Bevezetés az adatvédelemi jogba

Infokommunikációs- és technológiajog – nappali képzés

Dr. Liber Ádám, LLM, FIP, CIPP/E, CIPM, ügyvéd

KRE-ÁJK, Budapest, 2024. november 7; 21; 28.

Liber.Adam@provaris.hu

Agenda

1. Bevezetés
2. Alapfogalmak
3. Az adatkezelőkre vonatkozó kötelezettségek
4. Megfelelő szintű védelem és nemzetközi adattovábbítások
5. Az adatvédelem kölcsönhatása más jogterületekkel
6. Jogellenes adatkezelés következményei

1. Bevezetés

Az adatvédelemről általánosan

Adatvédelmi jogszabályok bármely azonosítható személyre (azaz érintettre) vonatkozó információ akár gépi, akár manuális kezelésére kiterjednek.

- E szabályok a magánszférát védik.
- Személyes adatok védelme / privacy - személyiségi jog (Ptk. 2:43. § e))
- Az adatok kezelésére az adatvédelmi alapelvek (jogszerűség, célhoz kötöttség, tisztességes adatkezelés elve, átláthatóság, pontosság) vonatkoznak. Személyes adatok csak ezen alapelvekkel összhangban kezelhetőek.
- Az adatvédelmi jogszabályok meghatározzák az érintettek jogait, jogorvoslati lehetőségeit.

Miért védjük a személyes adatokat?

Az adatvédelmi szempontból kifogásolható vállalatoktól az ügyfeleik is elfordulnak

- A válaszadók 94 %-a elkerüli azon vállalatokat, melyekről úgy gondolják, hogy nem védik a magánszférát (SlickText survey)
- Az ügyfelek 84%-a lojálisabb azon vállalatokkal, melyek erősebb biztonsági intézkedéseket alkalmaznak (Salesforce)
- Az ügyfelek 72%-a nem vásárolna árut vagy szolgáltatást adatvédelemi problémák által érintett cégtől a jövőben. (Salesforce)

Bizalom - az adatvédelem keretrendszere segíti meggyőzni az ügyfeleket, beszállítókat és munkavállalókat, hogy megosszák személyes adataikat egy üzleti vállalkozással

Egy üggyel kapcsolatosan is címlapra lehet kerülni

A privacy megsértésének „veszélyei” - bírságok

Meta – 1,2 milliárd EUR (nemzetközi adattovábbítás, 2023. május)

Amazon - 746 millió EUR (cookie hozzájárulás, 2021. június)

Instagram - 405 millió EUR (gyermekek adatainak kezelése)

TikTok - 345 millió euró (gyermekek adatainak kezelése)

LinkedIn - 310 millió euró (online hirdetések, jogszerűség, transzparencia. 2024. október)

Uber - 290 millió euró (nemzetközi adattovábbítás, 2024 augusztus)

Meta - 260 millió EUR (data scarping ügy).

WhatsApp - 225 millió EUR (adatkezelés transzparenciájával kapcsolatos hiányosságok).

Budapest Bank - 625 000 EUR (a call centerrel kapcsolatba lépő ügyfelek profilozása gépi tanulásos módszerrel)

A privacy megsértésének „veszélyei”

- **Pénzbírság**

  a GDPR alapján az adatvédelmi jogszabályok megsértése esetén kiszabható pénzbírság mértéke elérheti a vállalatcsoport teljes éves világpiaci forgalmának 4 %-át / 20 millió eurót

- **Jó hírnév sérelme**

  az adatvédelem fontos a közvélemény számára,

  a sajtó pedig szívesen lecsap adatszivárgási,

  adatlopási botrányokra

- **Részvények értékének elvesztése**
- **Költségek**

  a pénzbírság mellett pl. a jogi képviseletért fizetendő ügyvédi munkadíj, válságkezelés költsége, stb.

2. Alapfogalmak

Mi a személyes adat?

- Minden személyes adat védett.
- **Személyes adat** = élő személyre vonatkozó bármely információ (pl. név, elérhetőségi adatok, képmás, teljesítményértékelési információk vagy ezek kombinációja stb.).
- A személyes adatok azonosított vagy azonosítható természetes személyre vonatkoznak, és elegendő, ha a személy közvetlenül vagy közvetve azonosítható:
- Példák személyes adatokra:

Név és lakcím	Nem	Anyja leánykori neve
Mobil telefonszám	Iskolai végzettség	Családi állapot
E-mail cím	Személyazonosító igazolvány/útlevél száma	A gyermekvállalás ténye; a gyermekek száma és kora
Üzlet vezetőjének elérhetőségei	Hogyan jár valaki dolgozni (pl. busszal vagy autóval)	Személyről készült fényképek, hangfelvételek, videofelvételek
TAJ szám	Munkahely	A számítógép IP-címe
Adószám	Vállalati belépőkártya száma	Bűnügyi kivonat

Mi a személyes adat? – különleges adatok

- A személyes adatok különleges kategóriái („**különleges adatok**") további garanciákat élveznek, mivel gyakran szolgálnak a hátrányos megkülönböztetés alapjául.
- **Az érzékeny adatok közé tartoznak:**
  - **Faji vagy etnikai származás**
  - **Egészségi állapotra vonatkozó adatok** (pl. az Ön betegsége) ↔ DE: pl. a HR-osztálynak nyilván kell tartania a betegszabadságon töltött napok számát.
  - **Politikai vélemény, vallási vagy világnézeti meggyőződés.** Kerülje például, hogy azt mondja a kollégáinak, hogy "támogatom a Hóvirágpártot". Ehelyett csak annyit mondjon, hogy "szavaztam".
  - **Szakszervezeti tagság** ↔ DE: ezekre az adatokra szükség lehet a bérszámfejtéshez
  - **Biometrikus (egyedi azonosításra szolgáló) vagy genetikai adatok** ↔ DE: pl. egy fénykép, ujjlenyomat vagy retinaszkenner része lehet egy gyár biometrikus beléptető rendszerének.
  - **Szexuális életre vonatkozó adatok** (pl. nem irányultság, de élettárs, házastárs neve is elegendő lehet ehhez, EU Bíróság C-184/20)

„A személyes adatok” kezelése

A „adatkezelés" (manuális vagy automatikus) tágan értelmezett, és magában foglalja a következőket:

GYŰJTÉS

- Gyűjtés
- Rögzítés
- Hozzáférés
- Tárolás
- Megőrzés
- Lekérdezés
- Visszakeresés
- Nyomon követés

FELHASZNÁLÁS

- Felhasználás
- Módosítás
- Tagolás
- Megosztás
- Továbbítás
- Elemzés
- Következtetés levonása
- Mentés

TÖRLÉS

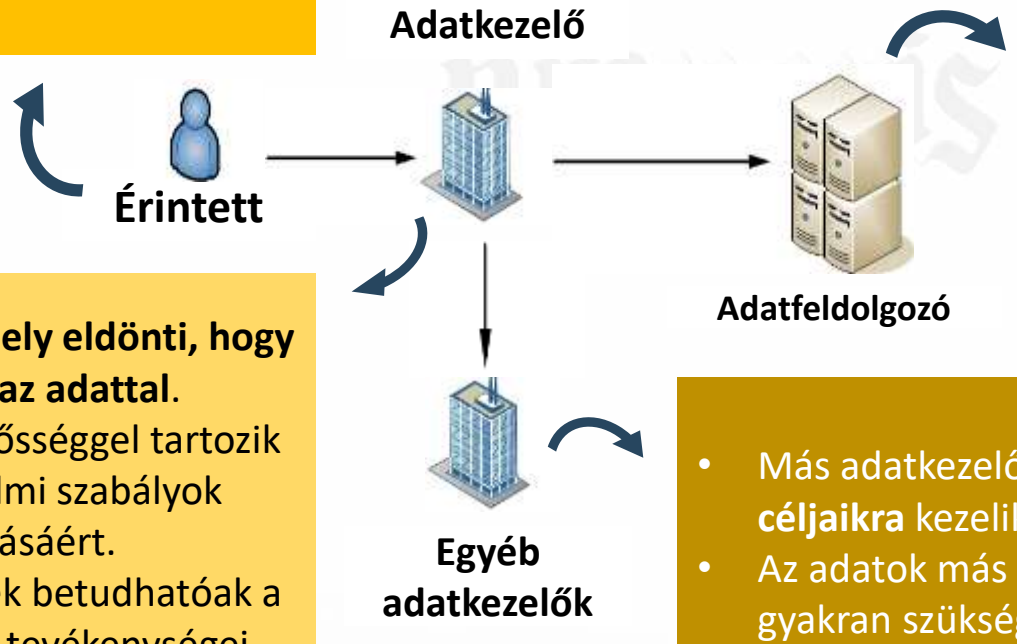
- Törlés
- Megsemmisítés
- Anonimizálás (a megsemmisítés alternatívája)
- Darálás

- „Háztartási adatkezelési kivétel": a GDPR nem vonatkozik a személyes adatok kezelésére, ha azt "*természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzik*".

Az adatvédelem területének szereplői

= a természetes személy, akire az információ vonatkozik.
(pl. egy természetes személy ügyfél, annak családtagja)

Az **adatkezelő és az adatfeldolgozó közötti különbségtétel** lényeges, ugyanis ez határozza a rájuk vonatkozó különböző követelményeket és külön feladatokat.



= a személy, aki/amely **az adatkezelő nevében kezel személyes adatokat.**
- kizárólag az adatkezelő utasításai alapján járhat el.

Pl. könyvelő, IT szolgáltató.

= **a személy, aki/amely eldönti, hogy mi történjen az adattal**.
- elsődleges felelősséggel tartozik az adatvédelmi szabályok betartásáért.
- az adatkezelőnek betudhatóak a munkavállalói tevékenységei

- Más adatkezelők az adatkezelőtől kapott adatokat **saját céljaikra** kezelik.
- Az adatok más adatkezelőknek történő továbbításához gyakran szükséges az érintettek hozzájárulása.

Az adatvédelem területének szereplői

Érintett: akinek az adatait kezelik, az adatvédelmi jogok alanya

Adatkezelő: lehet önálló vagy közös adatkezelő (vö. GDPR 26. cikk);

Adatfeldolgozó (vö. GDPR 28. cikk): az adatkezelő döntése alapján kezel adatokat, ilyen lehet a kiszervezés

Munkavállaló vagy egyéb **közreműködő** (vö. GDPR 29. cikk);

Harmadik fél (vö. GDPR 4. cikk 4.): aki nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt állnak

Egyéb fél: Nem végez adatkezelést, sem adatfeldolgozást, pl. „facilitátor”, posta, hírközlési szolgáltató

Európai uniós adatvédelmi rezsim

Releváns szabályok – GDPR és ePrivacy

- *EU általános adatvédelmi rendelete* (GDPR) – európai adatvédelmi reform eredménye, 2018. május 25-től közvetlenül alkalmazandó európai jogszabály és a személyes adatok kezelésének biztosít keretrendszert.
- *Elektronikus hírközlési adatvédelmi irányelv* (ePrivacy irányelv) - végfelhasználói eszközökön történő információ tárolása és ahhoz történő hozzáférés, és forgalmi adatok kezelése - a GDPR rendelkezéseit az online térben az ePrivacy irányelv rendelkezései *pontosítják és kiegészítik – ennek felülvizsgálata folyamatban van.*

Adatvédelmi követelmények

Az európai unió adatvédelmi joga megköveteli az *adatvédelmi alapelvek* betartását. Ennek kötelezettje az adatkezelő, aki meghatározza a személyes adatok kezelésének célját és eszközeit.

A digitális platformok jellemzően *adatkezelőnek*, az online ökoszisztéma más szereplőivel, felhasználóival együtt *közös adatkezelőnek* minősülnek, melyet tágan kell értelmezni. (lásd. Wirtschaftsakademie, Fashion ID és IAB Europe ügyek)

Adatvédelmi alapelvek

jogszerűség + tisztességes eljárás + átláthatóság	Engedély nélkül minden adatkezelés tilos, a jogalapot meg kell határozni. Az adatkezelés nem lehet indokolatlanul hátrányos, diszkriminatív, az érintett számára váratlan vagy félrevezető. Mindenki számára követhetővé és érthetővé kell tenni a személyes adatok kezelését. – Érthetőség, egyértelműség, relevancia, többrétegűség.
célhoz kötöttség	• Az adatkezelő meghatározott, egyértelmű és jogszerű célból gyűjthet adatokat, és azokat nem kezelheti a gyűjtésük céljával össze nem egyeztethető módon. Pl. nem megfelelő, ha az adat-elemzés olyan módszereket és felhasználási mintákat foglal magában, amelyeket sem az adatokat gyűjtő szervezet, sem az érintettek nem vettek figyelembe, vagy nem is számoltak fele az adatgyűjtés időpontjában. • Amennyiben további adatkezelésre kerül sor, vizsgálni kell, hogy ezen adatkezelés céljai összeegyeztethetők-e az eredeti célokkal. – tudományos kutatás esetén viszont vélelmezett a kompatibilitás
adattakarékosság	• Csak olyan személyes adatok kezelhetők, amelyek a cél szempontjából megfelelőek és relevánsak, valamint a szükségesre korlátozódnak és nem gyűjthető a szükségesnél több személyes adat. Különböző rendszerekből és forrásokból származó adatok integrációja problémás.
pontosság	A személyes adatoknak pontosnak és naprakésznek kell lenniük. Különösen releváns automatizált egyedi döntés esetén.
korlátozott tárolhatóság	A személyes adatok tárolása az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teheti lehetővé
integritás, bizalmasság rendelkezésre állás	A személyes adat biztonságát (CIA) mindenkor biztosítani kell.
elszámoltathatóság	Nem elég, hogy a vállalat megfelel az adatvédelmi jognak → ezt tudni kell igazolni is

Az adatkezelés jogszerűsége

Személyes adatok csak akkor kezelhetőek, ha az alábbi jogalapok egyike fennáll:

- a **hozzájárulás** legyen egyértelmű, önkéntes, tájékozott és konkrét:
    - *egyértelmű:* a döntés aktív kinyilvánítása, nem puszta hallgatás, nem előre bejelölt négyzet;
    - *önkéntes*: az érintettnek nem kell hátrányos következményektől tartania, ha hozzájárulását nem adja meg vagy visszavonja
    - *konkrét*: nem foghatja át „az összes személyes adatot” és „az összes lehetséges célt”
    - *tájékozott*: az érintett tudatában vannak, hogy mihez ad hozzájárulást

  Pl. elektronikus (pl. e-mail) direkt marketing.
- az érintett személlyel megkötött **szerződés teljesítéséhez** szükséges:
    - pl. szükséges az adós neve és lakcíme kezelése, hogy teljesíteni lehessen a részletfizetési megállapodás szerinti fizetési kötelezettséget, szükséges a munkavállalóval megkötött munkaszerződéshez
- az **adatkezelő jogszabályi kötelezettségei teljesítéséhez** szükséges:
    - pl. bírósági peres eljárás, bírósági végrehajtási eljárás adatkezelése, adózási, számviteli, pénzmosási tárgyú adatkezelések
- az adatkezelés az érintett vagy egy másik természetes személy **létfontosságú érdekeinek védelme** miatt szükséges; pl. kórházi sürgősségi ellátás
- közérdekű vagy az adatkezelőre ruházott **közhatalmi jogosítvány** gyakorlásának keretében végzett feladat végrehajtása:
    - pl. hatósági hatáskörök gyakorlása
- az adatkezelő vagy harmadik személy **elsőbbséget élvező jogos érdeke**:

Különleges adatokra vonatkozó korlátozás pl.: lásd GDPR 9. cikk (2) bekezdését

Ha a jogalap a hozzájárulás, annak kifejezettnek kell lennie
(„ráutaló magatartás” nem elégséges).

Érintetti jogok rendszere a GDPR-ban

- *Transzparencia / Tájékoztatás és jogok gyakorlása (GDPR 12-14. cikkek, 19. cikk)*
- *Az érintett hozzáférési joga (GDPR 15. cikk)*
- *A helyesbítéshez való jog (GDPR 16. cikk)*
- *A törléshez való jog („az elfeledtetéshez való jog”, GDPR 17. cikk)*
- *Az adatkezelés korlátozásához való jog (GDPR 18. cikk)*
- *Az adathordozhatósághoz való jog (GDPR 20. cikk)*
- *A tiltakozáshoz való jog (GDPR 21. cikk)*
- *Automatizált döntéshozatal alóli mentesség joga (GDPR 22. cikk)*

Az érintett jogai általánosan

Tájékoztatás és hozzáférés

Joga van megerősítést kapni, hogy a személyes adatát kezelik-e + az érintett számára érthető formában az **adatok másolatát megkapni**

Adatok helyesbítése és törlése

Az érintettről szóló adat:

- **helyesbítése**, ha az helytelen volt vagy elavult;
- **törlése** vagy **kezelésének korlátozása**, ha máskülönben nem felel meg az adatvédelmi jogszabályoknak

Adathordozhatóság

- a jog, hogy adatait újrahasznosítható elektronikus formátumban megkapja
- csak akkor igényelhető, ha hozzájáruláson vagy szerződésen alapul az adatkezelés.

Tiltakozáshoz való jog

- az érintett érdekei élveznek elsőbbséget az adott esetben (az adatkezelőnek nincs azt felülíró jogos érdeke), vagy
- az adatokat közvetlen üzletszerzési célból kezelik, vagy
- személyes adat alapján automatizált (emberi beavatkozás nélküli) döntést hoznak.

Jogok gyakorlásának szabályai:

- Főszabály szerint 1 hónapon belül választ kell adni
- Határidő hosszabbítás kivételesen, és 2 hónappal, késedelem okainak megjelölésével
- Ingyenesen

3. Adatkezelőkre vonatkozó kötelezettségek

Az EU adatvédelmi keretrendszere

Európai adatvédelmi reform eredménye, 2018. május 25-től közvetlenül alkalmazandó európai jogszabály.

Bírságmaximum összege 20 000 000 euró vagy az előző pénzügyi év globális árbevételének 4 %-a lehet, amelyik magasabb.

Elszámoltathatóság elve

az adatkezelő tartozik bizonyítani, hogy adatkezelése megfelel a jogszabálynak és ennek érdekében intézkedések megtételére köteles

Adatvédelmi Rendelet | Főbb kötelezettségek 1.

- Adatvédelmi alapelvek és az adatkezelés jogszerűsége – lásd adatvédelmi alapelveknél
- Adatvédelmi tisztviselő kinevezése – kötelező, ha érintettek rendszeres és szisztematikus, nagymértékű megfigyelését végzik vagy nagy számban kezelnek különleges adatokat
- Adatvédelmi incidensek bejelentése – 72 órán belül hatósági bejelentés és magas kockázat esetén az érintettek tájékoztatása kötelező
- Adatkezelési tevékenységek nyilvántartása – állandó és kockázatos adatkezelésekre külön is szükséges nyilvántartást készíteni
- Beépített és alapértelmezett adatvédelem

Adatvédelmi Rendelet | Főbb kötelezettségek 2.

- Egyablakos ügyintézés és együttműködés – határokon átnyúló adatkezelés esetén tagállamonként egy vezérhatóság, a fő letelepedési hely szerinti hatóság illetékes
- Érintetti jogok – adathordozhatóság, felejtéshez való jog, profilalkotási korlátozások
- Transzparencia – rövid, tömör, többrétegű, könnyen hozzáférhető tájékoztatás; írásban vagy más módon – elektronikus úton és díjmentesen
- Beszállítók kezelése – önálló vagy közös adatkezelők, adatfeldolgozók – megállapodást vagy szerződést kell kötni, jogszabályban meghatározott kötelező tartalmi elemekkel
- Adatvédelmi hatásvizsgálat – magas adatvédelmi kockázat esetén kötelező a kockázat csökkentése
- Elszámoltathatóság elve – a szuperalapelv és bizonyítási teher kapcsolódik hozzá

Adatvédelmi elszámoltathatóság a gyakorlatban

PRIVACY IRÁNYÍTÁS	• Adatvédelmi keretrendszer irányításáért személyében felelős kijelölése
SZABÁLYZATI KERETRENDSZER	• Belső adatvédelmi szabályzati keretrendszer kialakítása • Információbiztonsági szabályzatok • Adatkezelésekkel kapcsolatos tájékoztatók • Érintetti jogosultságokkal kapcsolatos keretrendszer • Adatmegőrzés szabályozása • Hatásvizsgálatok szabályozása • Beépített és alapértelmezett adatvédelem • Incidensek kezelése
ROPA / DOKUMENTÁCIÓ	• Vállalati szinten egységes adatkezelési tevékenységek nyilvántartása • Naprakészen tartáshoz szükséges intézkedések
ADATVÉDELMI TISZTVISELŐ (DPO)	• adatvédelmi hatásvizsgálatokkal kapcsolatban segít • felügyeli a megfelelést • a felügyeleti hatóság felé a kapcsolattartó • koordinálja az adatvédelmi incidensek bejelentését, kezelését • oktatási célokat határozhat meg • általános adatvédelmi tanácsadói funkcióval bír
TRÉNING	• Mindenkinek kötelező, rendszeres tréningek • Specializált tréningek egyes területekre

4. Megfelelő szintű védelem, nemzetközi adattovábbítások

Nemzetközi adattovábbítási követelmények

Szabályozás: EEJE. 8. cikk, EU Charta 8. cikk, GDPR V. fejezet – 44. cikk – 49. cikk

Szabályozási cél: Az európai adatvédelmi irányelv nemzetközi adattovábbítással kapcsolatos kulcsfogalma a „megfelelő szintű védelem”, és hogy az EU adatvédelmi rezsimet ne lehessen megkerülni

A külföldre irányuló adattovábbítás kockázatai:

Az érintett magánszférájába történő beavatkozás nem felel meg európai emberi jogi követelményeknek, így

- olyan indokból is hozzáférnek az adatokhoz, ami egy demokratikus társadalomban nem szükséges (így tömeges titkosszolgálati megfigyelésekkel)
- adatvédelmi alapelveket nem tarják be;
- érintetti jogokat nem biztosítják, nincs jogorvoslat.

Nemzetközi adattovábbítás fogalma

GDPR nem határozza meg az adattovábbítás fogalmát. Előzmény EU Bírósági ügy: Case C-101/01 - Bodil Lindqvist ügy

Az általános adatvédelmi rendelet 3. cikke és V. fejezete közötti kölcsönhatásról szóló 5/2021 EDPB iránymutatás szerint egy adatkezelés adattovábbításnak minősül, ha:

(1) az adatátadó (adatkezelő vagy adatfeldolgozó) az adott adatkezelés tekintetében a GDPR hatálya alá tartozik; ÉS
(2) az adatátadó közlés útján továbbítja vagy egyéb módon hozzáférhetővé teszi a személyes adatokat az adatátvevő (egy másik adatkezelő, közös adatkezelő vagy -feldolgozó) számára; ÉS
(3) az adatátvevő egy harmadik országban található vagy nemzetközi szervezet és attól függetlenül, hogy a GDPR hatálya alá tartozik-e.

Nem minősül adattovábbításnak: közvetlenül az uniós érintettektől saját kezdeményezésükre történő adatgyűjtés vagy ha nem másik adatkezelő vagy adatfeldolgozó részére történik közlés.

„Megfelelő szintű védelem” - Wp254rev.01

„Megfelelő szintű védelem” fogalma, ennek két alapeleme

(i) *anyagi jogi szabályok léte* (emberi jogok, és elvek célhoz kötöttség, adatminőség, szükségesség arányosság, transzparencia, érintetti jogok, etc), továbbá

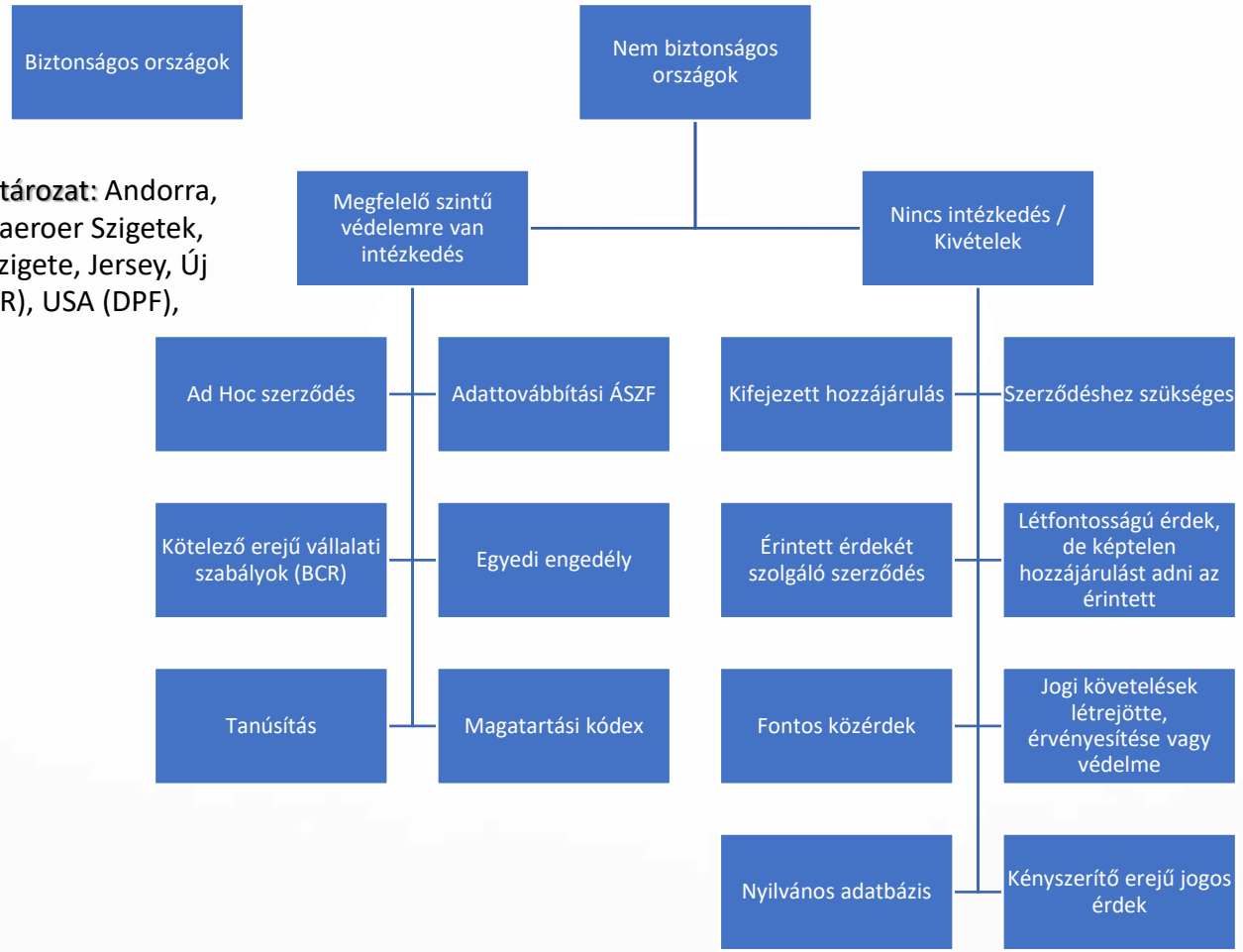
(ii) *hatékony érvényesítés, végrehajtás eszközei*, ideértve (a) adatkezelés független hatósági felügyelete; (b) a hatékony jogérvényesítés jó szintje; továbbá (c) elszámoltathatóság (d) jogsértés esetén hatékony jogorvoslat biztosítása.

Értékelése: EU Bizottság határozatával, az Európai Adatvédelmi Testület bevonásával (GDPR 45. cikk (2) bek határozza meg az elemeit).

EUB szerint: az „adatvédelem szintjének” az EU-n belül biztosított szinttel „lényegében azonosnak” kell lennie. a cél nem az uniós jogszabályok pontról pontra történő lemásolása, hanem a jogszabályok lényegi – alapvető követelményeinek kialakítása. Biztossági határozat célja, hogy a tagállamokra nézve kötelező hatállyal is megerősítse, hogy a védelmi szint lényegileg megegyezik (ekvivalencia)

Nemzetközi adattovábbítás szabályozása

EU bizottsági megfelelőségi határozat: Andorra, Argentína, Kanada (részben), Faeroer Szigetek, Guernsey, Izrael, Japán, Man Szigete, Jersey, Új Zéland, Svájc, Urugay, USA (PNR), USA (DPF), UK, Dél-Korea



Egyedi, „ad hoc” szerződések

GDPR 46. cikk (3) bekezdés – Ún. „Ad hoc” szerződéses feltételek

Előny	Hátrány
Rugalmasan alakítható	• Egyedi engedélyt igényel • Költséges és időigényes a bevezetése

Általános szerződési feltételek

Bizottság által jóváhagyott ÁSZF (GDPR 46. cikk (2)(c))

- Bizottság (EU) 2021/914. sz. végrehajtási határozata (2021. június 4.) a személyes adatok harmadik országokba történő továbbítására vonatkozó általános szerződési feltételekről - 4 modullal, amelyek a C2C, C2P, P2P és P2C adattovábbításokra vonatkoznak.
- Tagállami ÁSZF (GDPR 46. cikk (2)(d))

Előny	Hátrány
• Kész feltételek • Nincs engedély • Megköthető önállóan vagy más szerződés részeként • Tág körben elfogadott, elismert és használt	• Nem módosítható, illetve nem lehet eltérni tőle • Kérésre ki kell adni az érintett részére

Kötelező erejű vállalati szabályok (BCRs)

A BCR-ok a személyes adatok védelmére vonatkozó szabályzat, amelyet

- vállalatcsoport vagy közös gazdasági tevékenységet folytató vállalkozások csoportja alkalmazhatja;
- jogilag kötelező erejű, alkalmazandó és érvényesített;
- rendelkezniük kell az érintetteknek a személyes adataik kezelése tekintetében kikényszeríthető jogaikról.

WP 256 rev. 01: - Adatkezelői

WP 257 rev. 01: - Adatfeldolgozói

Előny	Hátrány
Rugalmasság Jogbiztonság Globális alkalmazás Magas védelmi szint	Csak csoporton belül alkalmazható Időt, koordinációt és komoly erőforrást igényel az elfogadása

Magatartási kódexek

- Kire vonatkozik: Adatkezelők vagy adatfeldolgozók kategóriáit képviselő szervezetek, egyesületek fogadhatják el
- Háttere az adattovábbítás megkönnyítésének eszközeként alkalmazható magatartási kódexekről szóló 04/2021. számú iránymutatás és a 1/2019-es iránymutatás

Előny	Hátrány
• Önszabályozás, iparágra szabható • Harmadik országbeli adatkezelők és adatfeldolgozók is alkalmazhatják, anélkül, hogy az exportőr a hatálya alatt állna	• Elfogadása hatósági / bizottsági jóváhagyáshoz kötött; csak megfelelő garanciákkal • Megfelelést ellenőrző szervezetet akkreditálni kell hozzá

Tanúsítás

- Tanúsítási szempontok szerint folytatott megfelelőség értékelés, amelyet egy harmadik személy / hatóság végez el és igazol, tárgya adatkezelési művelet vagy műveletek összessége lehet
- Eredménye a tanúsítvány, bélyegző vagy jelölés
- Háttere a 1/2018 tanúsítási kritériumokról és 1/2019 iránymutatás a magatartási kódexekről és ellenőrző szervezetekről

Előny	Hátrány
• Önszabályozás, átláthatóság • Jogbiztonság	• max 3 évre és megújítandó • tanúsító szervezet hatósági akkreditációjához, tanúsítási szempontok jóváhagyásához kötött

Schrems I. döntés és a hatása

2015. október 6. - Schrems döntés - C-362/14 EU Bíróság: a Safe Harbor döntés érvénytelen, az USA nem biztosít megfelelő szintű védelmet

Indoka:

- PRISM (Snowden) botrány - tömeges, szükségtelen és aránytalan titkosszolgálati megfigyelések; nincs ezzel szemben jogorvoslat az USÁ-ban; a „privacy” lényegét korlátozzák
- Safe Harbor általános és korlátlan eltérést enged az adatvédelmi elvektől nemzetbiztonsági, közérdekű és bűnüldözési okokból

Következménye: az EU adatvédelmi hatóságok az EU ÁSZF-ek, BCR-ok alkalmazását is megkérdőjelezik, a 29. cikk szerinti munkacsoport szerint a Safe Harbor nem alkalmazható, de végrehajtási moratóriumot adott 2016. január végéig

2016. július 12 - „EU-US Privacy Shield” – a Safe Harborhoz hasonlóan továbbra is önszabályozás alapján áll, DoJ és FTC felügyelte,

Schrems II. döntés és a hatása

2020. július 16-i EU Bírósági döntés (C-311/18): EU - US Privacy Shield érvénytelen

Az adattovábbítási ÁSZF-ek (modellszerződések) és kötelező erejű vállalati szabályok (BCR) nem érvénytelenek és továbbra is alkalmazhatók, de csak akkor, ha

(i) a címzett szerinti harmadik ország joga nem korlátozza az adattovábbítási garanciák (érintetti jogok) szerződéses vagy szabályzati érvényesülését; vagy ha mégis korlátozzák, úgy

(ii) kiegészítő jellegű jogi, műszaki és szervezési intézkedések, azaz további garanciák eseti bevezetésével ez a korlátozás ellensúlyozható és ezzel megteremthető a megfelelő szintű védelem.

Következménye: Adattovábbításra vonatkozó hatásvizsgálatot (transfer impact assessment) kell végezni a harmadik országba történő adattovábbítást megelőzően

Adattovábbítási hatásvizsgálat (TIA)

Nem hatásvizsgálat, de az ekvivalencia vizsgálatát el kell végezni és ahhoz mérten kell meghatározni a kiegészítő intézkedéseket

1. Lépés: adattovábbítások azonosítása, megismerése
2. Lépés: megfelelő adattovábbítási eszköz azonosítása
3. Lépés: adattovábbítási eszköz hatékonyságának ellenőrzése, helyi jogszabályok és gyakorlatok ellenőrzése fényében – betartják-e, vannak-e problematikus szektorok vagy gyakorlatok (USA: Cloud Act, FISA, Executive Order 12333)
4. Lépés: kiegészítő technikai, szerződéses és szervezeti intézkedések azonosítása és elfogadása a továbbított adatok védelmére (példákat a 01/2020. számú ajánlás 2. sz. melléklete tartalmaz, pl. titkosítás)
5. Lépés: minden szükséges eljárási lépés megtétele az intézkedések bevezetéséhez
6. Lépés: Megfelelés időszakosan visszatérő ellenőrzése / újraértékelés

EU - US Data Privacy Framework

2023. július 10-én az Európai Bizottság elfogadta az EU és az Egyesült Államok közötti adatvédelmi keretrendszer megfelelőségéről szóló határozatát (DPF) – szintén önszabályozáson alapul

„Egyesült Államok hírszerzési tevékenységeire vonatkozó garanciák megerősítéséről" szóló végrehajtási rendelet új, kötelező erejű garanciákat vezetett be az Európai Unió Bírósága által a 2020. júliusi Schrems II. határozatában felvetett pontok kezelése érdekében.

Lényege:

- *kötelező biztosítékok*, amelyek a nemzetbiztonság védelméhez szükséges és arányos mértékre korlátozzák az amerikai hírszerző hatóságok adatokhoz való hozzáférését;
- az amerikai hírszerző szolgálatok tevékenységeinek *fokozott felügyelete* a megfigyelési tevékenységekre vonatkozó korlátozások betartásának biztosítása érdekében; és
- *független és pártatlan jogorvoslati mechanizmus* létrehozása, amely magában foglalja egy új adatvédelmi felülvizsgálati bíróságot, amely kivizsgálja és megoldja az amerikai nemzetbiztonsági hatóságok adataihoz való hozzáféréssel kapcsolatos panaszokat.

2024. szeptember – *a DPF az első felülvizsgálat alapján átment*

5. Az adatvédelem kölcsönhatása más jogterületekkel

Adatvezérelt üzleti modellek és trendek

- Az adatvezérelt üzleti modellek megjelenése: az információs technológia fejlődésével szorosan összefügg, és kiemelkedő fontosságra tett szert az adatok felhasználása és az adatkormányzás.
- A digitális szolgáltatások piacát elsősorban az amerikai és távol-keleti technológiai óriások uralják, akik adatmonetizációs stratégiákat alkalmaznak.
- Ezzel szemben az Európai Unió gyakran kritikus a (személyes) adatok kezelése és az adatbázisok felhasználása kapcsán, ami hozzájárult ahhoz, hogy az innovatív, adat alapú gazdasági szektorokban nem az EU-ban székhellyel rendelkező vállalatok vezetnek.

Az EU válasza - EU digitális stratégiája

- Piacvédelmi intézkedések bevezetése adatvédelmi, fogyasztóvédelmi és versenyjogi háttérrel. Ezek a területek elválaszthatatlanul összekapcsolódnak és kiegészítik egymást, különösen az online platformok szabályozása esetében.
- Ex ante ellenőrzési és szabályozási mechanizmusok alkalmazása az EU új digitális stratégiájában, amely magában foglalja a Digital Governance Act (DGA), Data Act, Digital Services Act (DSA), Digital Markets Act (DMA), a mesterséges intelligenciáról szóló rendelet (AI Act).

Digitális platformok adatkezelései

- Nagy külföldi technológiai vállalatok pénzügyi erővel és piaci dominanciával
- Kiterjedt adatgyűjtés, ideértve a felhasználói tevékenységek követését, felhasználók tevékenységének és magatartásuk megfigyelését, célzott hirdetések alkalmazását és ezen adatok együttes, mélyreható elemzését gazdasági haszonszerzési célból, gyakran az adatvédelmi követelmények hátra sorolásával
- Online manipuláció - felhasználók, választók hírfolyamának vagy keresési eredményeinek befolyásolása, véleménybuborékok, fake news – lásd Cambridge Analytica ügyet
- USA FTC jelentés (2024. szeptember 19.) közösségi média és videó streaming szolgáltatások adatvédelmi gyakorlataitól:
  - Felhasználókról és a nem felhasználókról egyaránt tömegesen adatgyűjtés, átláthatóság hiánya és érintetti jogok biztosításának hiánya
  - Magas kockázatú invazív targetált hirdetések, sokszor érzékeny adatokra támaszkodva
  - Algoritmusok, az adatelemzés, vagy a mesterséges intelligencia (AI) széles körű alkalmazása, automatizált döntésekkel
  - Kiskorúak védelmének hiánya, jogaik sérelme
  - Verseny hiánya, piaci erőfölény, belépési korlátok és általánosan fogyasztóknak káros magatartások

Az önszabályozás nem működik és nem is opció ezen a területen, fogyasztókat megkárosító adatvédelmi gyakorlatok és versenyellenes hatások tapasztalhatók.

Fogyasztóvédelem és adatvédelem kapcsolata

- A „fogyasztói jólét” követelménye keretében relevánsak az adatvédelmi követelménye
- A fogyasztók érintettnek minősülnek, ezért tisztességtelen az online szolgáltatás lényeges jellemzőivel kapcsolatos megtévesztő adatvédelmi tárgyú információk nyújtása. Ilyen lehet:
  - „Adattal fizetés” – ingyenesség és a személyes adat szolgáltatása mint „ügyleti döntés”: VJ/85/2016. - Facebook ügy – 1,2 milliárdos bírság – Kúria nem értett azonban egyet ezzel
  - Személyes adatok biztonságával és adatkezeléssel kapcsolatos megtévesztő tájékoztatás - VJ/88/2016. – Google Allo ügy – kötelezettségvállalással zárult
  - Adatvédelmi jogokról adott megtévesztő tájékoztatás következményei
- Meta Platforms / Bundeskartellamt ügy: erőfölénnyel visszaélés - C-252/21 - versenyhatóság vizsgálhatja a GDPR megsértését;

Versenyjog és adatvédelem kapcsolata

Versenykorlátozó megállapodás, erőfölénnyel visszaélés és összefonódások

- Személyes adatok mint immateriális javak - piaci erő mérése a kezelt személyes adatok volumene, nem pedig az árbevételi adatok alapján
- Fogyasztói jólét koncepciójában az adatvédelmi aspektusok figyelembevétele
- Erőfölényben lévő vállalkozás megtagadja a nélkülözhetetlen személyes adatokhoz („essential facilities”) való hozzáférést
- Tisztességtelen szerződési feltételek az adatkezelési tájékoztatóban mint erőfölénnyel visszaélés; *Meta Platforms / Bundeskartellamt ügy*: erőfölénnyel visszaélés - C-252/21 versenyhatóság vizsgálhatja a GDPR megsértését
- Magánélet védelmét erősítő technológiák fejlesztése érdekében kötött horizontális megállapodások
- Adathordozhatóság mint versenyt serkentő tényező

GDPR és e-Privacy kapcsolata

A GDPR és az e-Privacy Irányelv (a 2002/58/EK irányelv a magánélet és az elektronikus hírközlés védelméről) az EU jogának két fontos eleme, amelyek a személyes adatok és a magánélet védelmét szabályozzák.

Az irányelv kifejezetten az elektronikus hírközléssel kapcsolatos adatvédelmi kérdésekre összpontosít. Pontosítja és kiegészíti a GDPR szabályait azáltal, hogy részletesebb szabályokat állapít meg a személyes adatok elektronikus hírközlési szektorban történő kezelésére vonatkozóan. Ez magában foglalja a sütikre és hasonló technológiákra, az elektronikus kommunikáció titkosságára és a kéretlen elektronikus üzletszerzésre vonatkozó szabályokat.

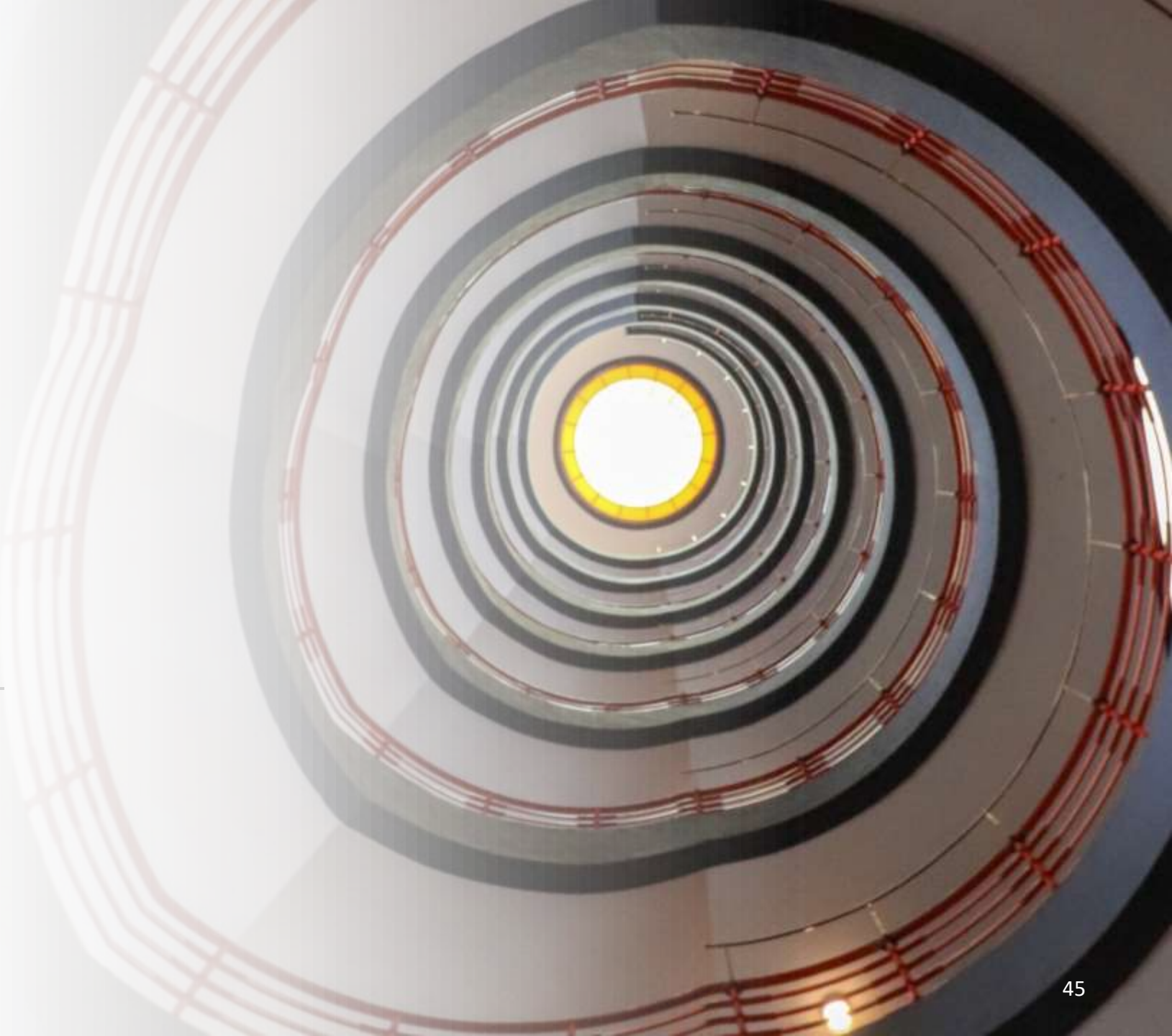
- **Hozzájárulási követelmények:** Mind a GDPR, mind az e-Privacy Irányelv megköveteli a hozzájárulást az adatkezeléshez, de az e-Privacy Irányelv részletesebb a sütikre és hasonló technológiákra vonatkozó hozzájárulási követelmények tekintetében.
- **Kommunikációk bizalmassága:** Az e-Privacy Irányelv konkrét szabályokat határoz meg az elektronikus kommunikáció bizalmasságára vonatkozóan, amelyeket a GDPR nem fed le kifejezetten. Például előírja, hogy az elektronikus hírközlési szolgáltatók biztosítsák a kommunikáció és a kapcsolódó forgalmi adatok titkosságát.
- **Marketing kommunikációk:** Az e-Privacy Irányelv kifejezetten foglalkozik az elektronikus úton történő közvetlen üzletszerzés szabályaival, ideértve a "soft opt-in" lehetőséget és a tiltakozási jogot.

Jelenleg folyamatban van az e-Privacy Irányelv, amelynek célja a GDPR szabályaival való szorosabb összehang, valamint az elektronikus hírközlési technológiák fejlődésére való válaszadás.

Jogérvényesítés és fórumok

- Európai Adatvédelmi Testület (EDPB)
- Adatvédelmi Főfelügyeleti Hatóságok / itthon Nemzeti Adatvédelmi és Információszabadság Hatóság – 20 millió euró vagy világpiaci forgalom négy százalékáig terjedő bírság (amelyik magasabb)
- Nemzeti Média és Hírközlési Hatóság – jogsértő elektronikus hirdetés esetén ötvenezer forinttól ötszázezer forintig terjedő összegű elektronikus kereskedelmi bírság
- Gazdasági Versenyhivatal – a határozat meghozatalát megelőző üzleti évben elért világszintű nettó árbevételének tizenhárom százaléka (184/2024. (VII. 8.) számú Korm. Rendelet szerint 15%)
- Fogyasztóvédelmi hatóság – Kormányhivatalok - január 1-jével Nemzeti Kereskedelmi és Fogyasztóvédelmi Hatóság
- Magyar Nemzeti Bank – NAIH és MNB negyedévente találkoznak
- Rendőrhatóságok / ügyészség – személyes adattal visszaélés
- Bíróságok – peres eljárás kezdeményezhető, sérelemdíj

6. A jogellenes adatkezelés következményei



Jogérvényesítés és érintetti jogorvoslati jogok

- Az érintett panasszal élhet a felügyeleti hatóságnál, a hatóság köteles a panasz elbírálására és annak eredményéről tájékoztatnia kell az érintettet
- Közigazgatási bírósági jogorvoslattal élhet a hatóság rá vonatkozó döntésével szemben, ideértve a hatóság által tett panaszt elutasító döntését
- Jogai megsértése miatt polgári bírósági eljárást indíthat az adatkezelővel és /vagy az adatfeldolgozóval szemben
- Vagyoni vagy nem vagyoni kártérítést igényelhet a GDPR rendelkezéseinek megsértéséből eredő kárának megtérítésére, illetőleg sérelemdíjat igényelhet
- Büntető feljelentést tehet a bűncselekmény gyanúja esetére

Jogellenes adatkezelés következményei

Közigazgatási eljárási / hatósági út – az érintett panasszal élhet a Nemzeti Adatvédelmi és Információszabadság Hatóság előtt – szankciók: bírság, helyesbítés, törlés, tiltás; határozat azonosító adatokkal való közzététele, melynek reputációs kockázata van

Bírósági út – személyhez fűződő jogok megsértése, adatbiztonsági követelmények megsértése - adatkezelő köteles bizonyítani az adatkezelés jogszerűségét, következmény: kártérítés és sérelemdíj

Büntetőjogi következmények – visszaélés személyes adattal - jelentős érdeksérelem vagy haszonszerzési cél esetén; levéltitok megsértése - következmény: szabadságvesztés és pénzbüntetés

GDPR szerinti szankciók

A magánélet megsértésének következményei lehetnek:

- Jó hírnév sérelme
- Közigazgatási bírságok
- Kártérítési / sérelemdíj igények az érintettek részéről

A felügyeleti hatóságok széleskörű vizsgálati és korrekciós hatáskörrel rendelkeznek, beleértve a figyelmeztetéseket, kötelezések alkalmazását, elitáltást és a közigazgatási bírságokat (GDPR 58. cikk).

Bírságok akár az éves globális árbevétel 2%-áig (legfeljebb 10 millió euróig) is terjedhetnek, és akár 4%-áig (legfeljebb 20 millió euróig) alapelvi jogsértés esetén.

A bírságokat a nemzeti felügyeleti hatóságok szabják ki az Európai Adatvédelmi Testület által kiadott iránymutatások alapján, figyelemmel a tagállami jogban erre meghatározott szabályokra.

A felelősség a vállalkozásokat terheli, beleértve a közös irányítás alá tartozó vállalkozáscsoportokat is.

Felelősség

- Az adatkezelő felelős minden olyan kárért, ami a GDPR megsértéséből származik.
- Az adatfeldolgozó felelős minden olyan kárért, ami a kötelezettségei megsértéséből vagy az adatkezelő jogszerű utasításának megsértéséből vagy azok figyelmen kívül hagyásából ered.
- Egy adatkezelésben a részt vevő adatkezelők és adatfeldolgozók egyetemlegesen felelnek a teljes kárért. A teljes kárért helytálló személyt visszkereseti jog illeti meg.
- Az adatkezelő, illetve az adatfeldolgozó mentesül a felelősség alól, ha bizonyítja, hogy a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség.

Polgári Törvénykönyv - 2:52. § [Sérelemdíj]

Akit személyiségi jogában megsértenek, sérelemdíjat követelhet az őt ért nem vagyoni sérelemért. A sérelem bekövetkezését a jogalkotó a jogsértés megvalósulásával vélelmezi, ezért azt bizonyítani nem kell.

A sérelemdíj mértékét a bíróság az eset körülményeire - különösen a jogsértés súlyára, ismétlődő jellegére, a felróhatóság mértékére, a jogsértésnek a sértettre és környezetére gyakorolt hatására - tekintettel, egy összegben határozza meg.

Bírói gyakorlat: Fővárosi Ítélőtábla Polgári Kollégiuma az 1/2013. (VI. 17.) kollégiumi véleménye – nem kell bizonyítani a hátrányt

Új Ptk. Tanácsadó Testület: a nem vagyoni sérelem bekövetkezése a sérelemdíj megítélésének feltétele. Jogsértés megállapítása mellett is elutasítható a sérelemdíj iránti igény.

Liber.Adam@provaris.hu

provaris
VARGA & PARTNERS

Central Palace V. emelet, H–1053 Budapest, Károlyi utca 9.
www.provaris.hu