GDPR Dióhéjban

Dr. Soós Andrea Klára


HITELES ADATVÉDELMI TANÁCSADÓ CÉG
DATAPROTECTION.EU

Mi a GDPR?

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE

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)

Hatálybalépés: **2016. április 27.**

Alkalmazás kezdete: **2018. május 25.**

Mit jelent az, hogy rendelet?

Mi lesz a magyar jogszabállyal?

Alkalmazandó jogszabályok

- Alaptörvény
- Munka törvénykönyve (módosítás várható)
- Polgári törvénykönyv
- Infó törvény (módosítással)
- Ágazati jogszabályok (Eker tv. Reklámtörvény, Hpt., Eüatv.)

Evolúció vagy revolúcó:

- Miben új és miben nem?
- Új lehetőségek
- Az implementáció tapasztalatai
- Az E-Privacy rendelet tervezete

Mennyire új a GDPR?

(1) A számítógéppel vagy más módon történő adatkezelés és adatfeldolgozás a személyhez fűződő jogokat nem sértheti.
(2) A nyilvántartott adatokról tájékoztatást - az érintett személyen kívül - csak az arra jogosult szervnek vagy személynek lehet adni.
(3) Ha a nyilvántartásban szereplő valamely tény vagy adat nem felel meg a valóságnak, az érintett személy a valótlan tény vagy adat **helyesbítését** külön jogszabályban meghatározott módon követelheti.

Miért érdekes?

- Ombudsman (-2011): csak kérhet
- NAIH: bírság 20 millió forintig
- GDPR: 20 milló EUR vagy a teljes éves világpiaci forgalom 4%-a
- Büntető tényállás

Az információs önrendelkezési jog doktrínája

- Duális jogalaprendszer
- „[…] az adatalany hozzájárulásának visszavonása megszünteti az adatkezelés jogalapját, tehát azt meg kell szüntetni. A jog ismeri a joggal való visszaélés, a rendeltetésszerű joggyakorlás vagy a jóhiszeműség fogalmát, ám ezen fogalmak használata kivételesen merülhet föl az alkotmányos jogok gyakorlásánál. […] Az adatkezelőnek nincs mérlegelési joga a kérés teljesítését illetően, hiszen az Avtv. alapján az érintett kérelmére törölni kell az adatokat.”ABI 2000, 104.

Alapfogalmak a rendelet szerint

- 1. **„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;
- 13. **„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;

Alapfogalmak a Rendelet szerint

- 14. **„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;

15. „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

Alapfogalmak a rendelet szerint

9. **„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;

10. **„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;

Alapfogalmak a rendelet szerint

- 18. **„vállalkozás”**: gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is;
- 19. **„vállalkozáscsoport”**: az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások;

Jogalapok

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 közérdekű vagy az adatkezelőre ruházott **közhatalmi jogosítvány** gyakorlásának keretében végzett feladat végrehajtásához szükséges;

f) 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.

KÜLÖNLEGES ADATOK!

Egy kiemelt jogalap

Érdekmérlegelési teszt:

1. adatkezelő jogszerű érdekének értékelése (I. Alapvető jogok II. Szélesebb közérdek III. Egyéb jogszerű érdek IV. Érdek kulturális/társadalmi elismertsége
2. Az érintettekre gyakorolt hatás értékelése (”hatásvizsgálat”) során kielemelt tényezők: I. adatok jellege (biometrikus adatok!), ideértve azok nyilvánosságát is, II. Az adatkezelés módja (széleskörű? Hatásai kiszámíthatók?), III. Az érintett ésszerű elvárásai, IV. Az adatkezelő és az érintett státusza (érintett: gyermek! beteg!)
3. ideiglenes mérlegelés (előzetes következtetéssel)
4. kiegészítő biztosítékok (pl.: mennyiségi korlátozás, azonnali törlés, funkcionális szétválasztás (GDPR: „álnevesítés), PETek, beépített adatvédelem, megnövelt átláthatóság, feltétel nélküli letiltási jog biztosítása, adathordozhatóság biztosítása)

Jogos érdek

Mi a jogos érdek?

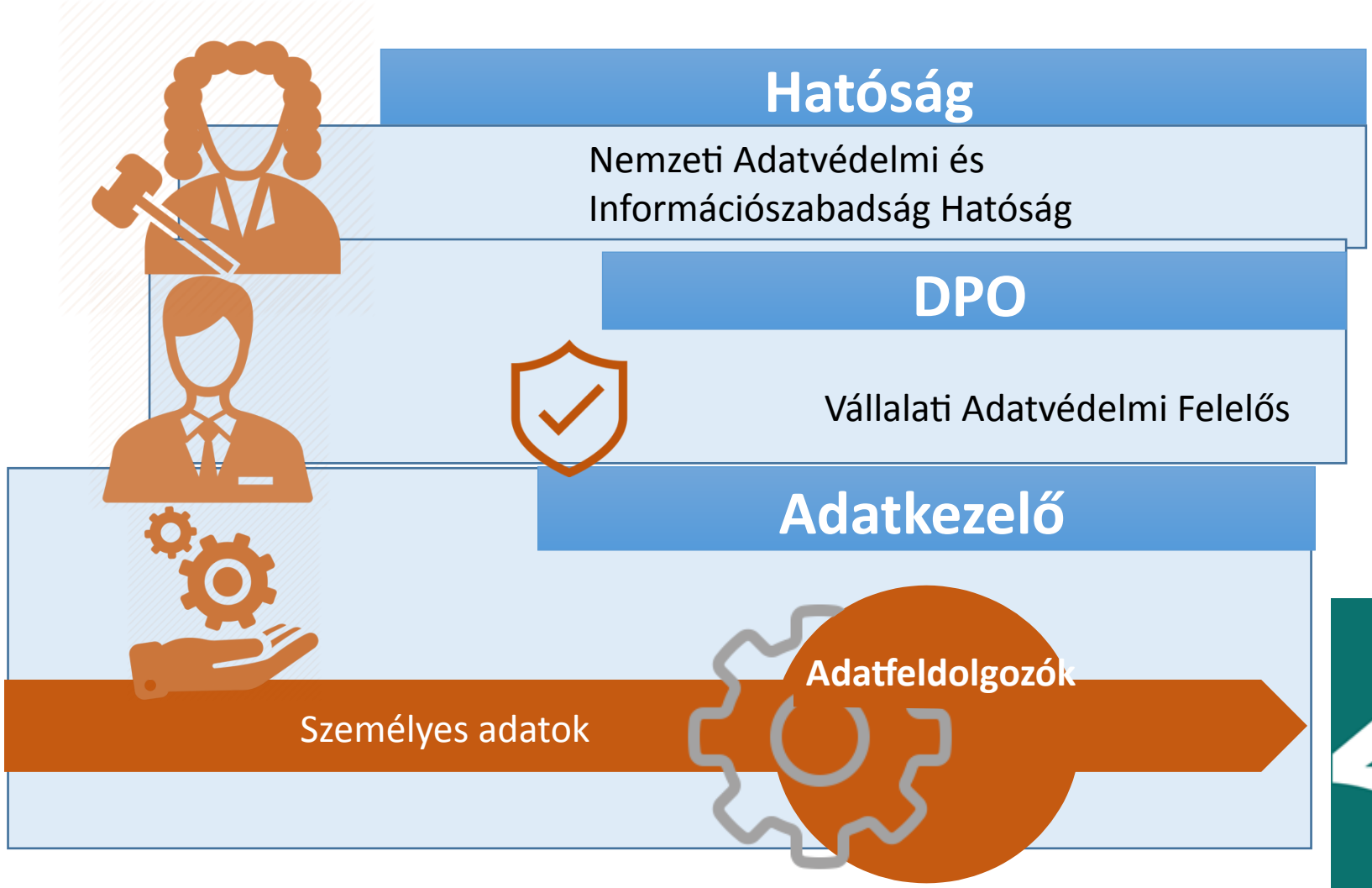
(a GDPR 47. preambulumpont példákat ad)

- Közhatalmi szervek feladataik során végzett adatkezelésére nem alkalmazható
- Releváns és megfelelő kapcsolat az érintett és az adatkezelő között (érintett ügyfél vagy alkalmazott)
- Érintett számíthat-e ésszerűen az adott célú adatkezelésre?
- Csalás megelőzése céljából történő feltétlenül szükséges adatkezelés
- Személyes adatok közvetlen üzletszerzési célú kezelése *(! vs 1995. évi CXIX tv.)*
- Elvi szinten az […] jogos érdeke lehet az engedményezéssel megvásárolt követelések érvényesítése, behajtása, azonban [….] (NAIH, 2015)

Jogszerű adatkezelés a GDPR szerint

1. Az adatkezelés tisztességes célja
2. Az adatkezelés megfelelő jogalapja
3. Az adatkezelői kötelezettségek megtartása a teljes élettartam alatt
4. Az érintetti jogok biztosítása a védelmi idő alatt
5. Adatbiztonság

Szereplők az adatkezelési folyamatban



Személyes adatok

Egy kiemelt alapelv

A célhoz kötöttség elve

Meghatározza, hogy meddig őrizhető egy adat:

A munkaviszony megszűnésétől számított három év

De: jelenléti ívek, egyedi kérelmek, hivatalos levelezések

Egy kiemelt érintetti jog

A törlés joga

- Jogalaptól függ
- Nem törölhető a jogi kötelezettség teljesítése, szerződés és érdekmérlegelés miatt kezelt adat

- Kötelező törölni akkor, ha a jogalap már megszűnt-

Adatfeldolgozók

- Adatfeldolgozó: aki az adatfeldolgozó evében adatot kezel
- A magyarországi adatfedolgozáshoz nem kell hozzájárulás
- De: szerződés kell
- A szerződésnek kötelező feltételei vannak
- Tipikus adatfeldolgozók:
- Bérszámfejtő, könyvelő, host szolgáltatás

Egyéb kötelezettségek a GDPR alapján

- Adatvagyonleltár elkészítése
- “data protection by design” és pszeudonimizáció
- Adatvédelmi tisztviselő /DPO/ (magyar állásfoglalás is van már)
- Adatvédelmi hatásvizsgálat /PIA/
- Adatbiztonsági követelmények
- Adatibiztonsági incidensek kezelése
- Iparági magatartási kódexek

Adatvédelmi akcióterv felállítása

- - “tudatosság erősítése”
- - Felül kell 2018-ig vizsgálni a rendelkezéseket és kiszűrni a jogellenes gyakorlatot
- - “mini audit elvégzése”
- - az adatkezelési folyamatok feltérképezése

- 1. lépés: az adatkezelés céljainak meghatározása
- 2. lépés: a választott célhoz tartozó jogalapok áttekintése
- 3. lépés: az adattárolás (kezelés időtartama)
- 4. lépés: adatfeldolgozók azonosítása

A jogszerű adatkezelés

- 1. az adatkezelés célja jogszerű és megfelel az alapelveknek
- 2. az adatkezelés jogalapja mindvégig ugyanaz
- 3. az érintetti jogok megfelelően biztosítottak
- 4. a biztonsági elvárások megfelelően teljesítettek

Magatartási kódexek

- **Magatartási kódexek**
- A tagállamok, a felügyeleti hatóságok, a Testület és a Bizottság ösztönzik olyan magatartási kódexek kidolgozását, amelyek – a különböző adatkezelő ágazatok egyedi jellemzőinek, valamint a mikro-, kis- és középvállalkozások sajátos igényeinek figyelembevételével – segítik e rendelet helyes alkalmazását.
- A csatlakozás a jóhiszeműséget segíti

Adatvédelmi hatásvizsgálat (PIA)

Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

Adatvédelmi incidens

Fogalma: **data breach:** 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

72 óra: hatóság

Érintettek: nem mindig

Implementáció 1: Adattérkép

- Személyes adatok körének felmérése
- Új Infotv - újdonságok! (elhunyt személyek)

Implementáció 2: Adattisztítás

- Mi kell üzletileg?
  - Régen lezárt szerződések?
  - Árazás?
  - Különleges adatok?
- Ha tényleg kell: jogi megalapozás (jogalapok, cél, tárolási idő)
- Adatgazda kijelölése

Implementáció 3: Dokumentáció

- Szerződések
- Tájékoztatók, nyilatkozatok
- Szabályzatok (adatvédelmi szabályzat, indicensjelentés, panaszkezelés)
- Érdekmérlegelési teszt, PIA
- Adatkezelések (belső) nyilvántartása

  - ---››› elszámoltathatóság (és fenntarthatóság)

A GDPR közérthetően

1. Először mindig gondolj az érintettekre
2. Legyél tudatában, hogy **milyen személyes adatokat k**ezelsz (leltár)
3. Pontosan tudd, hogy **hol vannak** ezek az adatok, és **hogyan áraml**anak a szervezeten belül
4. Az adat **életciklusának minden periódusában** foglalkozz a személyes adatok védelmével
5. **Rendszeresen vizsgáld és elemezd** a személyes adataiddal kapcsolatban felmerül **kockázataidat**
6. Bizonyosodj meg róla, hogy **megfelelő kontrollokat alkalmazol**
7. Alakítsd ki az a **biztonsági incidens felderítés lépéseit.**
8. Gondoskodj arról, hogy **megbízhatónak** lássanak

Felmerült kérdések

andrea.soos@dataprotection.eu

www.facebook.com/dataprotectioneu

I