Általános tájékoztatás a 2018. május 25. napjától alkalmazandó GDPR rendeletről

Európai Parlament és a Tanács 2016/679 rendelete - általános adatvédelmi rendelet

A GDPR az Európai Parlament és a Tanács 2016/679 rendelete (általános adatvédelmi rendelet) a személyes adatok áramlásáról, védelmének erősítéséről szól.

2018. május 25-től kötelezően alkalmazandó a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett adatkezelésére. A rendelet hatálya a „háztartási" adatkezelésen kívül **minden adatkezelésre vonatkozik.**

I. Fogalom meghatározás:

„Érintett":

minden olyan természetes személy, akinek személyes adatait valaki tárolja és kezeli.

Személyes adat :

Az azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ, amivel elérhető vagy azonosítható az érintett. (Személyes adat például: név, lakcím, anyja neve, születési hely, idő, okmányazonosítók, telefonszám, e-mail cím, felhasználónév, bankszámla adatok .)

Adatkezelő :

Természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy **bármely egyéb szerv, amely a személyes adatokat kezeli.** Adatkezelő minden olyan személy vagy 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 személy vagy szerv, amely **az adatkezelő nevében személyes adatokat kezel.**

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.

Felügyeleti hatóság :

Egy tagállam által az Európai Parlament és a Tanács 2016/679 rendeletének 51. cikkének megfelelően létrehozott független közhatalmi szerv.

II. Alapelvek:

1. Jogszerűség, tisztességes eljárás és átláthatóság

A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.

2. Célhoz kötöttség

A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon.

3. Adattakarékosság

A személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükséges mértékre kell korlátozódniuk.

4. Pontosság

A személyes adatok kezelésének pontosnak és szükség esetén naprakésznek kell lenniük. Az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul törlendők vagy helyesbítendők.

5. Korlátozott tárolhatóság

A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.

6. Integritás és bizalmas jelleg

Biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

7. Elszámoltathatóság

Az adatkezelőnek kell bizonyítani tudni, hogy az adatkezelése megfelel a GDPR rendelet 5. cikk 1. bekezdésében foglalt elveknek.

III. Jogalap:

1. Hozzájáruláson alapuló
2. Szerződésen alapuló
3. Jogi kötelezettségen alapuló
4. Az érintett érdekeinek védelme
5. Közérdekű feladat végrehajtása
6. Jogos érdek

IV. Érintettek jogai:

1. Tájékoztatás joga
2. Hozzáférés joga
3. Helyesbítés joga
4. Törlés-elfeledtetéshez való joga
5. Adatkezelés korlátozásának joga
6. Adathordozhatóság joga
7. Tiltakozás joga
8. Automatikus döntéshozatali eljárások egyedi ügyekben

Mi tartozik a személyes adatok különleges kategóriájába?

A faji, vagy etnikai származásra, a politikai véleményre, vallási vagy világnézeti meggyőződésre, szakszervezeti tagságra vonatkozó, a genetikai- és biometrikus adatokra, egészségügyi állapotra, szexuális életre, vagy szexuális irányultságra vonatkozó adatok. A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok kezelésére vonatkozó szabályokat a rendelet a személyes adatok különleges kategóriáján kívül, külön szabályozza. Ezek kezelésére abban az esetben kerülhet sor, ha az közhatalmi szerv adatkezelésében történik, vagy ha az adatkezelést az érintett jogai és szabadságai tekintetében megfelelő garanciákat nyújtó uniós vagy tagállami jog lehetővé teszi.

Mit jelent az adatkezelés?

A személyes adatokon vagy adatállományokon, az alkalmazott technológiától függetlenül végzett bármely művelet, így például a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

Mikor jogszerű az adatkezelés?

Ha meghatározott céllal, jogalappal és tárolási idővel rendelkezik az adott adatkezelési folyamat. A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:

- az érintett **hozzájárulását adta** személyes adatainak egy vagy több konkrét célból történő kezeléséhez;

- 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;

- az adatkezelés az adatkezelőre vonatkozó **jogi kötelezettség teljesítéséhez** szükséges;

- az adatkezelés az érintett vagy egy másik természetes személy **létfontosságú érdekeinek védelme** miatt szükséges;

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

- 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.

Mit jelent az adatvédelmi incidens?

Adatvédelmi incidens a biztonság olyan sérülése, amely a kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. (például személyes adatok megküldése téves e-mail címre vagy a nyilvántartások szervezett külső támadása)

Az incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az a tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. 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. Az

adatvédelmi incidens személyek jogaira gyakorolt hatását, hogy jár-e kockázattal vagy a besorolása magas kockázatú, mindig az adatkezelőnek kell mérlegelnie. Felügyeleti hatóság Minden tagállam köteles kijelölni vagy létrehozni egy vagy több független közhatalmi szervet, amelyek felügyeleti hatóságként eljárva biztosítják a GDPR alkalmazásának ellenőrzését. Magyarországon a felügyeleti hatóság jogszabály általi kijelölése még nem valósult meg, de az Alaptörvénnyel és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) rendelkezéseivel összhangban **a NAIH megfelel az általános felügyeleti hatósággal szemben támasztott kritériumoknak.**

Mi a felügyeleti hatóság fő feladata?

A felügyeleti hatóság a vizsgálati jogkörének gyakorlása során széles hatáskörrel fog bírni, például hozzáférést kell biztosítani az adatkezeléshez használt eszközökhöz. A hatóság vizsgálatot folytathat bejelentésre és hivatalból egyaránt. A vizsgálat során minden adatkezelőnek képesnek kell lennie a GDPR-nak való megfelelés igazolására.

Milyen lépések szükségesek a GDPR-ra való felkészüléshez?

Az Európai Parlament és a Tanács 2016/679 rendeletének első fejezetében a 2. cikk által meghatározott tárgyi hatálya alá eső összes adatkezelőre fogalmazza meg a jogokat és kötelezettségeket. **A rendelet nem tér ki pontosan (taxatíve) a kötelező elemek megfogalmazására.**

<u>Az alábbiakat mindenképpen javasolni lehet:</u>

- Az adatkezelő szervezetén belüli a GDPR ismeret megalapozása oktatással

- Folyamatok felmérése, adatkezelési folyamatok azonosítása

- Automatikus döntéshozatal felmérése

- Harmadik ország érintett-e

- Adatvagyon feltérképezése

- Incidens kezelés

- Informatikai működés felülvizsgálata (adatbiztonság, szabályzatok, nyilvántartások)

- Régebbi adatbázis felülvizsgálata

- Adatvédelmi szabályzat elkészítése

- Adatkezelési tájékoztatók elkészítése - Munkavállalókra - Szerződéses partnerek szerződéseinek kiegészítése, érintettekre, weboldalra,

- Nyilvántartások elkészítése - Adatkezelési folyamat nyilvántartás - Adatvédelmi incidens nyilvántartás - Kockázat elemzési, hatásvizsgálati nyilvántartás

- Szabályzatok és nyilvántartások hatályba léptetése, oktatása

- Jogszabályfigyelés

- Adminisztrációs és tudásbázis naprakészség biztosítása

- Rendszeres auditálás

A felkészülést segítő források:

• A hatályos adatvédelmi szabályozás megismerése: az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

• A GDPR szövege:

https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32016R0679

• A 29-es cikk szerinti Adatvédelmi Munkacsoport iránymutatásai:

https://www.naih.hu/29-es-munkacsoport-iranymutatasai.html

• NAIH állásfoglalások: https://www.naih.hu/az-adatvedelmi-reformmal-kapcsolatos-allasfoglalasok.html

https://naih.hu/felkeszueles-az-adatvedelmi-rendelet-alkalmazasara.html