Horváth Kiss & Bene Ügyvédi Társulás

GDPR alkalmazása a gyakorlatban

Dr. Horváth Péter Károly ügyvéd

Szeged, Vitéz utca 26. H-6722 Hungary

www.hkb.hu

horvath@hkb.hu

GDPR –Általános adatvédelmi rendelet

- Digitalizáció, globalizáció nagyfokú terjedése, egységes szabályozás
- 2 évvel ezelőtt (2016 május) fogadták el (felkészülés időszaka)
- Közvetlen hatály (Unió területén, Unión kívül is, ha az Unióban tartózkodó érintettek számára ad el árut, vagy nyújt szolgáltatást)
- 2018.05.25. napjától alkalmazandó

Az általános adatvédelmi rendelet (GDPR) legfontosabb fogalmai

- **Személyes adat:** azonosított vagy azonosítható természetes személyre (érintett) vonatkozó bármely információ (pld. név, szám, helymeghatározó adat, online azonosító, testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális, vagy szociális azonosságára vonatkozó egy vagy több tényező)
- **- különleges kategóriák:** faji, etnikai, politikai, vallási, világnézeti, szakszervezeti tagság, genetikai, biometrikus adatok, egészségügyi adatok, szexuális élet, irányultság. *Ezek kezelése fő szabály szerint: tilos*
- **Adatkezelés:** személyes adatokon, adatállományon automatizált, vagy nem automatizált módon végzett bármely művelet (gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés, összehangolás, korlátozás, törlés, megsemmisítés)
- **Érintett hozzájárulása:** önkéntes, konkrét, megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítás, félreérthetetlenül kifejező cselekedet útján

Alapelvek, jogalapok

Alapelvek: jogszerű, tisztességes eljárás, átláthatóság, **célhoz kötöttség, adattakarékosság,** pontosság, **korlátozott tárolhatóság** (cél eléréséhez szükséges ideig), **integritás és bizalmas jelleg** (megfelelő technikai vagy szervezeti intézkedések alkalmazása), **elszámoltathatóság**

Jogalapok:

- **érintett hozzájárulása**
- **szerződés teljesítéséhez szükséges**
- **adatkezelésre vonatkozó jogi kötelezettség teljesítése** (uniós, tagállami jog rögzíti)
- **érintett vagy egy másik természetes személy létfontosságú érdeke miatt**
- **közérdekű, vagy közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása** (uniós, tagállami jog rögzíti)
- **adatkezelő vagy harmadik fél jogos érdekeinek érvényesítéséhez szükséges** (kivéve, ha ezen érdekkel szemben elsőbbséget élvez az érintett érdeke, alapvető jogai (pld. gyermek)

Adatkezelő tájékoztatási kötelezettsége / Érintett hozzáférési joga

adatkezelő kiléte, elérhetősége, adatvédelmi tisztségviselő (ha van), tervezett **adatkezelés célja**, adatkezelés jogalapja, ha jogos érdek az alap, akkor annak részletezése, **személyes adatok címzettjei, kategóriái** (ha van ilyen), annak ténye, hogy harmadik országba kívánja továbbítani

További kötelezettség:

személyes adatok tárolásának időtartamáról, ha nem lehetséges az időtartam meghatározás szempontjáról, érintett jogairól **(hozzáférés, helyesbítés, törlés, kezelés korlátozása, tiltakozás, adathordozhatóság kérelmezése),** hozzájárulás bármikori visszavonásához való jog, **felügyeleti hatósághoz címzett panasz benyújtásának joga,** ha a személyes adat szolgáltatása jogszabályon, szerződéses kötelezettségen, vagy szerződés kötésének előfeltétele-e, érintett köteles-e a személyes adatokat megadni, mi a lehetséges következménye ennek elmaradása, **automatizált döntéshozatal ténye, profilalkotás (adatkezelés milyen jelentőséggel, következménnyel jár)**

Érintetti jogok:

- **hozzáférési jog** (lásd fenn)
- **helyesbítéshez való jog** (pontosság érdekében)
- **törléshez való jog** (ha nincs szükség rá a cél megvalósítása érdekében, érintett visszavonja a hozzájárulást (nincs más jogalap), jogellenes a kezelés, jogszabály írja elő a törlést)
- **adatkezelés korlátozásához való jog** (vitatja a pontosságot, adatkezelés jogellenes, nincs szükség rá, de az érintett igényli, hogy maradjon a jogi igényének érvényesítése, vagy védelme miatt) kezelni nem lehet CSAK tárolni
- **adathordozhatósághoz való jog** (HA hozzájáruláson/szerződésen alapul a kezelés ÉS az adatkezelés automatizált módon történik)
- **tiltakozáshoz való jog** (közérdekű feladatvégrehajtás és jogos érdekérvényesítési jogalap esetén, közvetlen üzletszerzés érdekében kezelik az adatokat - továbbiakban nem lehet e célból kezelni-)

Adatkezelő feladatai, Beépített és alapértelmezett adatvédelem

- az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a jogokra jelentett változó valószínűségű és súlyosságú kockázat figyelembevételével **megfelelő technikai és szervezési intézkedéseket hajt végre, és felülvizsgálja, valamint naprakészen tartja**
- tevékenységgel arányos **megfelelő belső adatvédelmi szabályokat hoz**
- **magatartási kódexet fogad el vagy jóváhagyott tanúsításhoz mechanizmushoz csatlakozik** (annak bizonyításaként, hogy teljesíti a kötelezettségét)
- alapértelmezés szerint **kizárólag olyan személyes adatok kezelésére kerüljön sor**, amelyek **az adott konkrét adatkezelési cél szempontjából szükségesek** (különösen azt kell biztosítani, hogy **ne válhassanak hozzáférhetővé meghatározatlan számú személy számára**)

Adatfeldolgozó feladatai

- Adatfeldolgozó az adatkezelő **előzetes írásban tett meghatalmazása nélkül további adatfeldolgozót nem vehet igénybe,** ha igénybe vesz ugyanazon feltételeket, kötelezettségeket kell telepíteni + megfelelő garanciák
- **írásbeli szerződést kell kötni** (vagy más jogi aktus), amely az **ADATKEZELÉS TÁRGYÁT, IDŐTARTAMÁT, JELLEGÉT, CÉLJÁT, SZEMÉLYES ADATOK TÍPUSÁT ÉS KATEGÓRIÁJÁT, valamint ADATKEZELŐ KÖTELEZETTSÉGÉT ÉS JOGAIT** tartalmazza, továbbá tartalmazza a következőket:
- **kizárólag az adatkezelő írásbeli utasítása alapján kezeli az adatokat**, kivéve, ha jogszabály írja elő az adatkezelést (ebben az esetben erről előzetesen értesíteni köteles adatkezelőt -kivéve ha az értesítést jogszabály tiltja-)
- **biztosítja, hogy a kezelésre feljogosított személyek titoktartási kötelezettséget vállalnak**, vagy jogszabályon alapuló titoktartási kötelezettség alatt állnak
- meghozza a 32 cikkben (**adatkezelés biztonsága) előírt intézkedéseket**, **megfelelő technikai és szervezési intézkedésekkel segíti adatkezelőt a kötelezettségei** (érintett jogainak biztosítása) **teljesítésében, segíti adatkezelőt** a 32-36 cikk **kötelezettség teljesítésében** (adatkezelés biztonsága, adatvédelmi incidens, adatvédelmi hatásvizsgálat)
- **adatkezelési szolgálat befejezését követően** adatkezelő döntése alapján minden **személyes adatot töröl, visszaad, törli a meglévő másolatokat** (kivéve ha a jogszabály az adatok tárolását írja elő)
- **adatkezelő rendelkezésére bocsát minden információt**, amely a kötelezettségek **teljesítéséhez szükségesek**, továbbá amely **lehetővé teszi** az adatkezelő vagy más ellenőr **auditját, helyszíni vizsgálatát** (és haladéktalanul jelzi ha valamely utasítás adatvédelmi rendelkezést sért)

Adatkezelési tevékenység nyilvántartása

Írásban, elektronikus formában (felügyeleti hatóságnak köteles rendelkezésre bocsátani, ha kéri és van ilyen), **250 főnél kevesebb személyt foglalkoztató vállalkozásnak nem kell vezetnie, ha az adatkezelés kockázattal nem jár, alkalmi jellegű, és nem kezel különleges vagy bűnügyi adatot**

ADATKEZELŐ a felelősségébe tartozóan végzett adatkezelésről nyilvántartást vezet a következőkről:

- adatkezelés célja, érintett kategóriáinak, személyes adatok kategóriáinak ismertetése, címzettek kategóriai (akikkel közli, vagy közölni fogják)

- harmadik országba/nemzetközi szervezet részére továbbításra vonatkozó információk (azonosítás, és 49 cikk (1) szerinti megfelelő garanciák részletezése)

- HA LEHETSÉGES (különböző adatkategóriák törlésére előirányzott határidők, valamint a technikai és szervezési intézkedések általános leírása

ADATFELDOLGOZÓ az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról nyilvántartást vezet az alábbiak szerint:

- adatfeldolgozó neve és elérhetőségei, az adatkezelő neve és elérhetőségei (akinek a nevében eljár), továbbá ezek képviselőjének és adatvédelmi tisztségviselőjének neve és elérhetősége, adatkezelési tevékenység kategóriái, harmadik országba/nemzetközi szervezet részére továbbításra vonatkozó információk (azonosítás, és 49 cikk (1) szerinti megfelelő garanciák részletezése)

- HA LEHETSÉGES (a technikai és szervezési intézkedések általános leírása)

ADATVÉDELMI INCIDENS

indokolatlan késedelem nélkül, legkésőbb 72 órán belül (késedelem esetén késedelem igazolását is be kell jelenteni) **kell jelenteni az illetékes felügyeleti hatóságnak KIVÉVE, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.** Az adatfeldolgozó az adatkezelőnek is jelent.

LEGALÁBB az alábbiakat:

- incidens jellege (érintettek és az érintett adatok kategóriája és hozzávetőleges száma), adatvédelmi tisztségviselő VAGY **kapcsolattartó neve, elérhetősége**, **incidens valószínűsíthető következménye**, **orvoslásra tett vagy tervezett intézkedés** (beleértve enyhítést célzó intézkedés)

Az adatkezelő a következő nyilvántartást vezeti: az incidenshez kapcsolódó tények, annak hatásai, és az orvoslásra tett intézkedések.

Valószínűsíthetően magas kockázat esetén **az érintett tájékoztatása is kötelező** (ugyanazt, amit a hatóságnak küldünk meg).

NEM KELL ÉRTESÍTENI, ha megfelelő technikai védelmi intézkedéseket hajtott végre, különösen, ha értelmezhetetlenné tette az adatokat, a az intézkedések miatt a magas kockázat nem valósul meg, tájékoztatás aránytalan erőfeszítést tenne szükségessé (ebben az esetben nyilvánosan kell közzétenni)

ADATVÉDELMI HATÁSVIZSGÁLAT, ELŐZETES KONZULTÁCIÓ

- Amennyiben az adatkezelés valószínűsíthetőleg magas kockázattal jár a természetes személyek jogaira.

KÖTELEZŐ

- módszeres és kiterjedt érékelés, amely **automatizált adatkezelésen** (profilalkotás) alapul, amely joghatással bíró vagy jelentős mértékben érintő döntések épülnek

- különleges személyes adatok

- nyilvános helyek nagymértékű, módszeres megfigyelése

- A felügyeleti hatóság erre jegyzéket fog összeállítani (ahol kötelező a hatásvizsgálat). Előzetes konzultáció kötelező, ha valószínűsíthető a magas kockázat.

ADATVÉDELMI TISZTSÉGVISELŐ

- csak a következő esetekben kötelező:

- közhatalmi szervek (kivéve bíróság)

- az adatkezelő és adatfeldolgozó **fő tevékenysége olyan adatkezelési művelet**, amely jellegénél fogva **rendszeres szisztematikus, nagymértékű megfigyelését teszi szükségessé az érintetteknek**

- adatkezelő, adatfeldolgozó **fő tevékenységei a különleges kategóriák, büntetőjogi felelősség megállapítására vonatkozó határozatokra** vonatkozik

Mit kell tennünk, hogy megfeleljünk a GDPR rendelkezéseinek

1. Meglévő adatbázisok felülvizsgálata (ADATVAGYONLELTÁR felmérése), ahol szükséges, ott a törlések, korlátozások végrehajtása, új adatbázisok építése

2. Érintetti tájékoztatók, hozzájáruló nyilatkozatok, illetve érdekmérlegelési tesztek ellenőrzése

3. Munkaügyi dokumentáció felülvizsgálata (NEM KÖTELEZŐ, DE AJÁNLOTT)

- munkaszerződés kiegészítése, intraneten kitett tájékoztatás (ÉRINTETTEK TÁJÉKOZTATÁSA) (külön pontban rögzíteni az adatkezelés körülményeit, illetve azt, hogy a GDPR alapján milyen jogai vannak a munkavállalónak)

- az adatkezelés végrehajtásában részt vevő **személyek oktatása (ADATVÉDELMI TUDATOSSÁG ERŐSÍTÉSE)**, valamint **írásos kötelezettségvállalási nyilatkozat aláíratása** (amely tartalmazza a legfontosabb kötelezettségeket)

- különböző szabályzatok elkészítése az informatikai biztonság fokozása céljából kameraszabályzat (ha van kamera), számítógép, telefon, e-mail használati szabályzat elfogadása stb.

- munkavállalónak joga van a munkáltatótól tájékoztatást kérni arról **(ÉRINTETT HOZZÁFÉRÉSI JOGÁNAK BIZTOSÍTÁSA)**, hogy milyen személyes adatokat tart nyilván a munkáltató róla. Az erre vonatkozó tájékoztató átadása ingyenes. **Érdemes ezért ezt már most az adatkezelési tevékenység nyilvántartásban összeírni hol, miért, és milyen személyes adatot kezelünk róluk.**

http://naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf

Mit kell tennünk, hogy megfeleljünk a GDPR rendelkezéseinek

- Egyes adatkezelési, adatfeldolgozói tevékenység nyilvántartása

- Adattovábbítás nyilvántartása

- Adatkezelés megszüntetésének nyilvántartása (Robinson lista)

- Adatvédelmi incidens nyilvántartása

Egyéb:

- érintetti, és hatósági megkeresés nyilvántartása
- Adatvédelmi tisztségviselő tevékenységének nyilvántartása
- Eltévedt megkeresések nyilvántartása
- Előzetes adatvédelmi hatásvizsgálat nyilvántartása

Mit kell tennünk, hogy megfeleljünk a GDPR rendelkezéseinek

Adatkezelés biztonságára vonatkozó belső szabályzat elkészítése, illetve megfelelő szervezeti és technikai intézkedések bevezetése, (a jogszabály azt írja, hogy az adatkezeléshez mérten megfelelő szintű legyen)

fizikai kontroll (riasztórendszer, kerítés, portaszolgálat, korlát, forgósorompó, kártyaolvasóval ellátott ajtó, biztonsági kamerák, stb.)

Adminisztratív (belső szabályzás üzletmentet-folytonossági terv, katasztrófaelhárítási terv) és logikai kontroll

hozzáférés, felhasználók szabályozása (hitelesítés felhasználónévvel, jelszóval, behatolásjelző rendszer, vírusellenőrző szoftver használata, szoftveres tűzfal, felhasználói profilok létrehozása, VPN technológia használata, mobil adattároló eszköz titkosítása, laptopokban lévő adattároló eszközök titkosítása, központi okostelefon-adminisztrációs szoftver használata)

adattároló eszközök, adatbevitel szabályozása (adminisztrátorok számának csökkentése a legszükségesebbekre, szerepkörök, jogosultságok „szükséges ismeret elve” alapján, alkalmazásokba való belépés naplózása, adattároló törlése újbóli felhasználás előtt, egyedi felhasználónév (nem felhasználói csoport), jogosultságok hozzárendelése a felhasználóhoz stb.)

rendelkezésre állás, megbízhatóság, adatok sértetlensége (szünetmentes áramellátás, tűz és füstjelző rendszerek, riasztás szerverszobában jogosulatlan belépés esetén, adatok helyreállíthatóságának tesztelése, biztonsági adatmentések tárolása elkülönített, biztonságos helyen, védett csatlakozóaljzatok, biztonsági mentési és helyreállítási terv kidolgozása, vészhelyzeti terv kidolgozása)

szétválaszthatóság, elkülönítés (fizikailag elkülönített tárolás, adatbázis jogosultság megállapítása, logikai ügyfélszétválasztás, álnevesítés, éles és tesztrendszerek elkülönítése stb.)

Mit kell tennünk, hogy megfeleljünk a GDPR rendelkezéseinek

- **Adatfeldolgozási szerződések megkötése, kiegészítése -ha van-** **(KÖTELEZŐ)**

- könyvelés, bérszámfejtés, weblap üzemeltetésével kapcsolatos szerződések, rendezvényszervezési szerződések kiegészítése, portaszolgálat (külső) stb.

- Természetes személy személyes adatainak megszerzése, és kezelése előtt a megfelelő **adatvédelmi tájékoztató elkészítése, megismertetése** (érintett jogairól való tájékoztatás, az adatkezelésre vonatkozó tájékoztatás) **a természetes személy nyilatkozatának rögzítése, hogy ezt megismerte és elfogadta** (érintett hozzájárulása) **KÖTELEZŐ**

- Köszönöm a megtisztelő figyelmet!