elektronikus megfigyelés, konténer tartalmának figyelemmel kísérése stb.).

Közérdekű bejelentő adatainak jogalap nélküli továbbítása

(NAIH/2019/596/3)
Bírság összege: 1 millió Ft.

Az érintett közérdekű bejelentést tett Kecskemét Megyei Jogú Város Önkormányzatánál, mely az Önkormányzat által alapított és felügyelt [...] intézmény működésére vonatkozott. A közérdekű bejelentést tett érintett az intézmény alkalmazottja volt a bejelentés időpontjában.

Az önkormányzatnak az intézmény felügyeletével kapcsolatos feladatokat ellátó alpolgármestere értesítette az intézményt a közérdekű bejelentés tényéről, illetve megkezdte annak kivizsgálását. Az intézmény vezetője további információként kérte a közérdekű bejelentés teljes tartalmának rendelkezésére bocsátását. A kérését teljesítették és személyes adatokat tartalmazó dokumentumot – az érintett közérdekű bejelentését – teljes terjedelmében, anonimizálás nélkül megküldték az intézménynek.

Az érintett közalkalmazotti jogviszonyát ezt követően az intézmény rendkívüli felmentéssel megszüntette, melynek egyik indokaként éppen az érintett által tett közérdekű bejelentést jelölte meg. Az érintett ezt követően tájékoztatást kért az

[558] NAIH/2019/4422/7, a hatóság nem hozta nyilvánosságra a határozatot

Önkormányzattól azzal kapcsolatban, hogy személyes adatai milyen módon és okból váltak ismertté munkáltatója számára, az ekkor szerzett tudomást az incidensről.

A panasztörvény[559] alapján

- ✓ a panaszost vagy a közérdekű bejelentőt – a Panasztv-ben foglaltak kivételével – nem érheti hátrány a panasz vagy a közérdekű bejelentés megtétele miatt;
- ✓ a panaszos vagy a közérdekű bejelentő személyes adatai – a Panasztv.-ben foglaltak kivételével – csak a panasz vagy a közérdekű bejelentés alapján kezdeményezett eljárás lefolytatására hatáskörrel rendelkező szerv részére adhatóak át, ha e szerv annak kezelésére törvény alapján jogosult, vagy az adatai továbbításához a panaszos vagy a közérdekű bejelentő egyértelműen hozzájárult. A panaszos és a közérdekű bejelentő személyes adatai egyértelmű hozzájárulása nélkül nem hozhatóak nyilvánosságra.

A NAIH megállapította, hogy

- ✓ a közérdekű bejelentő személyes adatainak harmadik személlyel való közlésével megvalósuló adatkezelésre – a panasztörvényben előírt kifejezett tiltás ellenére – jogellenesen került sor [megsértett rendelkezések: GDPR 5. cikk (1) bekezdés a) pontja és 6. cikk].
- ✓ „bár a jogsértés csak egyetlen érintettre terjedt ki, azonban az számára jelentős következménnyel járt, jelentős gazdasági és szociális hátrányt okozott neki, mivel a rendelkezésre álló iratok alapján megállapítható volt, hogy a jogsértés és a közalkalmazotti jogviszonyának megszüntetése között közvetlen ok-okozati kapcsolat áll fenn.”

Jármű Szolgáltatási Platform (Belügyminisztérium) adatvédelmi incidense

(NAIH/2019/721/6)

2019. január 6-án a totalcar.com újságírója megkereséssel fordult Belügyminisztérium Kommunikációs Főosztályához, amelyben felhívta a figyelmet arra, hogy a 2018. december 31. óta tesztüzemben működő Jármű Szolgáltatási Platform (JSZP) rendszeren keresztül különböző személyes adatok megismerésére is lehetőség van. A bejelentéshez mellékelte csatolta egy általa a JSZP rendszeren keresztül lekérdezett gépjármű adatlapját.

„Az incidens lényege, hogy a JSZP rendszeren keresztül a felhasználók egy gépjármű rendszáma alapján különböző, a járművel kapcsolatos adatokat igényelhetnek a gépjárművekkel kapcsolatos nyilvántartásokból (pl. évjárat, kilométeróra állása, motor stb.). Az Ügyfélnek az incidenst jelző újságíró azonban az általa teszt jelleggel végrehajtott néhány lekérdezés során arra lett figyelmes, hogy a JSZP rendszer a gépjárművek korábbi tulajdonosainak (vevők, örökösök) személyes adatait (név, születési dátum, anyja neve, néhány esetben cím) is megjelenítette. Ezen kívül a

[559] A panaszokról és a közérdekű bejelentésekről szóló 2013. évi CLXV. törvény (hatályon kívül helyezte a 2023. évi XXV. törvény a panaszokról, a közérdekű bejelentésekről, valamint a visszaélések bejelentésével összefüggő szabályokról)

műszaki és/vagy eredetiségvizsgálat során készített fényképeket tartalmazó galériában volt néhány olyan felvétel, amelyen természetes személyek láthatóak.

Az incidensbejelentés szerint az értesülés után az Ügyfél az üzemeltető IdomSoft Zrt-vel közösen azonnal megkezdte az informatikai rendszer átvizsgálását és az incidenst kiváltó ok elhárítását. Az incidenssel kapcsolatos belső vizsgálat megállapította, hogy a rendszer kijavításáig összesen 15 820 alkalommal került sor személyes adatok kiadására. (…)

A feltárt tényállás szerint a JSZP működésében kéttípusú adatvédelmi incidens történt:
– Az első típusba azok az esetek tartoznak, amikor a rendszer a gépjárművek korábbi tulajdonosainak személyes adatait is megjelenítette a lekérdezések során.
– A második típusba pedig azok az esetek tartoznak, amikor a műszaki és/vagy eredetiségvizsgálat során készített fényképeket tartalmazó galériában olyan felvételek szerepeltek, amelyen természetes személyek láthatóak.

Az első típusba tartozó incidensek oka, hogy rossz beállítás révén nem működött megfelelően a rendszer szűrője a megjelenített személyes adatok tekintetében. Az incidensről való tudomásszerzést követően az Ügyfél utasította az üzemeltető IdomSoft Zrt-t, hogy állítson be szűrést ezekre az adatokra, hogy azokat a rendszer a továbbiakban ne szolgáltassa a lekérdezések során. Ennek a szűrőnek az alkalmazása egyébként az eredeti rendszertervben is szerepelt. A szűrő alkalmazásával az incidens oka kijavításra került.

A második típusba tartozó incidensek jövőbeli megelőzésével kapcsolatban az Ügyfél „módszertani útmutatót" szerkesztett a gépjárművek eredetiség vizsgálatán készült fotók készítésének helyes módjáról. (…) Ezekkel az útmutatókkal kívánják elérni, hogy a fotókon a továbbiakban természetes személyek ne legyenek szerepeltetve. (…)
Az Ügyfél az incidens kockázati besorolását elhanyagolható kockázatúnak minősítette. A besorolás során figyelembe vette az incidensek számát. Mivel a jármű nyilvántartás kb. 5 millió gépjármű adatait tartalmazza, és ehhez kapcsolódóan 100 milliónál is több személyes adatot kezel, ezért a bekövetkezett incidensek során megismert személyes adatok száma (15 820 db lekérdezés, 11 614 db személyes adat) szerinte elhanyagolható a kezelt adatok számához mérten (0,0158%). Ezen felül az Ügyfél megítélése szerint ugyan a megismert személyes adatok azonosíthatóvá tették az érintetteket, azonban a személyes adatokkal való visszaélés esetei csak szűk körben okozhatnának kárt az érintettek számára. (…)

Az Ügyfél érvelésével szemben az érintetteknek az incidensről való tájékoztatására a Hatóság megítélése szerint azért van szükség, mivel az érintett magánszférájára jelentett kockázat a személyazonosításra alkalmas adatok (név, születési adatok, anyja neve, néhány esetben cím) nyilvánosságra kerülése esetén jellemzően magas. Ezen adatok birtokában elkövethető személyazonossággal visszaélés (pl. egy szerződés megkötésekor). (…)

Az összes kezelt adathoz képest nyilvánosságra került adatok alacsony arányának nincs jelentősége az érintettek magánszférájára jelentett kockázat megítélése szempontjából ebben a konkrét esetben.

A Hatóság megítélése szerint, ezért szükséges tájékoztatni az érintetteket, mivel a kikerült adatok tekintetében a magánszférájukra gyakorolt hatás és kockázatok csökkenthetőek azáltal, ha tudomással bírnak róla, hogy az adataik egy ilyen típusú incidensben lehettek érintettek. (…)

A Hatóság továbbá az incidens által okozott kockázatok csökkentése érdekében további intézkedésként írja elő, hogy az incidens időszakában a rendszeren keresztül adatokat lekérő felhasználókat is tájékoztassa az Ügyfél az incidens tényéről és következményeiről, továbbá arról, hogy a jogellenes esetleg birtokukba jutott adatokat töröljék. Ez az intézkedés a Hatóság megítélése szerint szükséges a természetes személyek jogaira és szabadságaira jelentett kockázat mérséklése szempontjából, mivel így megelőzhető és tovább csökkenthető a jogellenes adatkezelés kockázata."

Budapesti Rendőrfőkapitányság adatvédelmi incidense

(NAIH/2019/2471/6)
Bírság összege: 5 millió Ft

„A 2019. február 25-i incidensbejelentés szerint 2019. január 11. napon […] a Budapesti Rendőrfőkapitányság […] szolgálati feladatai ellátása során, az általa adattárolásra használt egyik 4 GB tárhellyel rendelkező pendrive-ot elveszítette. Az adathordozón megtalálható volt a BRFK teljes nevesített személyzeti állománytáblája, továbbá a rendvédelmi szolgálati jogviszonyváltásra vonatkozó teljes személyügyi anyag elektronikus másolatban. Az incidenssel érintett személyek számát az Ügyfél 1733 főben jelölte meg, amely a rendvédelmi alkalmazotti jogviszonnyal érintett teljes állományt takarja (adatok: születési név, születési idő, anyja neve, TAJ szám, beosztás, munkakör). Az adathordozó, valamint az azon található állományok semmilyen hozzáférésvédelemmel (pl. jelszó, titkosítás) nem voltak ellátva. Az adathordozón nem szerepelt egyébként olyan anyag, amely más forrásból ne lenne helyreállítható. (…)

Az Ügyfél arról is tájékoztatta a Hatóságot, hogy […] a személyes adatokat tartalmazó dokumentumokat nem a szolgálati, hanem magáncélra használt adathordozóra másolta át, és nem alkalmazott semmilyen biztonsági intézkedést a tárolt adatokkal kapcsolatban, ezzel pedig megszegte az Ügyfél Informatikai Biztonsági Szabályzatáról szóló 18/2018. (V. 31.) ORFK utasításában foglaltakat, így különösen a 109., 116. és 118. pontjait.[560] *Erre tekintettel Budapest Rendőrfőkapitánya – azóta jogerősen lezárult – fegyelmi eljárást rendelt el nevezettel szemben.*

[560] 18/2018. (V. 31.) ORFK utasítás:
109. pont: A Rendőrség által biztosított felhasználói eszközöket jelszavas védelemmel kell ellátni. Az eszköz zárolásra kerül 5 perc inaktivitást követően.
116. pont: Az adatot tartalmazó adathordozókat védelmi kell a jogosulatlan hozzáféréstől, visszaéléstől és
megrongálódástól.
118. pont: A mobil eszközöket biztonságos módon kell kezelni, annak érdekében, hogy ne kerülhessenek illetéktelen felhasználásra, ezért amennyiben a technológia rendelkezésre áll, a rajta tárolt információkat központi management eszközzel titkosítva kell tárolni.

Az adatokhoz való jogosulatlan hozzáférés tényére utaló információ, körülmény nem jutott az Ügyfél tudomására. Bejelentés a pendrive megtalálásával, illetve az adatokkal való visszaéléssel kapcsolatban nem érkezett az Ügyfélhez azóta sem. Az Ügyfél valószínűsíti, hogy az adathordozó az elveszítésének időpontjában fennálló időjárási körülmények miatt (hó, fagy, sáros környezet) megsemmisült. A nem megfelelően védett, átmásolt adatok elveszítésén túl így további biztonsági esemény (pl. jogosulatlan hozzáférés, nyilvánosságra hozatal) az adatokkal kapcsolatban nagy valószínűséggel nem történt. (…)

A Hatóság (…) egyetért azzal, hogy az incidens kockázatos besorolását az adja, hogy a pendrive-on tárolt adatok között megtalálhatóak voltak nem nyilvánosan hozzáférhető, illetve nem közérdekből nyilvános adatok is, így az érintettek születési adatai, anyjuk neve és TAJ száma. Ezen, nem nyilvánosan hozzáférhető adatok folyamatos bizalmassági sérülésnek való kitettsége pedig olyan kockázati tényező, amely indokolja az incidens bejelentését az általános adatvédelmi rendelet 33. cikk (1) bekezdése alapján.

Az általános adatvédelmi rendelet (75) preambulumbekezdésében foglaltak szerint, ha az adatkezelésből – így jelen ügyben az adatok pendrive-on való tárolásából – személyazonosságlopás vagy személyazonossággal való visszaélés fakadhat, úgy az alapvetően kockázatosnak minősül. Az érintettek születési adatai, anyjuk neve és különösképpen TAJ száma (a név és munkahely, beosztás ismerete mellett) olyan adatok, amelyekkel elkövethető személyazonosságlopás, személyazonossággal visszaélés.

A Hatóság kiemeli, hogy az adatvédelmi incidens fogalmának elemei közül csak az adatok elveszítése valósult meg jelen esetben. A biztonsági sérülés tehát közvetlenül csak az elveszítést eredményezte, másfajta incidens megvalósulására (pl. jogosulatlan hozzáférés, nyilvánosságra hozatal) nem utal konkrét körülmény. A további bizalmassági sérülésnek való kitettség kockázata azonban fennáll az ügyben, mivel az adathordozó és azon tárolt adatok nem voltak semmilyen technikai intézkedéssel védve a jogosulatlan hozzáféréstől. Az ilyen adatok megfelelő védelem nélküli elveszítése ezért önmagában is kockázatos adatvédelmi incidenst eredményez, akkor is, ha egyébként az azokhoz való jogosulatlan hozzáférés, nyilvánosságra hozatal, vagy az adatokkal való egyéb visszaélés ténye nem is állapítható meg. (…)

(…) az incidensről való tudomásszerzés és a bejelentés között összesen 45 nap telt el, amely az általános adatvédelmi rendelet által főszabályként előírt bejelentési határidő tizenötszörös túllépését jelenti. (…)

A késedelmes bejelentés indokait az adatkezelő abban jelölte meg az incidensbejelentésében, hogy az ügy teljes körű parancsnoki kivizsgálása volt szükséges, valamint állásfoglalást kért az ORFK-tól arra vonatkozóan, hogy az incidens az érintettek jogai és szabadságai tekintetében milyen kockázatúként értékelhető. A parancsnoki kivizsgálás az ügyben 2019. február 8-án zárult le, az ORFK állásfoglalása pedig 2019. február 12-én 15:45-kor került kézbesítésre az Ügyfél részére.

A Hatóság nem tudja elfogadni az Ügyfél fenti indokait a bejelentési határidő

többszörös túllépésére vonatkozóan. Ennek oka, hogy az incidens bekövetkezésének összes körülményéről, és az érintett személyes adatok köréről az Ügyfél már 2019. január 11-én, az erről szóló rövid utas értesítés megtételekor tudomást szerzett a pendrive-ot véletlenül elveszítő […]-tól. Az incidens kockázatértékeléséhez szükséges valamennyi tény és körülmény gyakorlatilag ettől az időponttól kezdve rendelkezésére állt az Ügyfélnek, illetve rövid úton tudott volna egyeztetni az incidensben érintett munkavállalójával annak további pontosítása érdekében. A Hatóság megjegyzi, hogy irreleváns a 72 órás bejelentési határidő számítása szempontjából, hogy az incidens pénteki napon történt és ezért az incidensbejelentési határidő hétvégi napokat is magába foglalt. Ez különösen azért is igaz, mivel az Ügyfél olyan kiemelt jelentőségű rendvédelmi feladatokat ellátó államigazgatási szervként működik, amelynek gyakorlatilag az év minden napján, napi 24 órában biztosítania kell, hogy el tudja látni a közfeladatait."

Ferencvárosi Szociális és Gyermekjóléti Intézmények Igazgatóság

(NAIH/2019/3854)
Bírság összege: 100 ezer Ft

„Ferencvárosi Szociális és Gyermekjóléti Intézmények Igazgatóság egyik munkatársa tévedésből kilenc darab, személyes adatot tartalmazó dokumentumot téves címzett részére postázott, Újpest Önkormányzatának Szociális Intézménye részére, amely azonos, jogszabályban előírt feladatot lát el más illetékességi területen. A dokumentumokban szereplő személyes adatokat ezáltal jogosulatlanul ismerhette meg a téves címzett, így sérült az adatok bizalmas jellege. Az adatvédelmi incidens 18 érintett, az Igazgatóság ügyfelei és családtagjaik, köztük kiskorúak következő személyes adatait érintette: azonosító adatok, elérhetőségi adatok, büntetett előélettel, bűncselekményekkel vagy büntetéssel, intézkedéssel kapcsolatos adatok, szociális azonosságra vonatkozó adatok, illetve az Igazgatóság által folytatott gyermekek védelmére irányuló eljárásokkal összefüggésben kezelt egyéb, a magánéletükre vonatkozó személyes adatok.

Az Igazgatóság tudomásszerzése és az adatvédelmi incidens bejelentése között 24 nap telt el. A késedelem igazolásában arra hivatkoztak, hogy az illetékes személy elsődlegesen a más halaszthatatlan, és alapfeladatával összefüggő feladatokat végezte el, ezért nem került sor a szerv vezetőjének tájékoztatására az incidensről, illetve a Hatóságnak történő bejelentésre sem. A Hatóság a késedelem Igazgatóság általi igazolását nem fogadta el.

Az Igazgatóság az incidenssel kapcsolatos intézkedések megtételéről – így különösen a kockázatelemzésről – is csak az incidensről való tudomásszerzést követő 24. napon intézkedett. „Az incidens kezelésének (érintett adatok pontos körének, egyéb körülmények, az incidens oka feltárásának) a megkezdése hiányában az incidensnek az egyes személyek jogait és szabadságait érintő tényleges kockázatai sem mérhetők fel kellőképpen, ami önmagában is kockázatot jelent."

Enyhítő körülményként vette figyelembe a Hatóság, hogy az incidens egy szervezeti egységnél történt gondatlan mulasztás eredménye, így a jogsértés nem vezethető vissza

az Igazgatóságon fennálló rendszerszintű problémára, illetve szándékosság gyanúja sem merül fel a jogsértéssel kapcsolatban."

Hungária Med-M Kereskedelmi és Szolgáltató Kft

(NAIH/2020/952/, NAIH/2019/5606)
Bírság: 7,5 millió Ft

„A Hatósághoz 2019. július 9-én közérdekű bejelentés érkezett, amely az Ügyfél online rendszerében fennálló, személyes-, köztük különleges adatokat érintő sérülékenységre hívta fel a figyelmet: az Ügyfél által üzemeltetett weboldal, a https://www.hungariamed.hu időpontfoglaló rendszerében – https://bejelentkezes.hungariamed.hu – kezelt orvosi leletek és beutalók nyilvánosan hozzáférhetők, illetve letölthetők jogosultsággal nem rendelkező felhasználók részére. A bejelentés mellékletét képezte egy képernyőfotó, melyet a bejelentő az általa elért, az időpontfoglaló rendszerben tárolt dokumentumok listáját megjelenítő felületről készített. A bejelentő elmondása szerint a problémát már jelezte az Ügyfélnél is közvetlenül, azonban visszajelzést nem kapott és a hiba sem került kijavításra. (…)

A sérülékenység a https://bejelentkezes.hungariamed.hu/doc/, illetve a https://fogleu.hungariamed.hu/doc/ URL-eket érintette, ahol a betegek leleteit tartalmazó .pdfkiterjesztésű dokumentumokat tárolták. A webszerver a fenti speciális, /doc/ végződésű URL-ek meghívásával a kért időpontfoglaló felület megjelenítése helyett, a webszerveren található összes tartalmat kilistázta a képernyőre. Ez lehetővé tette, hogy a fenti linkek ismeretében bárki, bejelentkezés, vagyis az oldalon történő regisztráció nélkül hozzáférjen az online felületen tárolt személyes adatokat tartalmazó dokumentumokhoz.

A Hatóság IT biztonsági munkatársa megállapította, hogy az adatvédelmi incidenssel érintett rendszerben fennálló sérülékenység abból adódóan valósulhatott meg, hogy az Ügyfél a szerverén nem megfelelő konfigurációs beállításokat alkalmazott. Megfelelő beállítások esetén egy /doc/ végződésű URL beírásakor a szerver egy hibaüzenetet jelenít meg, mely szerint az URL a szerveren nem található. Az említett konfigurációs hiba következtében azonban az érintett URL-ek meghívásával a szerver megjelenítette a weboldalon található könyvtárszerkezetet, így az ott tárolt személyes adatokat tartalmazó dokumentumokhoz hozzá lehetett férni. (…)

Az adatvédelmi incidenssel érintett rendszerben az Ügyfél körülbelül 15 000 személyes adatot kezel: az Ügyféllel szerződéses jogviszonyban álló partnerek munkavállalóinak neve, születési helye- és ideje, anyja neve, TAJ száma, e-mail címe, telefonszáma, lakcíme, munkaköre, és egészségügyi adatai. (…)

A Hatóság megítélése szerint az incidens Ügyfél általi kockázatértékelése nem elfogadható. Az, hogy az Ügyfélnek nem áll rendelkezésére arra vonatkozó bizonyíték, hogy az informatikai rendszerében fennálló sérülékenységet arra jogosulatlan személyek ténylegesen kihasználták volna, nem elegendő annak a megállapításához, hogy személyes adatokhoz való jogosulatlan hozzáférés nem történt. A Hatóság az eljárás során megállapította, hogy az Ügyfél naplózási rendszere nem volt alkalmas a külső hozzáférések kimutatására, mivel az Ügyfél által vizsgált időszakban a Hatóság

IT biztonsági munkatársa, valamint korábban a közérdekű bejelentő is hozzáfért a kezelt adatokhoz, anélkül, hogy ezt az Ügyfél észlelte volna.
A Hatóság nem tudja elfogadni az Ügyfél azon érvelését sem, miszerint az incidens azért nem járt kockázattal, mert a feltárt sérülékenységet annak észlelését követően azonnal kijavította. Azt ugyanis, hogy ez a sérülékenység pontosan mióta állt fent informatikai rendszerében, az Ügyfél szintén nem tudta megállapítani, így annak megállapítására sem volt képes, hogy az IBSZ[561]-ben foglalt naplózási időintervallumon kívül történt-e jogosulatlan hozzáférés.

Az általános adatvédelmi rendelet (75) preambulumbekezdésében foglaltak szerint, ha az adatkezelésből személyazonosság-lopás vagy személyazonossággal való visszaélés fakadhat, úgy az alapvetően kockázatosnak minősül. Az érintettek neve, születési adatai, anyjuk neve és különösképpen TAJ száma olyan adatok, amelyekkel elkövethető személyazonosság-lopás, személyazonossággal visszaélés.

Az érintettek jogaira jelentett magas kockázati besorolást továbbá önmagában is megalapozza az, hogy az Ügyfél az incidenssel érintett rendszerben tárolt nagyszámú (körülbelül 15 000 darab) személyes adat között egészségügyi adatokat is kezel, melyek az általános adatvédelmi rendelet 9. cikk (1) bekezdése szerint a személyes adatok különleges kategóriájába tartoznak. Ezen adatok kiemelését a személyes adatok általános fogalma alól az indokolja, hogy az ilyen információk az érintett életének érzékenyebb aspektusaira vonatkoznak, ezért azok illetéktelen általi megismerésének, vagy nyilvánosságra kerülésének lehetősége is különösen sérelmes lehet az érintett számára. Ezen adatok jogellenes kezelése negatívan befolyásolhatja az egyén jó hírnevét, magán- és családi életét, hátrányos megkülönböztetés oka vagy indoka lehet az érintettel szemben. A már említett (75) preamubulumbekezdés az egészségügyi adatok kezelését önmagában is olyan adatkezelésnek minősíti, amely az érintett személyek jogaira és szabadságaira nézve alapvetően kockázatos. (…)

A csupán egy egyszerű internetes link birtokában a kezelt egészségügyi adatokhoz való illetéktelen hozzáférések megakadályozásán túl, a konkrét hozzáférések (tkp. ebben az ügyben külső dokumentumletöltések), akár külső rosszindulatú támadások naplózására való képesség, továbbá az illetéktelen hozzáférő személyét kimutatni tudó hálózatbiztonsági eszközök megfelelő beállítások melletti, naprakész alkalmazása az Ügyfél IBSZ-ében is meghatározása került, mint belső szabály. A Hatóság megjegyzi, hogy véleménye szerint ezek a belső szabályok egyébként – az általános adatvédelmi rendelet 32. cikkében foglaltaknak megfelelően – a tudomány és technológia jelen állása szerint is elvárható biztonsági intézkedések nagyszámú egészségügyi adat kezelése kapcsán. Ez főleg igaz az olyan piaci szereplőkre, amelyek anyagi hasznot is realizálnak az ilyen adatok kezelésével összefüggő főtevékenységükkel. Az Ügyfél az illetéktelen hozzáférések kimutatásának elégtelenségével ezért nem csupán saját belső szabályzatának, hanem a kockázatokkal arányos, általánosan elvárható védelmi szintnek sem felelt meg."

[561] Informatikai Biztonsági Szabályzat

Ügyfélkapus azonosítók nyilvánosságra kerülése

(NAIH/2020/1137)
Bírság: 500 ezer Ft

„A Hatósághoz egy magánszemélytől közérdekű bejelentés érkezett, amelyben a bejelentő leírta, hogy birtokába került egy lista, amely természetes személyek és vállalkozások (kb. 100 db) különböző adatait tartalmazza. A lista az érintettek teljes nevét, adóazonosítóját, TAJ számát, születési adatait, édesanyjuk nevét, továbbá a magyarorszag.hu honlapon keresztül elérhető ügyfélkapus felhasználói neveiket és titkosítatlan jelszavaikat tartalmazza.

A beadványt előterjesztő elmondása szerint a lista úgy került a birtokába, hogy azt a […] alatti ingatlanjának kertjében szedte össze […] a szél által odafújt egyéb papírszemetekkel együtt. A megtalált listát a beadványozó eredetben továbbította a Hatóság részére. (…)

A NISZ Zrt. megerősítette, hogy a listában valóban az Ügyfélkapuhoz tartozó adatok szerepelnek, amelyek két cég és egy egyéni vállalkozó kivételével valósak és a jelen állapotot tükrözik. (…) A NISZ Zrt. elmondása szerint ezért a megtalált listában szereplő jelszavakat még a BM sem kezeli, csupán azok visszafejthetetlen lenyomata szerepel a nyilvántartásukban. A jelszót csak az a személy ismerheti, aki a regisztrációt elvégezte.

A NISZ Zrt. véleménye szerint a lista valószínűleg egy könyvelő által vezetett ügyfél adatbázis lehet, mivel abban szerepel még az adóazonosító, a TAJ szám és ÜCC kód is, amely adatok nem kapcsolódnak a KÜNY-höz[562]*.(…)*

A Hatóság a feltárt tényállás alapján megállapította, hogy a bekövetkezett adatvédelmi incidensről az Ügyfél saját elmondása szerint legkorábban akkor szerzett tudomást, amikor 2019. május 20-án az ügy ezirányú részleteiről is értesült a Hatóság NAIH/2019/4152/2. számú tényállás tisztázó végzéséből. (…)

Az általános adatvédelmi rendelet (75) preambulumbekezdésében foglaltak szerint, ha az adatkezelésből – így jelen ügyben az eszközök rendeltetésszerű használatából – személyazonosság-lopás vagy személyazonossággal való visszaélés fakadhat, úgy az alapvetően kockázatosnak minősül. Az Ügyfél kezeléséből kiszivárgott listán található adatok (érintett teljes neve, adóazonosítója, TAJ száma, születési adatai, édesanyjuk neve, a magyarorszag.hu honlapon keresztül elérhető ügyfélkapus felhasználói nevek és titkosítatlan jelszavaik) ismeretében pedig elkövethető személyazonosság-lopás, vagy személyazonossággal visszaélés, az érintett ügyfélkapus hozzáférésének tudta nélküli használata, ott tárolt egyéb adatok jogosulatlan megismerése.

A fentiek alapján a Hatóság megítélése szerint az adatvédelmi incidens alapvetően kockázatosnak tekinthető (…)

[562] Központi Ügyfél-regisztrációs Nyilvántartás

Az általános adatvédelmi rendelet 34. cikk (1) bekezdése alapján továbbá ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. A rendelet (86) preambulumbekezdése szerint a tájékoztatás fő célja, hogy az érintett is megtehesse a szükséges óvintézkedéseket az incidensből fakadó kockázatok mérséklése érdekében. A Hatóság jelen ügyben az incidenst, olyan magas kockázatú incidensnek tekinti, amely indokolja az érintettek tájékoztatását.

Az incidensről való tájékoztatásra a Hatóság megítélése szerint kifejezetten azért is van szükség, mivel az érintett magánszférájára jelentett kockázat a személyazonosításra alkalmas adatok közül különösen a felhasználónév és titkosítatlan jelszó párok nyilvánosságra kerülése esetén olyan jellegű (ezen adatok birtokában nagyon könnyen elkövethető személyazonossággal visszaélés), amelynek kockázatai csak úgy mérsékelhetők eredményesen, ha az érintettek erről tudomással bírnak, és megtehetik az általuk szükségesnek tartott további intézkedéseket.

A felhasználók szempontjából szinte minden esetben magas kockázatú körülményként kell értékelni a Hatóság megítélése szerint, ha egy rendszerbe történő belépést szolgáló felhasználónév és jelszó titkosítatlan (vagy akár nem megfelelően, elavult technikai módszerrel titkosított) formában kerül nyilvánosságra. Ennek fő oka, hogy a felhasználók ugyanezeket az adatokat esetleg más (leginkább online, de akár offline) szolgáltatás használata során is használhatják. A felhasználók jellemzően nem generálnak minden egyes internetes szolgáltatáshoz önálló felhasználónevet és jelszót, hanem nagyon sokszor ugyanazokat (vagy bizonyos változatait) használják."

Digi Távközlési és Szolgáltató Kft

(NAIH/2020/1160/10)
Bírság: 100 millió Ft

„A bejelentés szerint az Ügyfél legkésőbb 2019. szeptember 23-án szerzett arról tudomást, hogy egy támadó a www.digi.hu honlapon keresztül elérhető sérülékenységet kihasználva hozzáfért körülbelül […] érintett személyes adataihoz, akik nagyobb részt (kb. […] fő) az Ügyfél megrendelői és előfizetői, kisebb részt (kb. […] fő) pedig hírlevére feliratkozók voltak. A megrendelői, előfizetői személyes adatok között megtalálható volt az érintettek neve, anyja neve, születési helye és ideje, lakcíme, személyi igazolványszáma (esetenként személyi száma), e-mail címe, vezetékes és mobil telefonszáma. (…)

Az Ügyfél úgy szerzett tudomást a támadásról, hogy azt maga a támadó (etikus hacker) jelezte neki […]. A jelzésében a támadó jelezte, hogy – elmondása szerint – csak az érintett adatbázis egy sorát kérte le bizonyítékként, szándékai pedig segítő jellegűek, ezért a hiba technikai jellegét is ismertette Ügyfél előtt. Az Ügyfél ezek után a hibát kijavította, […].

Az incidenssel érintett adatok nagyobb része (kb. […] fő) egy […]-én tesztelési célból létrehozott […] megnevezésű adatbázis részét képezték. (…)

A hiba kiküszöbölése kapcsán létrehozott fenti tesztadatbázisba betöltött adatok forrását az Adatkezelő ügyfelei által korábban megadott személyes adatok képezték. (…)

A fenti hiba elhárítását, így az elérések helyreállítását követően a tesztadatbázisba feltöltött adatokat törölni kellett volna, ez azonban mulasztás következtében elmaradt. Ezen adatoknak a fenti sérülékenységen keresztüli elérhetőségéről a támadó bejelentéséig nem volt tudomása az Ügyfélnek. Az adatokhoz való hozzáférést a támadó részéről az Ügyfélnek nem sikerült detektálnia (pl. hálózatbiztonsági eszköz jelzése alapján), mielőtt arra maga a támadó felhívta volna a figyelmét.

A tesztadatbázison túl a felfedezett sérülékenységen keresztül a támadónak lehetősége volt hozzáférni az Ügyfél által fenntartott digi.hu honlap mögötti másik, […] adatbázishoz is, amely az oldalon hírlevélre feliratkozó érintettek személyes adatait tartalmazta. (…)

A jogosulatlan hozzáférést lehetővé tevő hiba oka, hogy az Ügyfél által használt […] 1 tartalomkezelő rendszerben megtalálható volt egy biztonsági rés, amit kihasznált a támadó. A biztonsági rés egyébként már több mint 9 éve ismert volt és rendelkezésre állt hozzá javítás is, amit azonban az Ügyfél korábban nem telepített. Ennek oka, hogy a javítás nem képezte részét a szoftverhez hivataloson kiadott javítás-csomagoknak. Az incidenst követően a javítócsomag telepítése megtörtént. (…)"

A bírságkiszabás szükségességének megállapítása során a Hatóság mérlegelte a jogsértések súlyosító és enyhítő körülményeit az alábbiak szerint:
Súlyosító körülmények:

- ✓ az Ügyfélnél bekövetkezett adatvédelmi incidens egy olyan adatbiztonsági hiányosságra vezethető vissza, amelyre a piacon régóta elérhető volt az ingyenes javítás, a sérülékenység pedig akár harmadik személy által is könnyen detektálható volt, így az adatokhoz való jogosulatlan hozzáférésnek való kitettség elhárítására az Ügyfélnek a kockázatok megfelelő felmérése esetén nagyon régóta lehetősége lett volna;
- ✓ az Ügyfél által az ügy kapcsán érintett adatok nagy száma, azok érzékenysége által jelentett kockázatok, továbbá az Ügyfél piaci pozíciója, amelyek alapján fokozottan elvárható tőle a megfelelő adatbiztonsági intézkedések alkalmazása;
- ✓ ahogy az saját belső szabályzataiban is megjelenik, az Ügyfél által használt (nyílt forráskódú) tartalomkezelő rendszer használatából adódó kockázatokat, illetve azok felmérését az Ügyfélnek kell viselnie és azokkal kapcsolatban helyt állnia. Az Ügyfél ezen intézkedések hiányával saját belső szabályzatai előírásainak sem tett megfelelően eleget;
- ✓ az érintett személyes adatokra alkalmazott titkosítás és ezzel kapcsolatos kockázatok felmérésének hiánya is megnövelte az incidensnek való kitettség kockázatait. Ezen intézkedés alkalmazása szintén megjelenik az Ügyfél vonatkozó belső szabályzataiban, amelynek szintén nem, illetve hiányosan tett eleget;
- ✓ a digi.hu honlap tekintetében az adminisztrátori (rendszergazdai) jogosultsággal rendelkező felhasználók érintettségét a Hatóság a biztonsági kockázatokat súlyosan növelő tényezőként vette figyelembe;

- ✓ a Hatóság a megállapított adatbiztonsági hiányosságokat olyan rendszerszintű problémának tekintette, amely alapján a jogsértő helyzet már az incidens bekövetkezése előtt is régóta fennállt az adatkezelő Ügyfélnél az érintett adatbázisok tekintetében;
- ✓ az adatbiztonsági hiányosságokon túl az incidens bekövetkezése közvetlenül visszavezethető a hibaelhárítási célból létrehozott tesztadatbázis alapelvi szinten jogsértő cél nélküli és az érintettek azonosítására alkalmas módon való hosszú ideig történő tárolására. Amennyiben a tesztadatbázis az alapelveknek megfelelően törlésre került volna a hibajavítási cél megvalósulása után, úgy az incidens által az érintettekre jelentett kockázatok is sokkal enyhébbek lettek volna, mivel az érintett adatalanyok száma ezen, tesztadatbázisban szereplők számával csökkenthető lett volna. Az adatbiztonsági hiányosságok a tesztadatbázis időben való törlése esetén csupán a direktmarketing adatbázisban kezelt személyes adatok és a digi.hu honlap rendszergazdai adatai esetén álltak volna fent;
- ✓ a cél nélkül kezelt adatok beazonosítását, az adatok megtisztítását, aktualizálását és szükség szerint törlését az Ügyfél belső előírásai is tartalmazták, amely szintén ellentétben állt az incidensben érintett tesztadatbázis kezelésének körülményeivel;
- ✓ az adatbiztonsági hiányosságok és az alapelvi szinten jogsértő adatkezelés nagyszámú érintett személyes adatait érintette, amely tartalmazza az Ügyfél lakossági ügyfeleit. Ez az ország lakosságának arányához viszonyítva is jelentős szám;
- ✓ a Hatóság a bírság összegének meghatározása során figyelembe vette, hogy az Ügyfél által elkövetett alapelvi jogsértések az általános adatvédelmi rendelet 83. cikk (5) bekezdése szerint a magasabb maximális összegű bírságkategóriába tartozó jogsértésnek minősülnek.

Budapest Főváros Kormányhivatala XI. kerületi Hivatala

(NAIH-2894-3/2021)
Bírság összege: 10 millió Ft.

„Ügyfél megsértette az általános adatvédelmi rendelet 32. cikk (1) bekezdés a)-b) pontjait és (2) bekezdését, amikor nem alkalmazott az egészségügyi adatok továbbításának kockázataival arányos adatbiztonsági intézkedéseket: Ügyfél a Covid-19 gyorstesztthez kapcsolódóan kezelt, rendkívül részletes és pontos egészségügyi adatokat és elérhetőségeket is tartalmazó adatbázist egy Excel-fájlban, körzetenkénti leválogatás nélkül, továbbá azok bizalmasságát garantáló hozzáférésvédelem vagy titkosítás alkalmazása nélkül egyszerű e-mailben továbbította a címzett körzeti orvosoknak. Ügyfél ezen adattovábbítással így közvetlenül lehetővé tette a magas kockázatú adatvédelmi incidens bekövetkezését.

Ügyfél megsértette az általános adatvédelmi rendelet 33. cikk (1) bekezdését, amikor a bekövetkezett magas kockázatú adatvédelmi incidensnek a Hatóság felé történő bejelentését nem tartotta szükségesnek, mivel nem megfelelően végezte el a kockázatelemzést.

Ügyfél megsértette az általános adatvédelmi rendelet 34. cikk (1) bekezdését, amikor a bekövetkezett magas kockázatú adatvédelmi incidensről nem kívánta tájékoztatni az érintetteket. (…)

A Hatóság megítélése szerint amennyiben az Ügyfél az adatok körzetek szerinti leválogatását és legalább jelszavas védelmet, továbbá a jelszó külön csatornán való megküldését alkalmazta volna a fájllal kapcsolatban, úgy az ügyben az adatbiztonság sérelme és emiatti adatvédelmi incidens sem következett volna be. A természetes személyek alapvető jogainak, így személyes adataik védelme szempontjából a Covid-19 járvány miatti veszélyhelyzet nem adhat teljes felmentést a megfelelő adatbiztonsági előírások betartása alól.

A Hatóság ugyanakkor ki kívánja ehelyütt azt is emelni, hogy az egészségügyi adatok továbbításával kapcsolatban egyáltalán nem tartja jó gyakorlatnak azok egyszerű Excel táblázatban, titkosítás nélkül, e-mailben történő elküldését. Erre sokkal biztonságosabb megoldást kínál egy erre a célra létrehozott, biztonságos platform (pl. az Egészségügyi Elektronikus Szolgáltatási Tér) használata."

ROBINSON-TOURS & Next Time Media Ügynökség Kft

(NAIH/2020/66/21)
Bírság összege:

- „ROBINSON-TOURS" Idegenforgalmi és Szolgáltató Kft. „f.a." („Ügyfél 1."): 20 millió forint
- Next Time Media Ügynökség Kft (Ügyfél 2.).: 500 ezer forint.

A hatóság megállapította, hogy Ügyfél 1.

- ✓ *„nem tett eleget (…) a beépített és alapértelmezett adatvédelem elvének, mivel a weboldala kialakításával nem megfelelően kiválasztott adatfeldolgozót bízott meg, ami súlyos, alapelvi szinten jogsértő és nem biztonságos adatkezelési tervezési hiányosságokhoz vezetett. A tervezési, kialakítási hiányosságok közvetlenül lehetővé tették azt, hogy az adatkezelés bizalmas jellegének sérülésével magas kockázatú adatvédelmi incidens következett be" [GDPR 25. cikk (1)-(2) bekezdés];*
- ✓ *„az általa kínált utazási szolgáltatásokkal összefüggésben kezelt személyes adatokat tároló rendszerét és honlapját úgy használta és üzemeltette, hogy ahhoz bárki hozzáférhetett az interneten keresztül egy sérülékenység fennállása miatt. Ezen hiányosság miatt az adatok kezelésének bizalmas jellege súlyosan sérült, ami közvetlenül lehetővé tette a magas kockázatú adatvédelmi incidens bekövetkezését." [GDPR 32. cikk (1) bekezdés b) pont];*
- ✓ *„nem tett eleget (…) tájékoztatási kötelezettségének a bekövetkezett adatvédelmi incidenssel kapcsolatban, amikor nem tájékoztatta a magas kockázatú adatvédelmi incidensről az érintetteket. [GDPR 34. cikk (1) bekezdés].*

A hatóság megállapította Ügyfél 2. mint adatfeldolgozó esetében, hogy „*az incidenssel érintett adatbázishoz bárki hozzáférhetett az interneten keresztül egy sérülékenység fennállása miatt, így az adatok feldolgozásának bizalmas jellege súlyosan sérült. Ennek oka, hogy Ügyfél 2. a weboldal üzemeltetése során az érintett teszt- és éles*

adatbázisok közötti kapcsolatot nem szüntette meg, továbbá a weboldalt nem vetette alá megfelelő biztonsági ellenőrzéseknek, sérülékenységi teszteknek. A mulasztás közvetlenül lehetővé tette a személyes adatok elérhetőségét és így az adatvédelmi incidens bekövetkezését." [GDPR 32. cikk (1) bekezdés b) pont]

„A Hatósághoz 2019. december 29-én közérdekű bejelentés érkezett, amely arra hívta fel a figyelmet, hogy a https://www.lastminute.robinsontours.hu/partnerkapu_foglalasaim weboldalon keresztül bárki számára elérhetőek Ügyfél 1. természetes személy ügyfeleinek személyes adatai, így többek között utasok neve, elérhetőségei, lakcímadatok, személyi igazolvány és útlevélszámok, foglalással és utazással, úticéllal, szállással, valamint a szerződéskötéssel kapcsolatos adatok. Az adatok https://www.robinsontours.hu/partnerkapu_foglalasaim linken keresztül is elérhetőek voltak. A bejelentés szerint erre a bejelentő úgy jött rá, hogy internetes böngészés közben édesapja nevét írta be a Google keresőjébe, majd az egyik találaton keresztül, bármilyen jogosultság ellenőrzés nélkül sikerült megnyitnia egy adatbázist.

A Hatóság ellenőrizte a fenti linkeket és NAIH/2020/66/2., NAIH/2020/66/3. és NAIH/2020/66/5. ügyiratszámú feljegyzéseiben megállapította, hogy a linkek birtokában, azt a webböngészőbe beírva, bármilyen jogosultságellenőrzés, vagy más informatikai biztonsági intézkedés közbeiktatása nélkül a weboldalon – a bejelentő által állítottaknak megfelelően – elérhető egy adatbázis, amely különböző természetes személy ügyfelek személyes adatait tartalmazza. Az adatbázisban található adatok alapján valószínűsíthető, hogy a legtöbben az utazási irodaként működő Ügyfél 1. utazási szolgáltatásait igénybe vevő ügyfelek. A Hatóság arról is meggyőződött, hogy az adatbázisban tárolt adatokhoz a Google keresőben rákeresve (pl. egy utas nevére való keresés) is el lehet jutni. A tartalmakat tehát a Google keresőmotorja is felderítette, és abban ezeket kulcsszavas kereséssel elérhetővé tette.

Az elérhető személyes adatok a következőek:

- *„vezérutas" neve,*
- *útitársak száma és neve,*
- *indulás és érkezés dátuma, foglalás dátuma,*
- *foglalás státusza (végleges/törölt/lekérés alatt),*
- *foglalási szám,*
- *lakcímadatok (ország, irányítószám, település, utca, házszám, emelet, ajtó pontossággal),*
- *személyi igazolvány száma kiállítási és lejárati dátummal együtt,*
- *útlevél száma kiállítási és lejárati dátummal együtt,*
- *e-mail cím, telefonszám,*
- *utazási szerződés készítésének dátuma.*

A honlapon a személyeket úticél és dátum alapján is lehetséges volt szűrni. Az adatbázisban ezen felül az egyes ügyfelekhez lehetősége van bárkinek útlevél fotót feltölteni, illetve megjegyzést írni az egyes foglalások mellé. Az útlevél fotó feltöltés lehetőségét választva nem csak képeket, hanem gyakorlatilag bármilyen formátumú fájlt ki lehetett választani feltöltésre.

A linkeken keresztül megtekinthető táblázat összesen 375 rekordot tartalmazott. Ezek között voltak valószínűsíthetően fiktív személyek is (pl.: „TESZT TESZT", „TESZT IVÁN" stb.), azonban többségük létező természetes személy ügyfeleket takart. Az útitársak száma és neve alapján ennél azonban sokkal több, ezer feletti személy adatai is elérhetőek voltak a honlapon keresztül.

A linkeken keresztül elérhető adatbázisból lehetőség volt arra is, hogy az egyes ügyfelekkel kötött utazási szerződéseket bárki szabadon letölthesse pdf formátumban. Az egyes szerződések közül a Hatóság eljáró ügyintézője bizonyítékul letöltött öt darabot, valamint egy e-mail-es foglalási igazolást is. A letölthető szerződések részletesen tartalmazták valamennyi szerződő utas személyes adatait, az úticélt, az utazás dátumát, a lefoglalt szállás adatait és a szolgáltatás bruttó árát személyekre bontva.

A Hatóság a fentiekre tekintettel hatósági ellenőrzést indított 2020. január 30-án, mivel a rendelkezésre álló adatok nem voltak elegendőek annak megítéléséhez, hogy Ügyfél 1. maradéktalanul eleget tett-e az általános adatvédelmi rendeletben foglalt kötelezettségeinek, így különösen a 32-34. cikkében foglaltaknak.

A későbbi napokon (2020. február 3.) történő, NAIH/2020/66/7. számú feljegyzéssel dokumentált újraellenőrzés szerint a nyilvánosan elérhető adatbázishoz folyamatosan újabb rekordok, benne személyes adatokkal és kapcsolódó szerződésekkel kerültek hozzáfűzésre, feltöltésre. Az ügyféladatbázis frissülése tehát ily módon élőben követhető volt a honlapon keresztül. Az adatbázis 2020. február 4-én már nem volt viszont ily módon elérhető. (…)

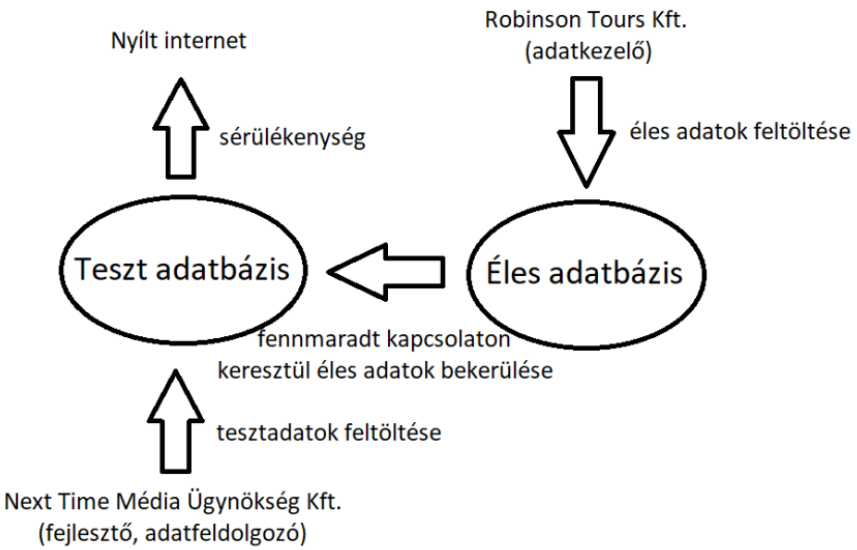
Ügyfél 1. incidensbejelentése alapján a sérülékenység 2019. november 13-tól 2020. február 4-ig állt fent a honlapon keresztül. A sérülékenység összesen 781 érintett, összesen kb. 2506 darab személyes adatát érintette, amelyek: név, cím, születési dátum, útlevél száma és lejárati dátuma, személyi igazolvány száma és lejárati dátuma, e-mail cím, telefonszám, indulás és érkezés dátuma, valamint az egyes utazási szerződések pdf formátumban és az abban található adatok (pl. szerződéses érték). Az incidenssel érintett adatbázisban kiskorúak adatai is szerepeltek. Az érintettek személyi köre Ügyfél 1-nél 2019. november 13. és 2020. február 4. közötti időszakban utazásokat foglaló magyar nemzetiségű utasokat és idegenvezetőket ölelt fel.

A Hatóság végzésének kézhezvétele után Ügyfél 1. azonnal jelezte telefonon Ügyfél 2-nek a sérülékenységet, aki haladéktalanul intézkedett arról, hogy URL-eken keresztül ne lehessen a továbbiakban elérni az éles adatokkal frissülő tesztkörnyezetet. Ügyfél 1. megítélése szerint az adatvédelmi incidenst kiváltó sérülékenység összességében Ügyfél 2. nem körültekintő, gondos eljárásából fakadt. Ügyfél 1. továbbá közölte a Hatósággal, hogy az incidens miatt szabályozási anyagát felülvizsgáltatja. Ügyfél 1. azt is közölte, hogy az érintettek tájékoztatását tervezi a hatósági eljárás eredményéről, annak lezárását követően. (…)

Ügyfél 1. ismertette, hogy a sérülékenység fennállásának időszakában (2019. november 13. – 2020. február 4.) összesen két IP címről történt külső, jogosulatlan hozzáférés 28 darab foglalás összesen 30 db dokumentumához, négy alkalommal

(2020. január 30. és 31., továbbá február 1. és 3. napjain). Kimutatható adatvédelmi incidens így ténylegesen ezen alkalmakkal kapcsolatban valósult meg.

Ügyfél 1. kifejtette, hogy a fejlesztés során létrejött tesztkörnyezet és ahhoz tartozó tesztadatbázis – tekintve, hogy a tesztelés nem éles adatokkal történt – nem került levédésre. A tesztelés végén az adatállomány azonban nem került törlésre és kapcsolatban maradt a különálló, immár éles rendszerrel és adatbázissal is. Az éles rendszerbe Ügyfél 1. által bevitt személyes adatok a tesztadatbázisba is átkerültek, mivel a két rendszer között fennmaradt egy adatkapcsolat. A sérülékenységen keresztül az éles adatokkal is folyamatosan frissülő tesztadatbázis volt elérhető (lásd az alábbi ábrát).



A sérülékenységen keresztül elérhető adatbázisban összesen 309 darab utazási szerződéshez lehetett hozzáférni. Ezek a korábbiakban ismertetett szerint összesen 781 érintett, összesen kb. 2506 darab személyes adatát tartalmazták. Az érintettek közül összesen 46 volt gyermekkorú (18 éven aluli).

(...)

Az adatvédelmi incidenst kiváltó sérülékenységről Ügyfél 1. saját elmondása szerint először a Hatóság NAIH/2020/66/4. ügyiratszámú tényállástisztázó végzéséből 2020. február 4-én szerzett tudomást. Korábban a sérülékenységről és az adatvédelmi incidensről nem volt tudomása. Ügyfél 1. utazási szolgáltatásait igénybe vevő érintettek adatait is tartalmazó adatbázishoz való hozzáférést Ügyfél 1-nek nem sikerült magától detektálnia, így az incidensről és azt lehetővé tévő sérülékenységről pusztán a Hatóság jelzése alapján értesült.

A Hatóság (...) magas kockázatot megalapozó körülményként értékeli, hogy az adatbázishoz mind a közérdekű bejelentő, mind a Hatóság hozzáfért, viszont az

illetéktelen hozzáférések teljes száma és a hozzáférők személye a sérülékenység idejére vonatkozó teljes naplóállomány hiányában nem mérhető pontosan fel. A hozzáférők személyét és számát Ügyfél 1. utólag már nem tudja felmérni és azonosítani, amely az incidensben érintett személyes adatok további sorsával kapcsolatban nagyfokú bizonytalanságra, aggodalomra ad okot. Az adatkezelő az általa felmérhetetlen fokú és mértékű, de bizonyítottan megtörtént adatszivárgásnál csak az érintettek tájékoztatásával próbálhatja meg csökkenti jelen esetben az egyébként is magas kockázatokat.

A Hatóság megítélése szerint a magas kockázatot megalapozó további körülmények, hogy az adatbázisban kezelt személyes adatokat a Google is indexálta, azok ezen keresőmotoron keresztül is elérhetőek voltak, így azokra sokkal könnyebben rá lehetett akár egyszerű internetes böngészés, névre történő találomra való rákeresés során is bukkanni. (…)

Ügyfél 1. adatkezelőként felelősséggel tartozik azért, hogy a bekövetkezett adatvédelmi incidens kockázatait fel tudja mérni. Ennek oka, hogy elsősorban az adatkezelő van tisztában azzal, hogy milyen személyes adatokat, milyen célokból és adatkezelési módszereket alkalmazva kezel. Az adatvédelmi incidens esetleges magas kockázati besorolása és ezért arról az érintetti tájékoztatás szükségességének megítélése Ügyfél 1. fő feladata, ezen kérdés megítélését nem háríthatja át a „hatósági eljárás eredményeinek függvényeire" hivatkozva a felügyeleti hatóságra. Az adatkezelőnek az érintetteket indokolatlan késedelem nélkül kell tájékoztatnia az incidensről, amint a tudomására jutott az általános adatvédelmi rendelet 34. cikke alapján, nem várhat a hatósági eljárás lezárulásáig. (…)

Az adatvédelmi incidenssel érintett rendszerben fennálló sérülékenység abból adódóan valósulhatott meg, hogy a személyes adatok kezelése során nem megfelelő biztonsági beállításokat alkalmaztak az érintett rendszerben az alábbiak szerint.

Ügyfél 2. a weboldal üzemeltetése során az érintett teszt- és éles adatbázis közötti kapcsolatot nem szüntette meg, továbbá a weboldalt nem vetette alá megfelelő biztonsági, sérülékenységi teszteknek. A tesztadatbázis és már valós adatokkal Ügyfél 1. által feltöltött és használt éles adatbázis között így fennmaradt egy kapcsolódási csatorna, amelyen keresztül az éles adatok folyamatosan, valós időben továbbításra kerültek a tesztadatbázisba. Ezt a valós idejű kapcsolatot Ügyfél 1. és Ügyfél 2. nyilatkozatai mellett a Hatóság által dokumentált próbaletöltések és hozzáférések is megerősítik.
A sérülékeny, éles adatokat tartalmazó tesztadatbázis azért volt elérhető a biztonsági résen keresztül, mivel annak biztonságával Ügyfél 2. a fejlesztés befejezése után már nem foglalkozott. Az incidens nem következett volna be, ha a tesztadatbázist Ügyfél 2. törli, vagy azt biztonságos környezetbe áthelyezi, vagy kapcsolatát az éles adatbázissal megszünteti. Ezek a mulasztások tehát közvetlenül lehetővé tették a személyes adatok elérhetőségét.

A tesztadatbázis a fentiek értelmében gyakorlatilag az éles adatbázis sérülékeny másolataként funkcionált, melynek mérete az idő előrehaladtával folyamatosan nőtt. Ez az ügyféladatok duplikálását eredményezte majd három hónapon keresztül. A

személyes adatokhoz rendkívül könnyen hozzá lehetett kívülről férni, anélkül, hogy ezt Ügyfél 1. vagy Ügyfél 2. észlelte volna.

Ügyfél 1. az általa kínált utazási szolgáltatásokkal összefüggésben kezelt személyes adatokat tároló rendszerét és honlapját a fentiek miatt úgy használta és üzemeltette, hogy ahhoz bárki hozzáférhetett az interneten keresztül egy sérülékenység fennállása miatt. Ezen biztonsági hiányosság miatt az adatok kezelésének bizalmas jellege súlyosan sérült, ami közvetlenül lehetővé tette a magas kockázatú adatvédelmi incidens bekövetkezését.

Ügyfél 1. is hivatkozott arra, hogy adatfeldolgozóként Ügyfél 2. nem járt el a rendszer kiépítése során elég körültekintően és gondosan, továbbá a rendszerhez nem volt jogosultságellenőrzési rendszer kiépítve.

A fentiekre tekintettel a Hatóság megállapítja, hogy

- *Ügyfél 1. az adatok rendszerbe való betöltése és ottani kezelése, tulajdonképpen a rendszer használata,*
- *Ügyfél 2. a rendszer hanyag üzemeltetése és nem megfelelő biztonsági ellenőrzése és tesztelése révén,*

megsértették az általános adatvédelmi rendelet 32. cikk (1) bekezdésének b) pontját, mivel a szolgáltatás futása során annak bizalmas jellegét sem az adatkezelés, sem az adatfeldolgozás során nem tudták garantálni. (…)

Ügyfél 2. az incidenssel érintett adatkezelés bizalmasságának garantálása kapcsán kifejtette, hogy az általa fejlesztett rendszer (ami gyakorlatilag Ügyfél 1. weboldala) egészét a fejlesztés során nem tesztelte, nem vizsgálta biztonsági szempontból, csupán „a belépési pont körül" végzett ellenőrzéseket, az incidenshez vezető hibát így korábban nem észlelhette. Ügyfél 2. továbbá a lefolytatott ellenőrzésekről sem rendelkezik jegyzőkönyvekkel, amelyekkel megtörténtüket bizonyítani tudná. Ügyfél 1. megbízása keretei között Ügyfél 2. tehát elmulasztotta elvégezni a weboldal és a rendszer megtervezése és kifejlesztése során azon biztonsági teszteket, illetve más intézkedéseket, amelyekkel a sérülékenységhez vezető okok kiszűrhetőek vagy megszüntethetőek lettek volna (pl. weboldal sérülékenység vizsgálata, a teszt- és éles adatbázis fennmaradó kapcsolatának megszüntetése, a tesztkörnyezet nyílt elérhetőségének megszüntetése).

A fenti tervezési intézkedések hiánya lehetővé tette, hogy mind az oldalra mutató link ismeretében, mind a Google keresőjén keresztül bárki, bármilyen előzetes jogosultságellenőrzés nélkül hozzáférjen az online felületen tárolt személyes adatokhoz és dokumentumokhoz. (…)

Az adatkezelés meghatározásakor, így jelen esetben a weboldal és kapcsolódó informatikai infrastruktúra megtervezése és kifejlesztésekor alkalmazott intézkedések nem voltak elegendőek ahhoz, hogy az általános adatvédelmi rendelet 25. cikkének megfelelően az adatkezelés bizalmas jellegét biztosítsák. Ennek köszönhetően később, a weboldalon keresztül a személyes adatok hozzáférhetővé váltak meghatározatlan számú személy számára.

Adatkezelőként Ügyfél 1. felelősséggel tartozik az általa megbízott adatfeldolgozó (Ügyfél 2.) tevékenységéért, így az adatfeldolgozói szerződés megkötése során kellő

gondossággal kell eljárnia a megfelelő adatfeldolgozó kiválasztásakor. Az adatfeldolgozói szerződés keretei között Ügyfél 2. hanyagul tervezte meg és fejlesztette ki a rendszert, amelyre csak az adatvédelmi incidens bekövetkezéskor derült fény, arról korábban sem Ügyfél 1., sem Ügyfél 2. nem szerzett tudomást.

Az alapelvi szinten jogsértő, nem biztonságos és súlyos incidenshez vezető adatkezelés így gyakorlatilag determinálva volt már a rendszer tervezési és kialakítási fázisában, amikor még a konkrét adatkezelés el sem kezdődött. A későbbi jogsértések bekövetkezése egyenes következménye a hanyag tervezésnek és a nem megfelelő adatfeldolgozó megbízásának. (…)

(…) Ügyfél 1. vonatkozásában (…)

A Hatóság súlyosbító körülményként vette figyelembe a következőket:

- *Az incidenssel érintett személyes adatok kezelése az adatok jellegéből fakadóan magas kockázattal jár, ezért az adatkezelőknek fokozott elővigyázatossággal kell eljárniuk a kockázat mértékének megfelelő szintű adatbiztonság garantálása érdekében. Ügyfél 1. ennek ellenére nagyszámú személyes adat (összesen 781 érintett, összesen kb. 2506 darab személyes adata, köztük gyermekkorúak adatai és szerződéses összegekre vonatkozó adatok) kezelésére használt rendszere folyamatos bizalmas jellegének biztosítása érdekében nem hozott megfelelő intézkedéseket.*
- *(…) egy alapvetően magas kockázatú adatkezelés tekintetében Ügyfél 1. a jogosulatlan hozzáférések kiküszöbölésére és kimutatására alkalmatlan, a kockázatokkal aránytalan adatbiztonsági intézkedéseket alkalmazott,* amikor *a személyes adatokhoz rendkívül könnyen hozzá lehetett kívülről férni, anélkül, hogy ezt Ügyfél 1. észlelte volna. Az ilyen adatok kezelésére való biztonsági felkészültség profit alapú vállalkozásoktól fokozottan elvárható.*
- *A Hatóság az adatvédelmi incidensről közérdekű bejelentés alapján szerzett tudomást, Ügyfél 1. által az adatvédelmi incidens észlelésére nem került sor.*
- *A Hatóság a megállapított adatbiztonsági hiányosságokat olyan rendszerszintű problémának tekinti, amely alapján a jogsértő helyzet már a bizonyítható jogosulatlan hozzáférések bekövetkezése előtt is hónapokkal fennállt az adatkezelőnél az érintett tesztadatbázis tekintetében.*
- *Az adatkezelés bizalmasságának sérülése gyakorlatilag determinálva volt már a rendszer hanyag megtervezésekor, amikor még a konkrét adatkezelés el sem kezdődött. A későbbi jogsértő adatkezelés egyenes következménye a hanyag tervezésnek és a nem megfelelő adatfeldolgozó megbízásának.*
- *Ügyfél 1. adatkezelőként felelősséggel tartozik azért, hogy a bekövetkezett adatvédelmi incidens kockázatait fel tudja mérni. Ennek oka, hogy az adatkezelő van tisztában azzal, hogy milyen személyes adatokat, milyen célokból és adatkezelési módszereket alkalmazva kezel. Az adatvédelmi incidens esetleges magas kockázati besorolása és ezért arról az érintetti tájékoztatás szükségességének megítélése Ügyfél 1. fő feladata, ezen kérdés megítélését nem háríthatja át a „hatósági eljárás eredményeinek függvényeire" hivatkozva a felügyeleti hatóságra. Az adatkezelőnek az érintetteket indokolatlan késedelem nélkül kell tájékoztatnia az incidensről, amint a tudomására jutott az általános adatvédelmi rendelet 34. cikke alapján, nem várhat a hatósági eljárás lezárulásáig.*

A Hatóság enyhítő körülményként vette figyelembe a következőket:

- *Az eljárás során a Hatóságnak nem jutott tudomására olyan információ, amely arra utalna, hogy az érintetteket a jogsértés nyomán kár érte volna.*
- *A feltárt tényállásból arra lehet következtetni, hogy a jogsértés nem volt szándékos, azt Ügyfél 1. gondatlansága okozta. Erre utal az is, hogy az Ügyfél az incidensről való tudomásszerzést követően azonnal intézkedéseket tett a feltárt sérülékenység megszüntetése érdekében.*
- *A Hatóság figyelembe vette, hogy az Ügyféllel szemben korábban nem állapított meg a személyes adatok kezelésével kapcsolatos jogsértést.*

Egyéb, figyelembe vett körülmények:

- *A bekövetkezett adatvédelmi incidensről való értesülése után Ügyfél 1. az incidens kezelésével kapcsolatos szinte valamennyi, az általános adatvédelmi rendelet 33. cikkei által előírt intézkedést azonnal megtette, így az incidenst kivizsgálta, azt a Hatóság részére a tudomásszerzéstől számított 72 órán belül bejelentette, a sérülékenységet Ügyfél 2. közreműködésével megszüntette, a jogszerűtlen kezelt adatbázist pedig törölte. A Hatóság így az Ügyfél 1. konkrét adatvédelmi incidenskezelési gyakorlatában problémát nem tárt fel. A Hatóság e magatartást – mivel a jogszabályi kötelezettségek betartásán nem ment túl – kifejezetten enyhítő körülményként nem értékelte.*
- *A Hatóság figyelemmel volt arra is, hogy Ügyfél 1. mindenben együttműködött a Hatósággal az ügy kivizsgálása során, noha e magatartást sem – mivel a jogszabályi kötelezettségek betartásán szintén nem ment túl – értékelte kifejezetten enyhítő körülményként. (…)*
-

A bírság kiszabása során a Hatóság végül figyelembe vette Ügyfél 1. gazdasági súlyát. E körben figyelembe vette, hogy

- *2019. évi beszámolója szerint 5.344.545.000 HUF (ötmilliárdháromszáznegyvennégymillió-ötszáznegyvenötezer forint) nettó árbevétele volt.*
- *2020. évi felszámolás miatti tevékenységet záró éves beszámolója szerint a 2020. január 1. és 2020. június 15. közötti időszakban 551.404.000 HUF (ötszázötvenegymillió-négyszáznégyezer forint) nettó árbevétele volt.*
- *2020. június 16-tól kezdve felszámolás alatt áll. (…)*

(…) Ügyfél 2. vonatkozásában (… a) Hatóság súlyosbító körülményként vette figyelembe a következőket:

- *Az incidenssel érintett személyes adatok kezelése az adatok jellegéből fakadóan magasabb kockázattal jár, ezért az adatfeldolgozóknak fokozott elővigyázatossággal kell eljárniuk a kockázat mértékének megfelelő szintű adatbiztonság garantálása érdekében. Ügyfél 2. ennek ellenére nagyszámú személyes adat (összesen 781 érintett, összesen kb. 2506 darab személyes adata, köztük gyermekkorúak adatai és szerződéses összegekre vonatkozó adatok) kezelésére használt, általa Ügyfél 1. részére fejlesztett és üzemeltetett rendszer folyamatos bizalmas jellegének biztosítása érdekében nem hozott megfelelő intézkedéseket.*
- *(…) egy alapvetően magas kockázatú adatkezelés tekintetében Ügyfél 2. a jogosulatlan hozzáférések kiküszöbölésére és kimutatására alkalmatlan, a kockázatokkal aránytalan adatbiztonsági intézkedéseket alkalmazott, amikor*

a személyes adatokhoz rendkívül könnyen hozzá lehetett kívülről férni, anélkül, hogy ezt Ügyfél 2. észlelte volna. Az ilyen adatok kezelésére való biztonsági felkészültség profit alapú vállalkozásoktól fokozottan elvárható.

- *A Hatóság az adatvédelmi incidensről közérdekű bejelentés alapján szerzett tudomást, Ügyfél 2. által az adatvédelmi incidens észlelésére nem került sor.*
- *A Hatóság a megállapított adatbiztonsági hiányosságokat olyan rendszerszintű problémának tekinti, amely alapján a jogsértő helyzet már a bizonyítható jogosulatlan hozzáférések bekövetkezése előtt is hónapokkal fennállt az érintett tesztadatbázis tekintetében.*
- *Ügyfél 2. elmulasztotta elvégezni a weboldal és a rendszer fejlesztése során azon biztonsági teszteket, illetve más biztonsági intézkedéseket, amelyekkel a sérülékenység kiszűrhető vagy megszüntethető lett volna (pl. weboldal sérülékenység vizsgálata, a teszt- és éles adatbázis fennmaradó kapcsolatának megszüntetése). Ezek a mulasztások Ügyfél 2-nek magas szinten felróhatóak, mivel fő tevékenységként informatikai szolgáltatásokat nyújtó vállalkozásként működik.*

A Hatóság enyhítő körülményként vette figyelembe a következőket:

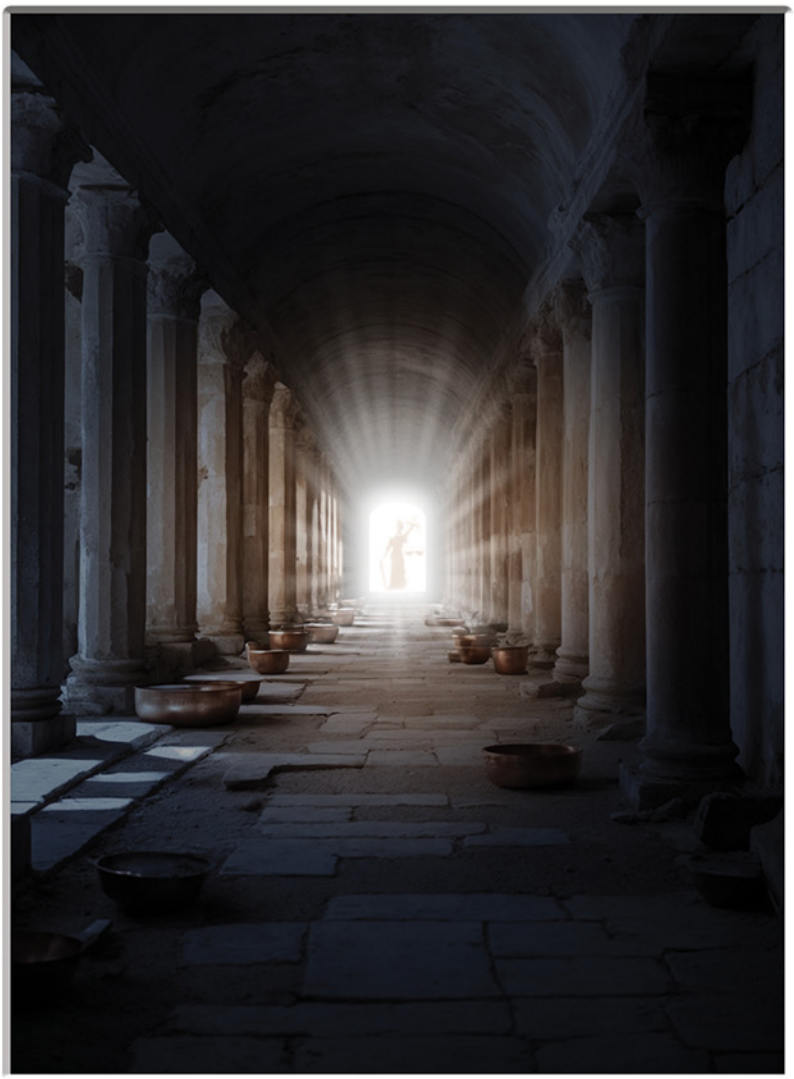
- *Az eljárás során a Hatóságnak nem jutott tudomására olyan információ, amely arra utalna, hogy az érintetteket a jogsértés nyomán kár érte volna.*
- *A Hatóság figyelembe vette, hogy az Ügyfél 2-vel szemben korábban nem állapított meg a személyes adatok kezelésével kapcsolatos jogsértést.*

Egyéb, figyelembe vett körülmények:

- *A Hatóság figyelemmel volt arra is, hogy Ügyfél 2. mindenben együttműködött a Hatósággal az ügy kivizsgálása során, noha e magatartást – mivel a jogszabályi kötelezettségek betartásán szintén nem ment túl – nem értékelte kifejezetten enyhítő körülményként. (…)*

A bírság kiszabása során a Hatóság végül figyelembe vette Ügyfél 2. gazdasági súlyát. E körben figyelembe vette, hogy

- *2019. évi beszámolója szerint 47.155.000 HUF (negyvenhétmillió-százötvenötezer forint) nettó árbevétele volt.*
- *2020. évi adónem áttérés miatti üzleti évet záró éves beszámolója szerint a 2020. január 1. és 2020. március 31. közötti időszakban 1.772.000 HUF (egymillió-hétszázhetvenkétezer forint) nettó árbevétele volt."*



Az Adatvédelemről alapfokon című könyv könnyen befogadható formában vezet be az adatvédelem és az Európai Unió általános adatvédelmi rendelet (GDPR) világába. Valós esetek segítségével tárja fel az adatvédelmi alapelveket és azok mindennapi alkalmazását, így kiválóan alkalmas az adatvédelem iránt érdeklődő laikusok számára, és az adatvédelemtől eltérő területekre szakosodott jogászok számára is nélkülözhetetlen olvasmány.

Amennyiben önt érdekli az adatvédelem, vagy munkája során fontos a GDPR ismerete, ez a könyv a legjobb választás.