GDPR összefoglaló

(EU) 2016/679 rendelet

I. Általános rendelkezések

- **A rendelet csak természetes személyek adataira vonatkozik**
- Nem kell alkalmazni a rendeletet, ha pl.: uniós jog hatályán kívül eső tevékenységek során kezel valaki adatokat, de alkalmazni kell akkor, hogy ha a cégnek van tevékenységi helye az EU-ban, függetlenül attól, hogy az adatkezelés az Eu-ban vagy azon kívül történik.
- A rendelet nem lehet ellentétes az infótörvénnyel (2011. évi CXII.), sőt, az infótörvény nem szabályozhat semmit, amit már a rendelet szabályozott. Ha a rendelet és az infótörvény között ellentét áll fenn, úgy a rendeletet kell alkalmazni.
- **Mi számít személyes adatnak: azonosított vagy azonosítható természetes személyre vonatkozó bármely információ:** tényleg bármi, pl.: IP cím, online azonosítók, biometrikus adatok, stb.

II. Alapelvek, amiket be kell tartani az adatkezelés során

- **Jogszerűség**: az adatkezelést jogszerűen, tisztességesen, és az érintett számára átlátható módon kell kezelni;
- **Célhoz kötöttség**: gyűjtés csak meghatározott, egyértelmű és jogszerű célból történhet;
- **Adattakarékosság**: az adatkezelés céljai az adatok szempontjából relevánsnak kell lenniük, és a szükségesre kell korlátozódniuk;
- **Pontosság**: az adatoknak pontosnak és naprakésznek kell lenniük. Minden ésszerű intézkedést meg kell tenni annak érdekében, hogy a pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;
- **Korlátozott tárolhatóság**: az érintettek azonosítását csak az adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé;
- **Bizalmi jelleg**: az adatokat úgy kell kezelni, hogy az adatok biztonságban legyenek a jogellenes kezeléstől, véletlen elvesztéstől, megsemmisítésétől stb.

Jogszerűségről bővebben:

- **Az adatok kezelése csak akkor jogszerű, ha legalább az egyik alábbi feltétel teljesül:**
    - **az érintett a hozzájárulását adta;**
    - az adatkezelés olyan szerződés teljesítéséhez szükséges, melyben az érintett az egyik fél, vagy a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges (uniós vagy magyar jog is lehet);
    - **az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;**
    - az adatkezelés a személy létfontosságú érdekeinek védelme miatt szükséges;
    - az adatkezelés közérdekű vagy közhatalmi jogosítvány gyakorlásához kell (uniós vagy magyar jog is lehet);
    - az adatkezelés az adatkezelő vagy 3. fél jogos érdekeinek érvényesítéséhez kell.
- **Az adatkezelés célját a jogalapra** (tehát a fentiek valamelyikére) **hivatkozással kell meghatározni. E mellett meg lehet jelölni még** az adatkezelés tárgyát képező adatok típusát, az adatkezelés céljára vonatkozó korlátozásokat, az adattárolás időtartamát stb.
- Ha az adatgyűjtés a céljától eltérő célból adatkezelés nem hozzájáruláson vagy jogszabályon alapul, úgy meghatározott szempontokat kell figyelembe venni annak eldöntésére, hogy az eltérő célú adatkezelés helyénvaló volt-e (pl.: a többlet adatkezelés céljai és az alap adatkezelés céljai között volt-e esetleges kapcsolat)

Hozzájárulás feltételei (csak akkor alkalmazandó, ha az adatkezelés alapja az illető hozzájárulása)

- **Az adatkezelőnek igazolni kell, hogy az érintett hozzájárult adatainak kezelésére**. Ha a hozzájáruló nyilatkozat más ügyekre is vonatkozik, akkor a hozzájárulást a más ügyektől megkülönböztethetően kell megadni.
- **Az érintett a hozzájárulást bármikor visszavonhatja, de a visszavonás előtti adatkezelés jogszerűségét ez nem érinti**. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint a hozzájárulás megadását.
- **A hozzájárulás önkéntességét vizsgálni kell**: figyelembe kell venni, hogy a szerződés teljesítésének feltételéül szabták-e az olyan adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.
- 16 év alatti gyereknél a hozzájárulást a szülői felügyeletet gyakorló adja meg.

Tilos olyan adatot kezelni, mely faji, etnikai származásra, politikai véleményre, szexuális irányultságra, egészségügyi adatokra vonatkozik. Ez alól van kivétel, pl. az érintett kifejezett hozzájárulása.

Büntetőjogi felelősség megállapítására vonatkozó adatokat csak közhatalmi szervek kezelhetnek.

Azonosítást nem igénylő adatkezelés: Ha azok a célok, melyek alapján az adatokat kezelik, nem teszik szükségessé az érintettek azonosítását, úgy az adatkezelő nem köteles kiegészítő információkat megőrizni, beszerezni, kezelni. Ha az adatkezelő bizonyítani tudja, hogy nincs olyan helyzetben, hogy azonosíthassa az érintettet, úgy lehetőség szerint erről tájékoztatnia kell az érintettet.

III. Az érintett jogai

1. átláthatóság és intézkedések (12. cikk)

- **Az adatkezelő megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a rendelkezésre bocsátandó információt** (13. és 14. cikk) (függetlenül attól, hogy az érintettől, vagy nem az érintettől gyűjtötték) **tömör, átlátható, érthető, könnyen hozzáférhető formában nyújtsa**.
- Az adatkezelő annak érdekében is megfelelő intézkedéseket hoz, hogy az érintett hozzáférési (15.), helyesbítési és törlési jogáról (16,17.), adatkezelési korlátozáshoz való jogáról (18.), adatkezelő értesítési kötelezettségéről (19.), adathordozhatósághoz való jogáról (20.), titkosításhoz való jogáról (21.), profilozás megtagadásához való jogáról (22.), valamint az adatvédelmi incidensről való tájékoztatáshoz való jogáról (34.) szintén tömör, átlátható, érthető, könnyen hozzáférhető formában nyújtsa.
    - **Ezekről az intézkedésekről az érintettet 1 hónapon belül kell tájékoztatni. Ha rengetek az ügyfél, úgy ez a határidő 2 hónappal meghosszabbítható,** de erről 1 hónapon belül tájékoztatni kell az érintettet.
    - Ha nincs 1 hónapon belül intézkedés, úgy tájékoztatni kell az érintettet az elmaradás okáról, továbbá arról is, hogy panaszt nyújthat be a Felügyeletnél, és élhet bírósági jogorvoslati jogával
    - A 13. és 14. cikk szerinti információkat és a fenti tájékoztatást **díjmentesen kell biztosítani**.
    - Ha az érintett kérelme egyértelműen megalapozatlan vagy túlzó, akkor ésszerű díjat fel lehet számolni, vagy meg lehet tagadni a kérelmet. A megalapozatlanság vagy a túlzás bizonyításának terhe az adatkezelőé.
- **Fentieket írásban kell nyújtani**. Szóban is lehet akkor, hogy ha a személyazonosságot más módon igazolták.

2. Tájékoztatás és az adatokhoz való hozzáférés (13., 14. cikk)

a, Rendelkezésre bocsátandó infók, ha az infógyűjtés az érintettől történik

- az adatkezelő és képviselőjének elérhetősége;
- az adatvédelmi tisztviselő elérhetőségei (ha van adatvédelmi tisztviselő);
- az adatok kezelésének célja, jogalapja;
- ha az adatkezelés az adatkezelő, vagy egy 3. fél jogos érdekeinek érvényesítéséhez szükséges (6. cikk 1. f. pont), úgy meg kell jelölni ezt a jogos érdeket;
- a személyes adatok címzettjei (ha van ilyen);
- annak a ténye, ha az adatkezelő 3. országba/nemzetközi szervezet részére kívánja továbbítani az adatokat.

+ az adatok megszerzésének időpontjában a további tájékoztatást kell adni:

- az adatok tárolásának időtartama/az időtartam meghatározásának szempontjai;
- az érintettet azon jogáról, hogy kérheti az adatokhoz való hozzáférést, azok helyesbítését, törlését, kezelésük korlátozását, valamint az érintett adathordozhatósághoz való jogáról;
- ha az adatkezelés hozzájárulás alapján történt, úgy tájékozatni kell az érintettet, hogy hozzájárulását bármikor visszavonhatja;
- a felügyelethez címzett panasz benyújtásának jogáról;
- az automatizált döntéshozatal tényét.

Tájékoztatni kell továbbá arról is, hogy ha az eredeti céltól eltérő célból további adatkezelés kíván végezni az adatkezelő, úgy a további adatkezelést megelőzően kell tájékoztatni az érintetteket erről az eltérő célról + minden releváns információról.

b, Az érintett rendelkezésre bocsátandó infók, ha a személyes adatokat nem az érintettől szerezték meg

- teljesen ugyanaz, mint fent.

Az adatok megszerzésének időpontjában nyújtandó tájékoztatás

- Ugyanaz, mint fent, de meg kell jelölni azt is, hogy mi volt a személyes adatok forrása, illetve, hogy az adatok nyilvános forrásból származnak-e.

Ezeket a tájékoztatásokat az alábbiak szerint kell megadni

- **az adatok megszerzésétől számított 1 hónapon belül kell az érintettet tájékoztatni**
- Az adatokat közölni kell az érintettel az első kapcsolatfelvételkor

Célon túli adatkezelésnél a fentiekhez hasonlóan kell tájékoztatni az érintettet.
Nem kell tájékoztatni az érintettet, vagyis nem kell alkalmazni a b, pontban leírtakat, ha

- az érintett már rendelkezik az infókkal;
- lehetetlen, vagy aránytalan nagy nehézségekkel járna az infókat az érintett rendelkezésére bocsátani;
- az adat megszerzését vagy közlését a jog kifejezetten előírja;
- a személyes adatoknak jogszabály által előírt titoktartási kötelezettség alapján bizalmasnak kell maradnia.

3, Az érintett hozzáférési joga (15. cikk)

Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy az adatainak a kezelése folyamatban van-e, és ha igen, úgy jogosult arra, hogy a személyes adatokhoz és a következő infókhoz hozzáférést kapjon:

- az adatkezelés céljai;
- az érintett személyes adatainak kategóriái;
- azon címzettek kategóriái, akikkel az adatokat közölték/közölni fogják (különösen a 3. országbelieket);
- az adattárolás tervezett időtartama/az időtartam meghatározásának szempontjai;
- az érintett joga, hogy kérelmezheti az adatok helyesbítését, törlését, vagy a kezelés korlátozását + tiltakozhat az ilyen adatok kezelése ellen;
- panaszjog a felügyelethez;
- ha nem az érintettől történt az adatgyűjtés, akkor ki kell adni a forrást;
- automatizált döntéshozatal ténye és erre vonatkozó információk.

Ha a személyes adatok 3. országba vagy nemzetközi szervezetekhez továbbítják, úgy tájékoztatást kell adni az érintettnek a 46. cikkben leírt garanciákról.
Az adatkezelőnek a kezelendő adatokról másolatot kell adnia az érintettnek.

4. Helyesbítéshez, törléshez (elfeledtetéshez) és korlátozáshoz való jog, valamint az ezekhez kapcsolódó értesítési kötelezettség (16 - 19. cikk)

Helyesbítés: az érintett jogosult arra, hogy kérésére az adatkezelő helyesbítse a rá vonatkozó pontatlan személyes adatokat. Az érintett kérheti a hiányos személyes adatok kiegészítését is.

Törlés: az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, ha az alábbi indokok bármelyike fennáll

- **az adatkezelésre már nincs szükség abból a célból, melyből az adatokat összegyűjtötték;**
- **az érintett visszavonja az adatkezelési hozzájárulását, és nincs más jogalapja az adatkezelésnek;**
- az érintett tiltakozik (21. cikk 1 bek alapján) az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
- **az adatokat jogellenesen kezelték;**
- az adatokat jogszabályban előírt kötelezettség teljesítése miatt törölni kell;
- közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor az adatgyűjtésre

Ha az adatkezelő nyilvánosságra hozta az adatokat, de a fenti okok valamelyike alapján törölni köteles ezeket az adatokat, úgy ésszerűen elvárható lépéseket kell tennie annak érdekében, hogy tájékoztassa a nyilvánosságra került adatok kezelőit, hogy az érintett kérte a személyes adatokra mutató linkek vagy e személyes adatok másolatának törlését.
A fenti indokok alapján se lehet kérelemre törölni az adatokat, amennyiben az adatkezelés szükséges a

- véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;
- személyes adatok kezelését előíró, az adatkezelőre alkalmazandó jog szerinti kötelezettség teljesítése, illetve közérdekből vagy közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;
- népegészségügy területét érintő közérdek alapján, közérdekű archiválás céljából;
- jogi tények előterjesztéséhez, érvényesítéséhez, védelméhez.

Az érintett kérésére az adatkezelő köteles korlátozni az adatkezelést, ha az alábbiak valamelyike teljesül:

- az érintett vitatja a személyes adatok pontosságát. Ekkor mindaddig korlátozódik az adatkezelés, míg az adatkezelő nem ellenőrzi az adatok pontosságát;
- az adatkezelés jogellenes, de az érintett nem törlést, csak korlátozást kér;
- az adatkezelőnek már nem kellenek az adatok, de az érintett igényli azokat jogi tények előterjesztéséhez, érvényesítéséhez vagy védelméhez;
- tömeges adatkezelésnél az érintett tiltakozott. Ekkor a korlátozás addig tart, míg megállapításra kerül, hogy az adatkezelő jogos indokai, vagy az érintett jogos indokai élveznek jogos elsőbbséget.

A korlátozott adatokat a tárolás kivételével csak az érintett hozzájárulásával, közérdekből, vagy jogok védelmének érdekében lehet kezelni. Az érintettet a korlátozás feloldásáról előzetesen kell tájékoztatni.

Az adatkezelő minden helyesbítésről, törlésről és korlátozásról tájékoztatja azokat, akikkel az érintett személyes adatot közölték, kivéve, ha ez lehetetlen vagy aránytalanul nagy erőfeszítést igényel. A címzettekről az érintettet csak kérésre kell tájékoztatni.

5. Adathordozhatósághoz való jog (20. cikk)

Az érintett jogosult arra, hogy az adatkezelőtől az adatait széles körben használt, géppel olvasható formátumban megkapja, és ahhoz is joga van, hogy ezeket az adatokat odaadja egy másik adatkezelőnek anélkül, hogy ezt akadályozna a régi adatkezelő, ha

- az adatkezelés hozzájáruláson vagy szerződésen alapul ÉS
- automatizáltan történik az adatkezelés

Az adathordozhatósághoz való jog gyakorlásakor az érintett arra is jogosult (ha ez technikailag megoldható), hogy kérje az adatinak az adatkezelők közötti közvetlen továbbítását.

6. A tiltakozáshoz való jog (21. cikk)

Az érintett jogosult arra, hogy tiltakozzon

- a személyes adatainak a közérdekű vagy közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges adatkezelése ellen;
- az olyan adatkezelés ellen, ahol az adatkezelő/3. fél jogos érdekeinek érvényesítéséhez szükséges, és ezek a jogok elsőbbséget élveznek az érintett jogaihoz képest.

A fentiekbe bele kell érteni a profilalkotást is. Ha a fentiek megvalósulnak, úgy az adatkezelő nem kezelheti tovább az adatokat, kivéve, ha bizonyítja, hogy az adatkezelést olyan jogos okok indokolják, melyek elsőbbséget élveznek az érintett jogaihoz képest, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

Ha az adatszerzés közvetlen üzletszerzés érdekében történik, az érintet jogosult arra, hogy bármikor tiltakozzon az ilyen adatkezelés ellen (beleértbe a profilalkotást is). Ha az ilyen tiltakozás megtörténik, úgy az adatok a továbbiakban e célból már nem kezelhetők…

7. Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást is (22. cikk)

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan automatizált adatkezelésen alapuló döntés hatálya, amely rá nézve joghatással járna, vagy jelentős mértékben érintené, kivéve, ha

- ez az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges;
- ezt az adatkezelőre alkalmazandó olyan jogszabály teszi lehetővé, mely az érintett jogainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít;
- ez az érintett kifejezett hozzájárulásán alapul.

Az utóbbi 2 esetben biztosítani kell az érintettnek, hogy emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

8. Korlátozások (23. cikk)

Jogszabály korlátozhatja az 5. cikkben leírt alapelveket az érintet jogai tekintetében, ha a korlátozás tiszteletben tartja a jogok lényeges tartalmát, valamint a következők védelméhez szükséges és arányos az intézkedés, pl.: nemzetbiztonság, honvédelem, bírói függetlenség, stb.

IV. Adatkezelő és adatfeldolgozó

1. Az adatkezelő feladatai, beépített és alapértelmezett adatvédelem (24.,25. cikk)

Az adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre azért, hogy a személyes adatok kezelése e rendelettel összhangban történjen. Ha arányos, az adatkezelő e körben belső adatvédelmi szabályokat is alkalmaz (pl.: magatartási kódexszel, vagy jóváhagyott tanúsítási mechanizmushoz való csatlakozással).

Az adatkezelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy kizárólag olyan adatok kezelésére kerüljön sor, melyek a konkrét adatkezelési cél szempontjából szükségesek. A fő, hogy az adatok az illető beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára. A jóváhagyott tanúsítási mechanizmus alkalmazása egyértelműen bizonyítja, hogy az adatkezelő eleget tesz a követelményeknek.

2. Közös adatkezelők (26. cikk)

Ha az adatkezelés céljait és eszközeit 2/több adatkezelő közösen határozza meg, akkor ők közös adatkezelőnek minősülnek. Az adatkezelők megállapodnak a rendelet szerinti kötelezettségek teljesítéséért fennálló felelősségük megoszlását. A megállapodás lényegét az érintett rendelkezésére kell bocsátani. Az érintett valamennyi adatkezelővel szemben gyakorolhatja a rendeletben meghatározott jogait.

3. Az adatfeldolgozó (28-29. cikk)

Adatfeldolgozó: **Az adatkezelő nevében valaki más végzi az adatkezelést**. Az adatfeldolgozó az adatkezelő utasításának megfelelően kell,hogy eljárjon. Az adatkezelés szerződésnek, vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben. A szerződésbe a Bizottság és a Felügyelet általános szerződési feltételeket határozhat meg. A szerződést írásba kell foglalni.

4. Az adatkezelési tevékenység nyilvántartása (30. cikk)

Az adatkezelőnek (és ha van: képviselőjének) **nyilvántartást kell vezetnie az adatkezelési tevékenységéről** (kivéve a 250 főnél kevesebbet foglalkoztató cég, igaz ott is van olyan kivétel, mely szerint a 250 fő alatti cégnek mégis kell nyilvántartást vezetnie). A nyilvántartás az alábbiakat kell, hogy tartalmazza:

- adatkezelő neve és elérhetősége;
- adatkezelés céljai;
- érintettek kategóriáinak illetve a személyes adatok kategóriáinak ismertetése;
- azok a címzettek, akikkel az adatokat közölni fogják;
- az adatok 3. országba, vagy nemzetközi szervezetekhez való továbbítására vonatkozó infók;
- adatkategóriák törlésére előirányzott határidők;
- a 32. cikkben leírt szervezési és technikai intézkedések leírása.

Az adatfeldolgozónak plusz kötelezettségei is vannak. A nyilvántartást megkeresésre a Felügyelet rendelkezésre kell bocsátani.

Ezek a szabályok (vagyis a 30. cikk) **nem vonatkoznak a 250 főnél kevesebb személyt foglalkoztató vállalkozásokra**, kivéve (vagyis mégis vonatkoznak rájuk), ha

- az adatkezelés az érintett jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár;
- az adatkezelés nem alkalmi jellegű;
- az adatkezelés kiterjed a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok kezelésére.

5. Az adatkezelés biztonsága (32. cikk)

Az adatkezelő köteles technikai és szervezési intézkedéseket végrehajtani azért, hogy a kockázat mértékének megfelelő adatbiztonságot garantálja, ideértve adott esetben:

- személyes adatok álnevesítését és titkosítását;
- adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását;
- fizikai incidensek esetén az arra való képességet, hogy a hozzáférést és a rendelkezésre állást kellő időben vissza lehet állítani;
- az adatkezelés biztonságának garantálására vonatkozó intézkedések hatékonyságának rendszeres tesztelésére és értékelésére szolgáló eljárás.

Legkönnyebben a magatartási kódexhez vagy a jóváhagyott tanúsítási mechanizmushoz való csatlakozással lehet bizonyítani, hogy eleget tett az adatkezelő/feldolgozó a fenti követelményeknek. Az adatkezelőnek/feldolgozónak biztosítania kell azt is, hogy az irányításuk alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező, természetes személyek kizárólag az adatkezelő utasításainak megfelelően kezelhetik az adatokat.

6. Adatvédelmi jelentés incidens esetén (33-34. cikk)

72 órán belül jelenteni kell a felügyeletnek. Az incidenseket, és azok orvoslását nyilvántartani kell. A nyilvántartás alapján ellenőrzi a felügyelet, hogy az adatkezelő eleget tesz-e a rendeletnek. Az incidensről tájékoztatni kell az érintettet is akkor, ha az valószínűsíthetően magas kockázattal jár jogaira és szabadságaira nézve.

7. Adatvédelmi hatásvizsgálat és előzetes konzultáció (35-36. cikk)

Ha az adatkezelés valamely típusa (figyelemmel annak jellegére, hatókörére, körülményére és céljaira) **valószínűsíthetően magas kockázattal jár** a természetes személyek jogaira és szabadságára nézve, akkor **az adatkezelő még az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek hogyan érintik a személyes adatok védelmét**. Egymáshoz hasonló típusú, hasonlóan magas kockázattal bíró adatkezelési műveleteket egyetlen hatásvizsgálat keretei közt is értékelhetőek. Ha van adatvédelmi tisztviselő, akkor a hatásvizsgálat elkészítésekor ki kell kérni az ő szakmai tanácsait is.

Az adatvédelmi hatásvizsgálatot különösen akkor kell elvégezni

- egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, mely automatizált adatkezelésen alapul, és melyre a természetes személy tekintetében joghatással bíró/jelentős mértékben érintő döntések épülnek, vagy
- különleges személyes adatok kategóriái/ büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése, vagy
- nyilvános helyek nagymértékű, módszeres megfigyelése.

A felügyelet összeállítja és nyilvánosságra hozza az adatkezelési műveletek típusainak a jegyzékét, amelyre vonatkozóan adatvédelmi hatásvizsgálatot kell végezni. Nem kötelező, de a felügyelet létrehozhat olyan adatkezelési műveletek típusainak jegyzékét, melynél nem kell hatásvizsgálatot végezni.

Az adatkezelési műveletek hatásainak értékelése során figyelembe kell venni, hogy a szóban forgó adatkezelők, illetve adatfeldolgozók teljesítik-e a magatartási kódex előírásait.

Ha az adatkezelés jogi kötelezettség teljesítése, vagy közérdekű/közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, és ezen adatkezeléseket előíró jogszabályok konkrét adatkezelési műveleteket is szabályoznak + a jogalap elfogadásakor egy általános hatásvizsgálat részeként már amúgy is végeztek hatásvizsgálatot, akkor nem kell újabb hatásvizsgálatot lefolytatni.

Az adatkezelő legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le. Az ellenőrzés célja, hogy az adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

Előzetes konzultáció: Erre akkor van szükség, hogy ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a kockázatok mérséklése céljából tett intézkedések hiányában magas kockázattal jár. A megállapítást követően az adatkezelő konzultál a felügyeleti hatósággal. Ha a felügyelet szerint is sértené a rendeletet az adatkezelés, úgy a megkereséstől számított 8 héten belül írásban tanácsot ad, és gyakorolja a hatásköreit.

8. Adatvédelmi tisztségviselő kijelölése, jogállása, feladatai (37-39. cikk)

Adatvédelmi tisztviselőt kell kijelölni, ha

- az adatkezelést közhatalmi vagy közfeladatot ellátó szervek végzik, kivéve a bíróságokat;
- az adatkezelő/feldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, mely jellegüknél fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszi szükségessé;
- az adatkezelő/feldolgozó fő tevékenységei a különleges adatok és a bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalja magában.

Vállalatcsoportnál és közhatalmi/közfeladatot ellátó szervnél lehet közös adatvédelmi tisztviselő is (ha…). Adatvédelmi tisztviselő vagy az adatkezelő/feldolgozó alkalmazottja lehet, vagy szolgáltatási szerződés keretében látja el a feladatát. Az adatvédelmi tisztviselő neve és elérhetősége nyilvános. Függetlenséget élvez.

V. Magatartási kódexek és tanúsítás (röviden)

1. Magatartási kódex (40-41. cikk)

Az adatkezelők/feldolgozók kategóriát képviselő egyesületek/egyéb szervezetek magatartási kódexeket dolgozhatnak ki. A Bizottság határozhat úgy, hogy a hozzá benyújtott kódexek az Unió területén általános érvénnyel rendelkeznek A jóváhagyott kódexet az Európai Adatvédelmi Testület fogja publikálni.

2. Tanúsítás (42. cikk)

A tagállamok, Bizottság stb. ösztönzik olyan adatvédelmi tanúsítási mechanizmusok, adatvédelmi bélyegzők, jelölések létrehozását, melyek bizonyítják, hogy az adatkezelő/feldolgozó által végrehajtott adatkezelési műveletek megfelelnek a Rendeletnek. A tanúsításnak önkéntesnek kell lenni.

A tanúsításokat a Tanúsító szervezetek vagy a tagállami felügyelet állítja ki. A tanúsítvány 3 évre szól, de megújítható. A Testület, akár csak a kódexeket, ezt is publikálja.

3. Tanúsító szervezetek (43. cikk)

A tanúsítvány kiállítását és megújítását olyan tanúsító szervezet végzi, amely az adatvédelem terén megfelelő szakértelemmel rendelkezik. A tagállamok akkreditálják ezeket a szervezeteket

Összefoglalva:

1. Amikor az ügyféllel kapcsolatot létesítünk, az első hogy meghatározzuk az adatkezelés célját (pl. jogi kötelezettség, vagy érintett hozzájárulása). Ha hozzájárulással történik az adatkezelés, akkor az adatkezelőnek igazolni kell, hogy az érintett tényleg hozzájárult a kezeléshez. Vizsgálni kell ilyen esetben az önkéntességet is.

2. **Az érintett részére tömör átlátható érthető tájékoztatást kell adni a jogairól** (hozzáférési, helyesbítési és törlési, adatkezelés korlátozási, értesítés, adathordozhatóság, titkosítás, profilozás, incidensről tájékoztatás), függetlenül attól, hogy az adatok közvetve vagy közvetlenül származnak az érintettől. **LÁSD: adatkezelési tájékoztató**

3. A jogokról röviden:

- Az érintettnek joga van arra, hogy az adatkezelőtől visszajelzést kapjon arról, hogy az adatait kezelik-e (hozzáférési jog). A kezelt adatokról másolatot kell adni az érintettnek.
- Az érintettnek joga van, hogy kijavíttassa a kezelővel a hibás adatokat. Joga van arra is, hogy töröltesse magát (meghatározott feltételek esetén, pl.: már nincs szükség az adatkezelésre abból a célból, miből az adatokat gyűjtötték) és arra is, hogy korlátoztassa az adatkezelést (pl.: ha az érintett vitatta az adatok pontosságát, úgy korlátozódik az adatkezelés a vitás helyzet tisztázásáig).
- Az érintettnek joga van arra, hogy az adatait mindenki számára elérhető (pl.: pdf) formátumban kapja meg (adathordozhatósági jog).
- Tiltakozhat is, de ennek csak közhatalmi adatkezelésre, meg olyan adatkezelésre vonatkozik, ahol az adatok jogos érdekérvényesítéshez kellenek.

4. Adatkezelő és feldolgozó

- Kötelesek megfelelő technikai és szervezési intézkedéseket végrehajtani jogszabályszerű működés eléréséért.
- Az adatkezelő köteles nyilvántartást vezetni az adatkezelési tevékenységről (aki 250 fő alatti cég, annak nem kell, kivéve, ha az adatkezelés nem alkalmi jellegű).

5. Adatvédelmi hatásvizsgálat, előzetes konzultáció

- Adatvédelmi hatásvizsgálat: Ezt akkor kell elvégezni, ha az adatkezelés valószínűsíthetően magas kockázattal jár az illető jogaira és szabadságára nézve. Ezt főleg akkor kell elvégezni, ha nyilvános helyeket figyelünk meg módszeresen.
- Előzetes konzultáció: Erre akkor van szükség, ha az adatvédelmi hatásvizsgálat megállapítja, hogy ha adatkezelés magas kockázattal jár.

6. Adatvédelmi tisztségviselő

- Ilyet nem kell kijelölni egy átlagos cég esetében (akkor kötelező, ha pl.: az adatkezelő olyan adatkezelői műveleteket végez, mely jellegüknél fogva az érintettek rendszeres és szisztematikus megfigyelését teszi szükségessé).

Konklúzió:

A GDPR sok általánosságot tartalmaz, melyeket a hazai szabályozásnak kellenek kibontania és részleteznie, a hazai szabályozás azonban nem teljes, az Infotörvény módosítására még nem került sor. A GDPR szerint a tagállami jogalkotóknak kell kijelölni a felügyeleti hatóságot, ez azonban hazánkban még nem történt meg. Ez a hatóság nagy valószínűséggel a Nemzeti Adatvédelmi és Információszabadság Hatóság lesz.

Nem tisztázott, hogy kiknek kell nyilvántartani az adatkezelési tevékenységet. A Rendelet szerint a 250 fő alatt foglalkoztató cégeknek nem kell, de ugyanakkor minden cég számára mérettől függetlenül kötelezővé teszi a nyilvántartás készítését, ha az „adatkezelés nem alkalmi jellegű". Az, hogy mi számít nem alkalmi jellegű adatkezelésnek egyelőre nem tisztázott.

Nem meghatározható az se, hogy például álláspályázatok esetén mit kell tennie a munkáltatónak a beérkezett önéletrajzokkal abban az esetben, ha valakit be sem hívnak interjúra, hiszen ebben az esetben nem lehet vele aláíratni az adatkezelési nyilatkozatot? A rendelet értelmezése azért is különösen nehéz, mert az egész Európai Unióban 2018. május 25-én lép hatályba a GDPR, tehát nincs más tagállami szabályozás, melyet figyelembe lehetne venni kétség esetén.

Jelenleg a 2018-as országgyűlési választások miatt az országgyűlés nem ülésezik, és várhatóan 2018. május közepéig nem is fog. A megalakuló Parlament várhatóan nem a GDPR által megkívánt haza szabályozás megteremtésével kezdi meg a jogalkotási munkát, így valószínűsíthető, hogy 2018. május 25. napjáig, azaz a GDPR hatályba lépésének napján nem lesz vonatkozó hazai szabályozás. Mivel nem lesz szabályozás, így egyelőre a bírságolás se lenne jogszerű. Álláspontunk szerint jelen jogi szabályozásra tekintettel a GDPR vonatkozásában az adatvédelmi tájékoztatás megadása az érintettek részére (amennyiben az lehetséges) elégséges és megfelelő magatartás.

Véleményünk szerint – mivel a hazai szabályozás az adatvédelem területén már így a legszigorúbbak között található az Európai Unióban – a GDPR elsősorban a nagy ügyfélforgalmat, adatforgalmat bonyolító cégek esetében jelent elsősorban kiemelt figyelmet a hatóságok részéről. Az ilyen vállalkozásoknak külön figyelmet kell majd fordítania az online felületüktől kezdve az adatvédelmi nyilvántartáson át az esetleges adatvédelmi tisztségviselőig minden területre, melyet a GDPR előír.

Budapest, 2018. április 25.

Dr.Buglos Katalin
Ügyvédi Iroda