**Mi az a GDPR?**

***2018. május 25.***napjától közvetlenül alkalmazandó Magyarországon is az Európai Parlament és a Tanács (EU) 2016/679 rendelete, ún. **Általános Adatvédelmi Rendelet *(GDPR).***

A GDPR meghatározza az adatkezelők és adatfeldolgozók legfontosabb kötelezettségeit és az Érintettek jogait is.

Felmerülhet a kérdés, hogy kik az adatkezelők, illetve az adatfeldolgozók.

A GDPR szerinti definíciók:

 „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;

Fontos, hogy az adatkezelő megbízásából kezeli az adatokat. (Az adatkezelés célját nem ő, hanem az adatkezelő határozza meg.)

„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.

Általánosságban ezek a szervezetek, hatóságok a törvényben meghatározott állandó adatátadásokkor fordulnak elő.

**GDPR célja**

Mi a tulajdonképpen a célja a GDPR-nak?

* a személyes adatok megfelelő biztonságának, védelmének megvalósítása;
* az adatok kezelése, felhasználása átláthatóságának biztosítása;
* a személyek jogainak bővítése (természetes személy), azaz nagyobb fokú rendelkezés a személyes adatok felett.

**Mi számít személyes adatnak?**

Természetesen az egyértelmű adatokon kívül, mint például, név, cím, születési adatok stb. lehetnek kevésbé egyértelmű adatok is, mint pl. IP cím, email cím, fénykép, IMEI szám, az internetes cookie stb. Érdemes tudni, hogy akár egy weboldal meglátogatásával is személyes adatokat adunk meg magunkról, hiszen IP címünk és ezzel a tartózkodási helyünk is küldésre kerül a szerver felé.

Meg kell megemlíteni a különleges személyes adatot is, amelyet a GDPR külön definiál:

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.

Ezen adatokat szükséges fokozott biztonsággal kezelni.

**Az adatkezelés jogalapja, azaz mikor kezelhet a Szervezet személyes adatokat? (GDPR 6. cikk)**

1. az Érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
2. 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;
3. az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
4. az adatkezelés az Érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
5. az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
6. 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.*

Az f) pont nem alkalmazható a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre.

A személyes adatok általában nem hozzájárulás alapján kerülnek kezelésre, túlnyomó többségben a 6. cikk (1) bekezdés e) pontja a megfelelő jogalap, a vonatkozó jogszabályok feltűntetésével.

Hozzájárulás csak abban az esetben lehet jogalap, ha nincs semmilyen vonatkozó jogszabály, amelyre hivatkozhatunk. Általában az Érintett által önként vállalt, nem kötelező feladatok/folyamatok esetén fordul elő.

**Meddig tárolhatók az adatok?**

Egyes esetekben törvény határozza meg a megőrzési időt, ilyenkor a megadott időket szükséges betartani.

Elfordulnak olyan folyamatok is, amikor az Érintett hozzájárulása a jogalap, pl. rendezvények esetén. Ezekben az esetekben az iratok nem kerülnek iktatásra, így tulajdonképpen bármikor törölhetők. Ilyenkor a rendezvény végéig, illetve az ügyfél hozzájárulásának visszavonásáig tart a megőrzés, vagy esetleg a polgári jogi igények elévülési idejéig, azaz 5 évig. Feltéve, hogy egyéb előírás nem vonatkozik rá (pl. projektek esetén).

**A GDPR alapelvei**

A GDPR számos alapelvet felsorol, amely elveknek a teljes adatkezelés folyamata során meg kell felelni, és tudni kell bebizonyítani, hogy az adatkezelés megfelel a GDPR alapelveinek – ezt a legfőbb alapelv, az elszámoltathatóság elve mondja ki. Ezen kötelezettség miatt szükséges minden adatkezelési műveletet, minden mozzanatot dokumentálni.

1. Az adattakarékosság elve

Fölöslegesen nem szabad adatot felvenni, csak is annyit, amennyit a jogszabály megenged, amennyi a feladat ellátásához szükséges, illetve amelyekhez az Érintett hozzájárult. Szükséges, hogy igazolható legyen adott személyes adat kezelésének célja.

Tehát nem szabályos nem szükséges adatot felvenni azért, mert a későbbiekben még szükség lehet rá.

2. Célhoz kötöttség

Az adatok csak is kizárólag az előre megadott cél érdekében gyűjthetők és kezelhetők. Ezen célokról az ügyfél az adatok megszerzésének pillanatában kap tájékoztatást. Akkor, ha ezen céltól eltérően szeretné a Szervezet felhasználni az adatokat, értesíteni/tájékoztatni kell az ügyfelet, esetlegesen hozzájárulását kérni.

3. Az adatok pontossága

Abban az esetben, ha pontatlan vagy javításra szoruló adat kerülne a rendszerbe, az a későbbiek során módosítható.

4. Elszámoltathatóság

A Hivatalnak képesnek kell lennie annak igazolására, hogy az adatvédelmi szabályoknak megfelel.

A GDPR az Érintettet védi. Vagyis a Szervezetnek-nek kell bebizonyítania, hogy helyesen járt el a személyes adatok kezelése során, nem pedig az Érintettnek, hogy helytelenül.

5. Jogszerűség, tisztességes eljárás és átláthatóság

Az adatok kezelését jogszerűen és tisztességesen, valamint az Érintett számára átlátható módon kell végezni. Ezen alapelv miatt szükséges minden adatkezelés esetében az Érintett számára érthető és átlátható módon megfogalmazott adatkezelési tájékoztató.

6. Korlátozott tárolhatóság

Az adatok tárolásának olyan formában kell történnie, amely az Érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, a GDPR-ban az Érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.

7.Integritás és bizalmas jelleg

Az adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

**Érintetti jogok és tájékoztatások**

Minden személyes adatkezelés kapcsán szükséges tájékoztatást adni az Érintettnek, illetve mindazoknak, akiknek bármilyen formában a személyes adatát kezeli a Szervezet, ilyen pl. a Szervezet honlapját meglátogató természetes személy, akinek az IP címét egy cookie letölti.

Ha az Érintettre vonatkozó személyes adatokat az Érintettől gyűjtik, az adatkezelő a személyes adatok megszerzésének időpontjában az Érintettet köteles tájékoztatni, tehát itt egy előzetes tájékoztatási kötelezettségről van szó.

A GDPR pontosan meghatározza azokat az elemeket, amelyeket egy adatkezelési tájékoztatónak tartalmaznia kell.

Ha az Érintettre vonatkozó személyes adatokat nem az Érintettől gyűjtik, a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül szükséges a tájékoztatást megadni. Ha a személyes adatokat az Érintettel való kapcsolattartás céljára használják, akkor legalább az Érintettel való első kapcsolatfelvétel alkalmával szükséges a tájékoztatás.

Nem szükséges újra tájékoztatni az ügyfelet, ha igazolható, hogy már megkapta a tájékoztatást.

Jogok

*Tájékoztatáshoz való jog*

Az ügyfelet tájékoztatni kell az adatkezelés GDPR-ban meghatározott lényeges tartalmáról.

*Hozzáférés joga*

Az Érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a GDPR-ban meghatározott információkhoz hozzáférést kapjon. Tehát egy utólagos, az adatkezelés megkezdését követő tájékoztatáshoz való joga van.

Az adatkezelő ebben az esetben az adatkezelés tárgyát képező személyes adatok másolatát az Érintett rendelkezésére bocsátja. Az Érintett által kért további másolatokért az adatkezelő az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel. Ha az Érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az Érintett másként kéri.

A másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait.

*Adathordozáshoz való jog*

Az Érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha:

a) az adatkezelés jogalapja az Érintett hozzájárulása vagy az adatkezelés szerződésen alapul; és

b) az adatkezelés automatizált módon történik.

Mindez azt jelenti, hogy amennyiben az adatkezelés automatizált módon történik, akkor az Érintettnek joga van az adatait digitális formában kikérni, sőt akár azt is kérni, hogy az adatokat közvetlenül egy másik adatkezelőnek küldjék meg (Szervezet esetében e joggal többnyire nem élhet, mert az adatkezelés általában közhatalmi jogosítványon alapul.)

*Helyesbítéshez való jog*

Az ügyfél kérheti pontatlan vagy nem naprakész adatainak javítását. Ezzel a jogával eddig is élhetett az ügyfél, ez most sincs másképp, az eljárás menete tulajdonképpen egyezik.

*Az adatkezelés korlátozásához való jog*

A GDPR-ban meghatározott esetekben az Érintett korlátozhatja az adatkezelést. Ilyen esetben a személyes adatokat a tárolás kivételével csak az Érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Európai Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni. Azaz az adatot tárolja a Szervezet, de semmit nem kezdhet vele a fentieken túl.

*Törlés joga*

Az Érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az Érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha az alábbi indokok valamelyike fennáll:

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;

b) az Érintett visszavonja a 6. cikk (1) bekezdésének a) pontja vagy a 9. cikk (2) bekezdésének a) pontja értelmében az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;

c) az Érintett a 21. cikk (1) bekezdése alapján tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az Érintett a 21. cikk (2) bekezdése alapján tiltakozik az adatkezelés ellen;

d) a személyes adatokat jogellenesen kezelték;

e) a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

f) a személyes adatok gyűjtésére a 8. cikk (1) bekezdésében említett, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

*Tiltakozáshoz való jog*

Az Érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a 6. cikk (1) bekezdésének e) (közhatalmi adatkezelés) vagy f) pontján (jogos érdek) alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos érdekek indokolják, amelyek elsőbbséget élveznek az Érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

*Automatizált döntéshozatal*

Az Érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen - ideértve a profilalkotást is - alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

Ilyen döntéshozatal egy Szervezet esetén általában nem fordul elő. Ha esetlegesen mégis alkalmazva lenne, úgy az ügyfélnek jogában áll emberi beavatkozást kérnie a folyamathoz.

Felhívjuk a figyelmet, hogy a GDPR szerinti *automatizált döntéshozatal* fogalma nem azonos az általános közigazgatási eljárásról szóló 2016. évi CL. törvény (Ákr) *automatikus döntéshozatal* fogalmával.

**Eljárás Érintetti kérelem esetében**

A GDPR Érintetti kérelmek nyilvántartásában dokumentálni kell ezeket a kéréseket.

A kérelemről a DPO-t haladéktalanul tájékoztatni kell, a kérelemmel kapcsolatban a DPO jár el.

Az Érintett kérelmét 1 hónapon belül kell megválaszolni, indokolt esetben ez kitolható kettő hónappal.

**Nyilvántartások**

A GDPR alapján, valamint a korábban már említett elszámoltathatóság alapelvéből következően a Hivatal számos nyilvántartás vezetésére köteles.

Ezeket a nyilvántartásokat a Szervezet által szolgáltatott adatok és információk alapján a DPO vezeti.

A nyilvántartásoknak létrehozásához a Hivatal dolgozók közreműködésére is szükség volt, naprakészen tartásához is elengedhetetlen a hivatali közreműködés. Ha ugyanis a DPO nem értesül arról, hogy pl. egy új eljárás került bevezetésre, nem fogja tudni a nyilvántartásban szerepeltetni. Ha nem értesül egy incidensről, akkor nem fog tudni intézkedni. Ha esetlegesen a rendszeresített dpo@kozinformatika.hu email cím mellett hivatali dolgozóhoz közvetlenül érkezik be kérelem pl. Érintettől, amelyben az egyik jogát szeretné érvényesíteni, azt is jelezni kell a DPO-nak.

A Hivatal adatvédelmi szabályzata pontosan meghatározza az eljárásokat, amelyeket követni kell az adatkezelés során.

A Hivatal-on belül létrehozásra került egy „adatvédelmi munkacsoport”, melynek tagjai tartják a kapcsolatot a DPO-val. A munkacsoportban minden igazgatóság képviselteti magát.

Elkészült a Szervezet **„Személyes adat térképe”**. Ez a nyilvántartás tartalmazza a Szervezet által a különböző folyamatokban kezelt személyes adatokat, amelyet kötelező vezetni a GDPR szerinti **adatkezelői nyilvántartásként**.

Ebben a nyilvántartásban tulajdonképpen az adatkezelési tájékoztatókban megemlített adatok kerülnek fölvételre. Tartalmazza a Szervezetben-ben lévő folyamatokat, az adatkezelés célját, megőrzési időt, adatátadást más szerveknek stb.

Szükséges továbbá számon tartani a beérkezett **adatvédelemmel kapcsolatos kérelmeket**. Erre külön nyilvántartás készült.

**Adatvédelmi incidensek nyilvántartása** is előírás, amely az adatvédelmi incidenseket tartalmazza, az incidens felismerésétől kezdve, az esetleges NAIH és Érintetti értesítésig.

**MI számít adatvédelmi incidensnek?**

GDPR szerint "adatvédelmi incidens" 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;

Minden adatvédelmi incidensről szükséges tudnia a DPO-nak, mivel az incidenst szükséges lehet jelezni (az ügy komolyságától függően) 72 órán belül a hatóságoknak, valamint az Érintettet is tájékoztatni szükséges.

Érdemes a DPO-t minden akár incidensnek tűnő esetről is értesíteni, hogy legyen mód annak eldöntésére, hogy szükséges-e incidensként kezelni az ügyet.

Minden olyan esetben, ami adatvédelemmel kapcsolatos, ahol esetlegesen GDPR vonzatú kérelem érkezett be, vagy új adatkezeléssel járó ügy került bevezetésre, a DPO-t kell keresni az alábbi elérhetőségen.

* Közinformatika Kft. (dpo@kozinformatika.hu)).