GDPR adatvédelmi szabályozás

General Data Protection Regulation


GDPR IS COMING...
imgflip.com

I. BEVEZETŐ

- **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)**
- Hatályba lépése: 2016. április 26.
- Moratórium: 2018. május 25.
- A türelmi idő végéig valamennyi adatkezelőnek és adatfeldolgozónak meg kell felelnie a GDPR-nak

- Területi hatály:
- Az EU-ban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggő adatkezelésre
- Az EU-ban tartózkodó érintettek személyes adatainak kezelésére akkor is, ha az adatkezelő az EU-n kívül van, de EU-ban nyújtott szolgáltatáshoz, vagy az érintettek megfigyeléséhez kapcsolódik

II. ADATVÉDELMI GYORSTALPALÓ

- **Ki az érintett, mi a személyes adat?**
- **Ki az adatkezelő, ki az adatfeldolgozó?**
- **Ki a hatóság?**
- **Milyen fő teendők következnek a GDPR bevezetéséből?**

Ki az érintett? Mi a személyes adat?

- *személyes adat:* azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ;

- *különleges személyes adatok:* faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

Ki az adatkezelő? Ki az adatfeldolgozó?

- *adatkezelés:* a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége;
-
- *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;
-
- *adatfeldolgozó:* az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel

Ki a hatóság?

- **NAIH**: Nemzeti Adatvédelmi és Információszabadság Hatóság
- 2012. január 1. óta működik,
- adatvédelmi hiányosságok esetén először figyelmeztetett, és csak a figyelmeztetés ellenére elmaradó jogkövetés esetén alkalmazott bírságot
- a bírság felső határa jelenleg 20.000.000- HUF
- **2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról**

Adatvédelmi hatóságok jelentősége a GDPR hatálya alatt

- A GDPR az adatvédelmi hatóságokat a versenyhatóságokkal (itthon a GVH) egy szintre emeli
- az adatvédelmet sokkal fajsúlyosabb jogterületté kívánja tenni,
- bírságolás előírt mértéke:
  - kisebb (bagatell) jogsértések: 10M EUR-ig, vagy előző évi forgalom 2%-áig;
  - nagyobb (hardcore) jogsértések: 20M EUR-ig, vagy előző évi forgalom 4%-áig.
  - A két bírságplafon közül mindig a magasabbat kell alkalmazni.

Milyen fő teendők következnek a GDPR bevezetéséből?

1. Személyes adatok körének felmérése
2. Adattisztítás
3. Hatásvizsgálat (opcionális)
4. Dokumentáció

1. Személyes adatok felmérése - példák

Belső	Külső
• Munkavállalók személyes adatai • Jelentkezők, önéletrajzok • Vagyonvédelmi biztonságtechnikai rendszer • Beléptető rendszer • Belső IT-rendszer által gyűjtött egyéb személyes adat • Egyéb? … bármi, ami itt nem szerepel	• Ügyfelek, beszállítók, partnerek személyes adatai • Elektronikus hírlevél, reklámlevél, DM-levél (spam) • Automatizált adatkezelés, profilalkotás, cookie-k • Alkalmai jellegű adatkezelések, nyereményjátékok, promóciók • Egyéb? … bármi, ami itt nem szerepel

2. Adattisztítás

- kell-e az összes jelenleg kezelt személyes adat?
- fennáll-e még az adatkezelés célja? megfelelő-e a jogalap?
- ha nem kell: törlés
- ha kell: jogalap, cél, tárolási idő, adatgazda kijelölése, és a GDPR-nak megfelelő új, vagy átdolgozott dokumentáció elkészítése

3. Hatásvizsgálat (impact assesment)

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; különösen indokolt az alábbi esetekben:

- automatizált adatkezelés, profilalkotás
- személyes adatok különleges kategóriáinak, bűnügyi személyes adatoknak a kezelése
- nyilvános helyek nagymértékű, módszeres megfigyelése

4. Dokumentáció (tájékoztatók, szabályzatok)

- ✓Hozzájárulási nyilatkozatok (hozzájáruláson alapuló adatkezelésnél)
- ✓Tájékoztatók (érintetti körök vagy adatkategóriák mentén, érintettnek címzett, áttekinthető)
- ✓Szabályzat (bonyolultabb adatkezelést végző, nagyobb szervezetek belső szabályzata)
- ✓Egyéb: táblák, piktogrammok

Tartalmi elvárások: adatkezelő, adatfeldolgozó személye, kezelt adatok köre, adatkezelés jogalapja, adatkezelés célja, időtartama, érintett jogai, adattovábbítás, jogorvoslati jog

III. Az adatvédelem gyakorlati kérdései

- Milyen jogalapok szerint lehet személyes adatot kezelni?
- Mi lehet az adatkezelés célja?
- Mik az érintettek jogai?
- Van-e a GDPR-nak az adatbiztonsággal kapcsolatos elvárása?
- Mi az adatvédelmi incidens?
- Mikor kell adatvédelmi (DPO) tisztviselőt foglalkoztatni?

Milyen jogalapok szerint lehet személyes adatot kezelni? I.

- GDPR 6. Cikk. A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:
- a) az érintett hozzájárulását 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 érdekeinek 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.

Milyen jogalapok szerint lehet személyes adatot kezelni? II.

- **hozzájárulás:** önkéntes, konkrét, egyértelmű, megfelelő tájékoztatáson alapuló akaratnyilvánítás, pl: hírlevél, nyereményjáték
- **szerződés teljesítése:** természetes személlyel kötött szerződés teljesítéséhez szükséges adatok
- **jogi kötelezettség teljesítése:** pl. munkavállalók mindazon adatainak kezelése, melyek bérszámfejtéshez, adatszolgáltatáshoz szükségesek
- **létfontosságú érdek:** ha cselekvőképtelensége folytán vagy más elháríthatatlan okból nem tud hozzájárulni, pl. egészségügyi adatok, kár, veszély elhárítása
- **közhatalmi jogosítvány gyakorlása:** hatóságok, állami szervek, közintézmények, törvényi felhatalmazás alapján
- **adatkezelő vagy harmadik fél jogos érdeke:** pl. vagyonbiztonsági rendszerek, beléptetők

Mi lehet az adatkezelés célja?

- GDPR: célhoz kötöttség: meghatározott, egyértelmű és jogszerű célból
- Infotv:
  - Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie.
  - Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas.
  - A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

Mik az érintettek jogai?

- tájékoztatáshoz való jog (írásban, elektronikus úton, tájékoztatók)
- hozzáférési jog (érintett kérelme alapján)
- helyesbítéshez való jog
- törléshez való jog (cél, jogalap megszűnt, vagy hozzájárulását visszavonta)
- adatkezelés korlátozásához való jog
- adathordozhatósághoz való jog
- tiltakozáshoz való jog
- automatizált döntéshozatal hatálytalanságához való jog

Van-e a GDPR-nak az adatbiztonsággal kapcsolatos elvárása?

- Igen, van – 32-34. Cikk. A GDPR az adatbiztonságot / információbiztonságot a személyes adatok vonatkozásában vezeti be,
- Mindenkinek, aki személyes adatot kezel, meg kell felelnie bizonyos sztenderdeknek (pl. ISO/IEC 27001:2013 szabvány az információbiztonságról) – de nincs definiálva.
- Alapelvárások: confidentiality, integrity, availability / bizalmasság, sértetlenség, hozzáférhetőség. Minden esetben IT-szakember, esetleg ISO-szakember közreműködésével megvalósítandó.
- Általában külön IT-biztonsági szabályzatban

Mi az adatvédelmi incidens?

- A biztonság olyan sérülése, amely a személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
- 72 órán belül be kell jelenteni a felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.
- Az adatvédelmi incidensekről nyilvántartást kell vezetni, és az érintetteket tájékoztatni kell róla.
- Az adatkezelőknek készíteniük kell egy adatvédelmi incidens bejelentési tervet, amely lehetővé teszi számukra, hogy incidens esetén azonnal cselekedni tudjanak.

Mikor kell adatvédelmi (DPO) tisztviselőt foglalkoztatni?

- Az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt jelöl ki minden olyan esetben, amikor:

a) az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve a bíróságokat;

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 különleges személyes adatok, illetve bűnügyi személyes adatok nagy számban történő kezelését foglalják magukban.

- - Adatvédelmi jogi és gyakorlati tapasztalatokkal rendelkező szakember, alkalmazott, illetve külsős szolgáltató is lehet.

Milyen feltételekkel továbbíthatók személyes adatok külföldre?

- Személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására akkor kerülhet sor, ha a Bizottság megállapította, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít. Az ilyen adattovábbításhoz nem szükséges külön engedély.
- A fenti határozat hiányában az adatkezelő vagy adatfeldolgozó csak abban az esetben továbbíthat személyes adatokat harmadik országba vagy nemzetközi szervezet részére, ha az adatkezelő vagy adatfeldolgozó megfelelő garanciákat nyújtott, és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.
- Az adattovábbításról az érintetteket tájékoztatni kell.

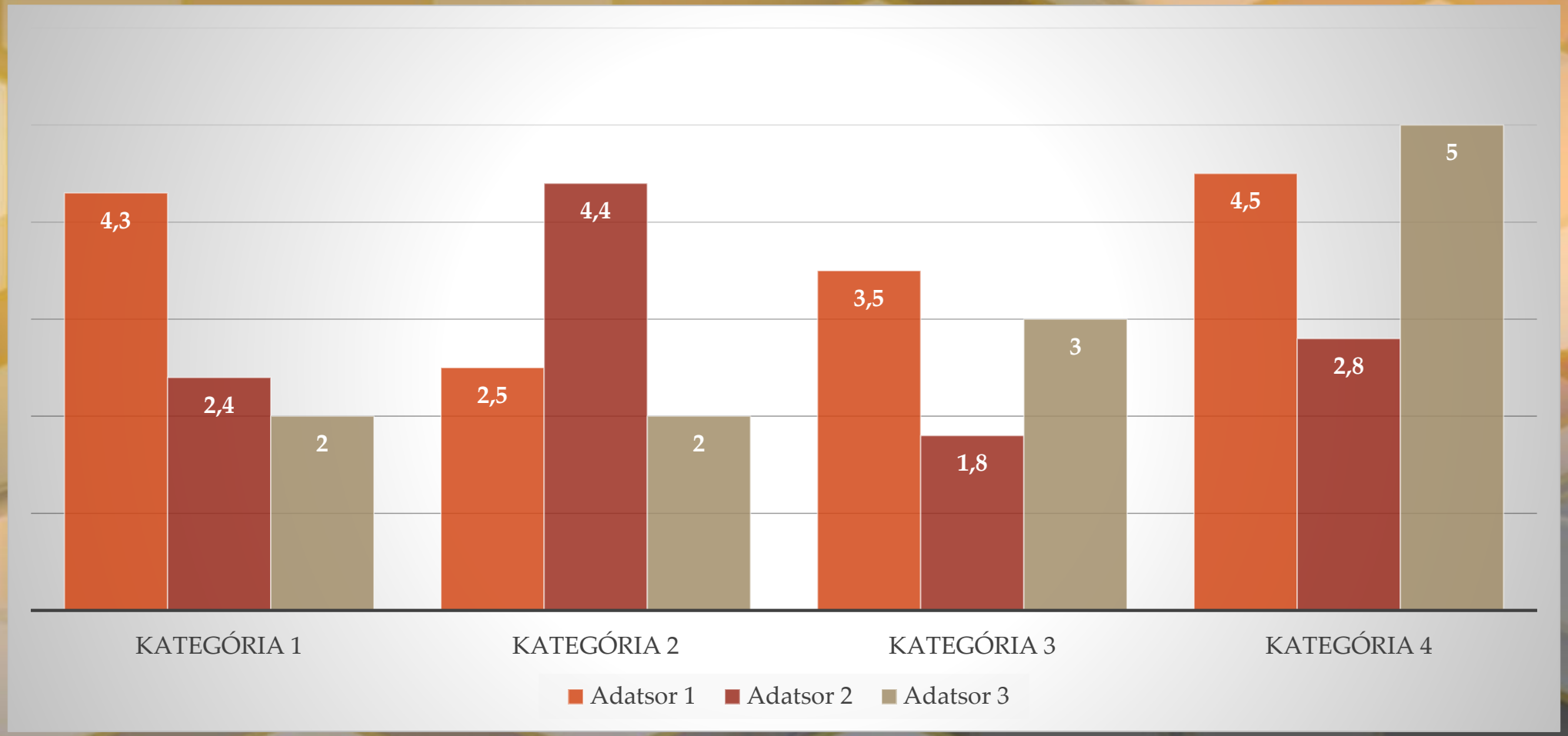
Kérdések???

Köszönöm a figyelmet!

Cím és tartalom listával

- Első szint
  - Második szint
    - Harmadik szint
      - Negyedik szint
        - Ötödik szint

Cím és tartalom diagrammal



Két tartalomrész elrendezés táblázattal

Osztály	A csoport	B csoport
1. osztály	82	85
2. osztály	76	88
3. osztály	84	90

- Első pont szövege
- Második pont szövege
- Harmadik pont szövege

Két tartalomrész elrendezés SmartArt-ábrával

- Első pont szövege
- Második pont szövege
- Harmadik pont szövege