GDPR - ÁLTALÁNOS ADATVÉDELMI RENDELET
2018. MÁJUS 25-TŐL

1. 2018. május 25-én hatályba lép az Európai Parlament és a Tanács (EU) 2016/679. számú rendelete 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)**

2. **A GDPR** az EU általános adatvédelmi rendelete, milyen olyan szervezetre, intézményre és vállalatra kiterjed a hatálya, ami EU állampolgárhoz kapcsolódó személyes adatot tárol, feldolgoz, felhasznál. Tehát a nagy cégektől az egyéni vállalkozókig, a kkv-ktől a civil szervezetekig mindenkire, aki személyes adatokat kezel, a GDPR szabályait alkalmazni kell.

3. Eddig is volt adatvédelemmel kapcsolatos szabályozás, a jelenleg is hatályban lévő infotörvény, a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. Ez a törvény bizonyos passzusait tekintve még szigorúbb, mint a most hatályba lépő EU-s rendelet, tehát akinek eddig e törvény alapján már volt adatvédelmi, adatkezelési szabályzata, annak annyi a teendője, hogy összhangba hozza szabályzatát az EU-s rendelettel.

4. A magyar jogi szabályozás sajnos késik, azonban - idézve Péterfalvi Attila, a Nemzeti Adatvédelmi és Információszabadság Hatóság elnökének (Varga Mihály miniszterhez írt) levelét, a GDPR közvetlen alkalmazása Magyarországon is kötelező, tehát függetlenül attól, hogy a hazai szabályozás megszületett vagy sem.

5. A GDPR hatálybalépése előtt több törvény – köztük kétharmados törvények – módosítására is szükség van. Pl. ahhoz, hogy a NAIH május 25. után is adatvédelmi hatóságként tudjon eljárni, a parlament kétharmados többségének meg kell szavaznia a szükséges törvénymódosítást, amelyben erre a feladatra kijelölik a hatóságot.

   A Parlament alakuló ülése már megvolt, kérdés, hogy milyen ütemben folyik majd a munka, hiszen az újonnan megválasztott Országgyűlés tárgysorozatán 29 törvényjavaslat, 1 határozati javaslat és 5 beszámoló maradt az előző ciklusról.

   Mivel az Európari Bizottság a nemzeti hatóságoktól státusjelentést is kér arról, hogyan állnak a GDPR alkalmazásához szükséges felkészüléssel, és amennyiben nem születnek meg a szükséges jogszabályok, akkor akár kötelezettségszegési eljárást is indíthatnak az adott országok ellen (Péterfalvi Attila korábbi nyilatkozata szerint), minden bizonnyal prioritást élveznek a GDPR-rel kapcsolatos törvénymódosítások az Országgyűlés törvénykezési programjában, annál is inkább, mert 2018. május 25-től az általános adatvédelmi rendelet alkalmazásáért felelős uniós szerv az Európai Adatvédelmi Testület, amelyet az egyes adatvédelmi hatóságok vezetői és az európai adatvédelmi biztos vagy ezek képviselői alkotják. Ez a testület kötelező erejű döntéseket is elfogadhat a határokon átnyúló adatkezelésre vonatkozó viták esetén,

biztosítva az uniós jogszabályok egységes alkalmazását, annak elkerülésére, hogy ugyanazt az ügyet a különböző joghatóságok esetleg eltérően kezeljék. Legfontosabb szerepe a testületnek: a tagállamok hatóságai közötti együttműködés intézményi megjelenése.

6. Az új szabályozással kapcsolatban minden cikkben, felhívásban, ismertetőben elsőként a mulasztókkal szembeni bírság kiszabása jelentik meg, a kötelezettségek megsértése esetén akár 20 millió eurós bírság is kiszabható. A GDPR az adatkezelés típusa alapján differenciálja a kiszabható bírság összegét, amely a jelenlegi - nálunk az infotörvény alapján kiszabható - 20 millió forintos maximumhoz képest 20 millió euró vagy a globális éves árbevétel 4 %-a is lehet. A magasabbat alkalmazzák.

   A Nemzeti Adatvédelmi és Információbiztonság Hatóság, a NAIH általában panaszbeadványok alapján jár el, nem valószínű, hogy váratlanul megjelenne az adatkezelőnél, de azokat a dokumentumokat elkérik, amivel igazolható, hogy az adatkezelők átvizsgálták adatkezelésüket és az megfelel a GDPR-nak.

   Tehát nem valószínű, hogy a bírságolást a civil szervezetekkel kezdenék, még akkor sem, ha időben megkapja a NAIH a törvényi felhatalmazást, azonban fontos, hogy a GDPR-nak való megfelelés érdekében **minden tagegyesületünk megtegye a legszükségesebb lépéseket.**

   Sok még a bizonytalanság, hiányoznak a hazai jogszabályok, ennek ellenére fontos célkitűzésünk kell legyen, mind a szövetségnek, mind a társaságoknak, hogy - mint első verziók - legyenek meg a tájékoztatók, szerződések, nyilatkozatok, történjen meg a folyamatok és teendők listázása.

   Néhány hónapja még alig találhattunk információt a GDPR rendelet szövegén és néhány ajánláson kívül, ma már ennél egyrészt jobb a helyzet, a GDPR rendelet értelmezéséhez kapcsolódó dokumentumok száma egyre nő, különösen a 29. cikk alapján létrehozott munkacsoport ajánlásai érdemesek a figyelemre.

   Ezek nagy része magyarul is letölthető. Amennyiben további információk rendelkezésre állnak, az anyagokat megfelelően módosítani, pontosítani, aktualizálni kell. Fontos, hogy az ne forduljon elő, hogy nincs semmiféle anyaga egy-egy társaságnak az adatvédelem szabályozására, és annak megfelelő gyakorlat sem működik.

   Másfelől ma már annyi információ, javaslat, értelmezés található a net-en (sokszor ezek az anyagok némely részeiben ellentmondóak, nem egészen pontosak), hogy elég nehéz az eligazodás.

7. A felkészülést négy fontos lépésre lehet osztani, de előtte a GDPR rendeletben szereplő néhány fogalom tisztázása szükséges, amelyekkel most foglalkozunk.

- a **<u>személyes adat</u>** nemcsak az eddig megszokott név, lakcím, személyigazolvány száma, anyja neve, esetleg adóazonosító, TAJ szám, hanem idetartozik minden olyan adat, amellyel adott személy azonosítható (azaz közvetlenül vagy közvetetten létrehozható a kapcsolat az adat és a személy között), pl. telefonszám, e-mailcím, a céges e-mailcím is, ha a személy neve szerepel benne, a számítógép IP címe, süti-azonosító, helymeghatározó adatok, pl. a mobiltelefon helymeghatározó funkciója, a bankszámlaszám, a kamerás megfigyelés adatai, fénykép, biometrikus adatok, személyes adat pl. a NEPTUN kód, vagy pl. egy banki hitelszerződés stb.

- maga a társaság az **ADATKEZELŐ,**

- a társaság weboldalának gondozója **ADATFELDOLGOZÓ**, ugyancsak adatfeldolgozó a társaság könyvelését ellátó könyvelőiroda vagy személy, valamint a webtárhely szolgáltatója.

I. A felkészülés során elsődlegesen **fel kell térképezni, hogy milyen személyes adatokat kezelünk,** ehhez tartozóan azt, hogy milyen célból, mennyi ideig, hol tároljuk azokat, kinek továbbítjuk. Fontos, hogy a papíralapú dokumentumokra is vonatkozik, nemcsak az elektronikus adatokra.

Milyen személyes adatok fordulhatnak elő egy társaságnál?
Mindenek előtt a társasági tagok személyes adatai.

- alapvetően a tagok személyes adatait kezeli egy társaság
  - az adatkezelés célja: a tagok tájékoztatása, a tagsági viszonyból eredő jogok és kötelezettségek gyakorlása, pl. közgyűlési meghívó, tagdíjértesítés stb.
    - itt lehet egy tagnyilvántartás (név, cím, e-mail stb.)
    - tagdíjjal kapcsolatos nyilvántartás, a könyvelőnél a tagdíjak befizetésével kapcsolatos dokumentáció, bankszámlakivonatok stb.

- lehetnek olyan szerződések a társaságnál, amelyekben személyes adatok (is) szerepelnek

- ha vannak munkavállalók, akkor azok bér, tb adatai, TAJ száma, adóazonosítója, bankszámlaszáma, e-mailcíme, lakcíme

- a társasági weboldalon szereplő személyes adatok - itt a regisztrált felhasználók adatai szerepelhetnek például.

Amikor feltérképeztük, hogy milyen személyes adatokat kezelünk és ezt le is írtuk, ezután azt is pontosan rögzíteni kell, hogy az adat jogszabályi kötelezettségen alapul, vagy hozzájáruló nyilatkozaton, ki az, aki hozzáfér az adatokhoz, milyen célból használja, dolgozza fel azokat, hová továbbítja, hol kezeli azokat.

II. Mivel a személyes adatok kezelése elsősorban **személyes hozzájáruláson** alapulhat, fontos, hogy a megfelelő tájékoztatót el kell készíteni, amelyben az érintett személyt tájékoztatjuk arról, hogy milyen személyes adatait, milyen célból, meddig kezeljük, hová továbbítjuk esetleg, tájékoztatjuk őt az adatkezeléssel kapcsolatos jogairól, a közérthető tájékoztatás megadását követően egyértelmű beleegyező nyilatkozatát kérjük.

Ezt **a hozzájáruló nyilatkozatot** minden érintettől, akinek személyes adatait kezeljük, be kell szerezni. A honlapra regisztráltak esetén ez a tájékoztató közlésével és megfelelő felület kialakításával, az érintett által elhelyezendő pipa alkalmazásával megoldható.
Arra ügyelni kell, hogy a web-es felületen ne legyen már előre bepipálva a hozzájárulás, azt a tájékoztató ismeretében az érintett személynek kell megtennie.

Ezt a honlap rendszergazdájának, egyeztetve a társasággal, el kell végeznie. Ezek nyilván többletfeladatok mind az adatkezelőnél, mind az adatfeldolgozónál.
Azon társaságok esetében, ahol az Intellimed Kft. a honlap kezelője, ezen kötelezettség teljesítése érdekében már megtörténtek az első lépések.

A hozzájáruló nyilatkozatban le kell írni, hogy az érintett hozzájárulása az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló, egyértelmű, határozott kinyilvánítása, amellyel félreérthetetlenül beleegyezését adja a személyes adatainak kezeléséhez.

III. adatfeldolgozói szerződések megkötése

a. elsősorban a honlap rendszergazdájával: a net-en találhatók erre vonatkozó adatfeldolgozói szerződés minták, amelyek természetesen nem egy az egyben használhatók, azokat megfelelően személyre kell szabni, a társaság, mint adatkezelő és

a weblap gondozója, mint adatfeldolgozó sajátosságainak és az adatfeldolgozói feladatoknak megfelelően.

b. legalább ilyen fontos, hogy adatfeldolgozói szerződést kell kötni a könyvelővel/könyvelőirodával, hiszen ott is lehetnek személyes adatok, pl. a tagdíjak könyvelése (bankszámla adatok, címek), pl. alkalmazottak bérszámfejtése kapcsán számos személyes adatot kezel, aki ezeket a feladatokat végzi.

c. Az adatkezelő csak olyan adatfeldolgozókat vehet igénybe, akik megfelelő garanciákat nyújtanak a GDPR szerinti, megfelelő technikai és szervezési intézkedések végrehajtására.

Az adatfeldolgozói szerződések minimális tartalmi elemei:

Olyan írásbeli szerződést kell kötni, amelyben - kitérnek arra, hogy

- az adatfeldolgozó a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli
- a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak
- az adatfeldolgozó megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázatok mértékének megfelelő szintű adatbiztonságot garantálja (ideértve az adatvédelmi incidensek esetén alkalmazandó eljárásrendet)

- segíti az adatkezelőt a kötelezettségeinek teljesítésében (például, ha az adatkezelő jogszerűtlen utasítást ad, erre figyelmezteti)
- az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós jog vagy a hazai jog a személyes adatok tárolását írja elő.
  (Pl. a számviteli törvény szabályainak megfelelő őrzési idő.)
- lehetővé teszi és elősegíti az adatkezelő vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

IV. Adatkezelési tájékoztató (korábban adatkezelési szabályzat) elkészítése: e dokumentumnak az a rendeltetése, hogy tájékoztassuk az érintetteket arról, hogy milyen formában történik az adatok kezelése. Az adatkezelési tájékoztató egy kulcsdokumentum, a NAIH minden esetben vizsgálja. Lényeges, hogy minden esetben az

adatfelvétel, adatkezelés megkezdése előtt történjen meg a tájékoztatás. Az adatkezelési tájékoztatót ki kell tenni a honlapra.

Ha feltérképeztük és leírtuk, hogy milyen adatokat, mi célból és meddig kezelünk, elkészítettük az adatkezelési tájékoztatót, bekértük a nyilatkozatokat az érintettektől, megkötöttük az adatfeldolgozókkal a szerződéseket, csak részben tettünk eleget a GDPR rendeletben foglaltaknak, a feltételeit teremtettük meg annak, hogy a GDPR szerint dolgozzunk a személyes adatokkal.

Mindenek előtt fontos, hogy az eddigi gondolkodásunkat alapvetően át kell állítani a GDPR filozófiájának megfelelően. A felkészülést meg kell előzze, hogy kialakuljon az adatvédelmi tudatosság. Nem elegendő csak elkészíteni a szabályzatokat, tájékoztatókat, a napi munka szintjén kell figyelembe venni az adatvédelmi szempontokat, a munkavégzés minden pontján, amikor személyes adatot kezelünk, ügyelni kell az adatok biztonságára, védelmére, az adatkezelési szabályok betartására.

A GDPR szerint a védelem együtt utazik a személyes adattal. Úgy kell tekinteni az egészre, mint pl. a folyamatba épített ellenőrzésre, itt folyamatba épített adatvédelemről beszélhetünk. (Beépített és alapértelmezett adatvédelemről van szó.) Éppen ezért nem elsősorban a jogászoknak és informatikusoknak kell elkészíteni ezt anyagot (bár nyilván, különösen az informatikai területet illetően a szakembereknek fontos szerepe van), mert maga az ADATKEZELŐ ismeri a folyamatokat, az adatkezelő tudja, hogy milyen adatokat, milyen célból, meddig kezel, hová küldi, hogyan tárolja azokat.

A védelemnek ki kell terjednie egyrészt a fizikai védelemre (pl. zárható és ténylegesen zárt), más által nem hozzáférhető helyen tároljuk a személyes adatokat is tartalmazó anyagokat, jogosulatlan személy ne férjen hozzá azokhoz (egy erre „szakosodott takarító" az íróasztalon, monitoron, itt-ott hagyott, különféle feljegyzéseket tartalmazó post it-ekből összerakhatja adott cég üzletmenetére, partnereire vonatkozó fontosabb adatokat. CLEAN DESK POLICY bevezetése fontos. Apróságnak tűnhet, de az információvédelemre különösen igaz, hogy miközben a hegyeket nézzük, kavicsokban botlunk meg.

Fontos, hogy csak azok férjenek hozzá a személyes adatokat is tartalmazó anyagokhoz, akiket erre – munkakörükből következően - feljogosítottak, és akiket az adatvédelemmel kapcsolatos szabályok betartását illetően megfelelő tájékoztatásban részesítettek.

A védelem másik része az informatikai biztonság, a számítógépek jelszavas védelmétől kezdve a jogosulatlan hozzáférés elleni védelmet biztosító intézkedések, az adatállomány helyreállításának lehetőségeit biztosító intézkedések, vírusvédelem, tűzfal, a számítógépek, szerverek fizikai védelme.

8. A GDPR-ban megfogalmazott alapelvek, amelyeket a személyes adatok kezelése során be kell tartani

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

  A jogszerűség azt jelenti, hogy más jogszabályoknak is meg kell felelni. Pl. banktitok vagy reklámtörvény megsértésével az adatvédelmet is megsértjük. A tisztességesség a jog érvényesülésén túli követelmény. Az átláthatóság követelménye azt jelenti, hogy mind az érintett, mind az adatkezelő, mind a hatóság számára átlátható kell legyen az adatkezelés.

- Célhoz kötöttség elve: azt jelenti, hogy a személyes adatok gyűjtése, kezelése csak meghatározott, egyértelmű és jogszerű célból történhet.

- Az adattakarékosság elvének megfelelően a személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk, tehát a legkevesebb adatot kezeljük a célunk eléréséhez, ezért minden esetben meg kell vizsgálni, hogy egyáltalán szükséges-e és mely adatok szükségesek az adatkezelési cél eléréséhez.

- A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük, valamint az adatkezelés szempontjából pontatlan személyes adatok törlésére vagy helyesbítésére haladéktalanul intézkedéseket kell tenni.

- A korlátozott tárolhatóság elvének megfelelően a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. Tehát amellett, hogy a legkevesebb adatot kezeljük a célunk eléréséhez, időben is korlátozni kell az adatok tárolását. Tehát a törlés idejét is meg kell határoznunk. Például egy álláshirdetésre jelentkezők önéletrajzait jogszerűen nem tárolhatjuk azután, hogy a meghirdetett állást betöltötték, hiszen elértük a célt.

  Kivételek a korlátozott tárolhatóság elve alól: közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból.

- A személyes 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 beleértve.

  Pl.: jelszóval védett számítógép, csak a szükséges ideig történő tárolás, IT védelem számítógépeken, csak az férjen hozzá az adatokhoz, akinek munkaköri kötelezettsége az adatokkal való különböző feladatok teljesítése.

- Az adatkezelő felelős a fenti elveknek megfelelő adatkezelési szabályok maradéktalan betartásáért, és képesnek kell lennie e megfelelés igazolására.

Ez azt is jelenti, hogy nem a hatóságnak kell bizonyítani azt, hogy az adatkezelő jogellenesen kezeli az adatot és felel a kárért, hanem az adatkezelőnek kell kimenteni magát, hogy megtette a megfelelő intézkedést.

Ezt úgy lehet megoldani, hogy naplózni, jegyzőkönyvezni, vagy bármi módon nyilvántartani kell az adatkezeléssel kapcsolatos történéseket, hogy bármikor rendelkezésre álljon adott személyes adattal kapcsolatos információ.

- Az érintettek jogai - a GDPR rendelet 15-22. cikke tartalmazza:

    - Az érintett hozzáférést kaphat adataihoz. Ha kéri az ügyfél, hogy milyen adatokat kezelnek róla, azt ki kell elégíteni. Alapvetően az egyén rendelkezik az adataival, joga van követni, hogy milyen formában tárolnak, kezelnek adatokat róla.

    - A helyesbítés joga azt jelenti, hogy a később változó vagy pontatlan adatokat módosítani kell. Ezen jog gyakorlása nem hátráltatható.

    - Törlés: Az adatkezelő köteles törölni, ha már nincs szükség az adatokra. Ezt az adatkezelőnek kell észlelnie. Minden nyilvántartást, ami időn túli, törölni kell. Törölni kell akkor is, ha az ügyfél visszavonja a hozzájárulását. Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy késedelem nélkül eleget tegyen ennek, amennyiben az jogszabályon alapuló kötelező adatkezelés miatt nem kizárt.

      Fontos kivétel, hogy a számviteli bizonylatokat a számviteli törvény előírásai alapján 8 évig meg kell őrizni, a keletkezés éve nem számít bele a 8 évbe. Ezért nem lehet törölni az adatokat még akkor sem, ha az érintett ezt kéri.

      Jelenleg még nem tisztázott, hogy csak törvények vagy alacsonyabb szintű jogszabályok is felülírhatják-e a GDPR ezen rendelkezését. Van olyan felfogás, hogy amennyiben jogszabály rendeli el az adatkezelést, nincs szükség a célhoz kötöttség vizsgálatára. A NAIH a törvényt tekinti jogalapnak, a rendeletet nem.

      A törléshez való jogot korlátozza ezen felül, ha közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzendő feladatot hajt végre, ha népegészségügy területén megvalósuló közérdek áll fenn, vagy közérdekű archiválás céljából, tudományos, történelmi kutatási, statisztikai célból, amennyiben a törléshez való jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné az adatkezelést. Ugyancsak korlátozza a törléshez való jogot a jogi igények előterjesztése, érvényesítése vagy védelme.

Valószínűleg ilyen esetek nagyon ritkán fordulhatnak elő egy-egy társaság adatkezelésében.

Hasznos tanácsként hangzott el a kétnapos előadáson, hogy "figyeljük az adatvédelmi testület büntetés-kiszabási gyakorlatát, nézzük meg, hogy szervezetünknél kiszabhattak volna-e ilyet, és foltozzuk be a lyukat."

- Adathordozhatósághoz való jog - új elem

Az érintett jogosult az általa az adatkezelő rendelkezésére bocsátott adatait megkapni, tagolt, széles körben használt, géppel olvasható formátumban, jogosult az adatait más adatkezelőhöz továbbítani, kérheti az adatok közvetlen továbbítását a másik adatkezelőhöz, ha ez technikailag megoldható. Kivétel a közérdekű vagy közhatalmi jog gyakorlása céljából végzett adatkezelés.
Az adathordozhatósághoz való jog akkor gyakorolható, ha automatizált módon történik az adatkezelés és az adatkezelő az érintett hozzájárulása vagy szerződéses jogalap alapján kezeli az adatokat.

Az adathordozást követően a régi adatkezelő köteles törölni az adatokat, ha az érintett úgy rendelkezik, hogy most már csak az új adatkezelő szolgáltatásait kívánja használni. ha az érintett nem rendelkezett, akkor az eredeti feltételek mellett tárolhatók az adatok a korábbi adatkezelő által.
Az adatkezelési tájékoztatókban fel kell tüntetni az adathordozhatósághoz való jogot, és annak gyakorlásának módját. Fő szabály szerint ez ingyenes.

- Az adatkezelés jogalapja:
  - a személyes adatkezelés akkor jogszerű, amennyiben a következők közül legalább egy teljesül:
    - a legalapvetőbb az érintett hozzájárulása személyes adatainak kezeléséhez, a korábban elmondottak szerint, megfelelő tájékoztatáson alapuló, önkéntes, egyértelmű, konkrét és határozott nyilatkozatra van szükség
    - az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél. Ez esetben nem kell semmiféle záradék, hogy a fél beleegyezik adatai kezeléséhez, mert itt a szerződés önmagában alapozza meg ezt. Szerződések esetében nem illeti meg az adatalanyt

a törléshez, tiltakozáshoz való jog, de megilleti az adathordozhatóság joga

- az adatkezelés jogalapja lehet, ha az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges (pl. az előzőekben említett, számviteli törvénynek megfelelő megőrzési idő)

- az adatkezelés az érintett létfontosságú érdekinek védelme miatt szükséges

- az adatkezelés közérdekű feladat végrehajtásához szükséges

Az adatkezelési tájékoztatóban néhány alapfogalmat - amely releváns lehet a társaság adatkezelésében - célszerű meghatározni, ezek a GDPR rendelet 4. cikkében találhatók.

9. Ugyancsak célszerű meghatározni az adatvédelmi incidens fogalmát és az adatvédelmi incidens esetén követendő eljárást, hiszen ilyesmi sajnos bármikor előfordulhat.

   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.

   Adatvédelmi incidens például egy céges telefon elvesztése, vagy például egy pendrive eltűnése, amelyen titkosítatlanul személyes adatok találhatók, és nincs jelentősége annak, hogy az egyébként nem bizonyított, hogy illetéktelen személy hozzáfért személyes adatokhoz. Egyetlen személy egyetlen személyes adatát érintő incidens is adatvédelmi incidensnek tekint**het**ő.

   Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, mint például
   - személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását,
   - a személyazonosság-lopást vagy személyazonossággal való visszaélést,
   - pénzügyi veszteséget,
   - a jó hírnév sérelmét,
   - a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését.

   Főszabály szerint az adatvédelmi incidenst indokolatlan késedelem nélkül, de legkésőbb a tudomásszerzést követő 72 órán belül be kell jelenteni a Hatóságnak.

Tudomásszerzésnek az tekinthető, amikor az adatkezelő ésszerű mértékű bizonyossággal rendelkezik arról, hogy olyan biztonsági esemény történt, amely személyes adatokkal kapcsolatos jogellenes műveletekhez vezethet. Nem kell bejelenteni a Hatóság részére, ha valószínűsíthetően nem jár kockázattal az érintettek számára. A hangsúly azon van, hogy az adatkezelőnek azonnali vizsgálatot kell kezdeményeznie annak megállapítására, hogy történt-e adatvédelmi incidens, és ha igen, milyen intézkedések szükségesek, illetve szükséges-e bejelentést tenni az adatvédelmi incidensről. Az incidenst az adatalanyok felé is közzé kell tenni, ha az incidens valószínűsíthetően magas kockázattal jár az érintett(ek) számára. Ezt is az adatkezelőnek kell mérlegelnie.

Függetlenül attól, hogy a Hatóság számára bejelentésre kerül vagy sem az adatvédelmi incidens, azokról kivétel nélkül nyilvántartást kell vezetni, abban fel kell tüntetni az incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. A nyilvántartás célja az, hogy lehetővé teszi a Hatóság számára, hogy ellenőrizze az incidensek bejelentésével összefüggő kötelezettségeknek való megfelelést.

Az adatvédelmi incidens bejelentésével összefüggő kötelezettségek megszegése esetén, mint például a késedelmes bejelentés, a bírság összege 10 millió euróig terjedhet, anyagi jogszabály megsértése (pl. nem megfelelő adatbiztonsági intézkedések) esetén 20 millió euróig terjedhet.

Az adatvédelmi incidens bejelentése a NAIH részére történik, az adatvédelmi tájékoztatóban a NAIH elérhetőségeit is rögzíteni kell.

10. Adatvédelmi tájékoztatót a weboldalra ki kell tenni.

Legfontosabb tartalmi elemei:

- szerepelnie kell benne az adatkezelő (a társaság) adatainak, elérhetőségének, esetleg az adatkezelésre felhatalmazott személy legalább e-mailes elérhetőségének.

- célszerű feltüntetni azokat az alapelveket, amelyek figyelembevételével történik az adatkezelés

- azon értelmező rendelkezések leírása, amelyek a társasági adatkezelés szempontjából relevánsak

- szerepeljen az adatkezelés jogalapja (hozzájáruló nyilatkozat, szerződés, adatkezelőre vonatkozó jogi kötelezettség /konkrét felsorolás/)

- szerepeljen a tájékoztatóban, hogy milyen személyes adatokat kezelnek, mennyi ideig, milyen célból kezelik azokat ,

- ha a honlapon is kezelnek személyes adatokat, akkor ezek felsorolása, célja

(konkrétan: pl. hírlevél küldés)

- fel kell sorolni az érintettek (adatalanyok) konkrétan az egyesületi tagok jogait az adatkezeléssel kapcsolatban. Az érintettek jogairól a korábbiakban már szó esett. Fel kell hívni a figyelmet arra, hogy amennyiben bizonyos adatainak törlését kéri az érintett, annak milyen következményei lesznek, valamint azt, hogy ahol jogi kötelezettség írja elő az adatok megőrzését, azok törlésére vonatkozó kérelem nem teljesíthető

- Fontos, hogy az érintett adataival kapcsolatos bármilyen kérését mielőbb, de max. 1 hónapon belül teljesíteni kell, ill. reagálni kell arra, ha kérése nem teljesíthető, és annak okait is részletezni kell. (az infotörvény erre 25 napot adott.)Az adatvédelmi tájékoztatóban legyen benne ez a határidő (mert ilyen hiányosság miatt már bírságolt korábban a NAIH (az infotörvény szabályai alapján).

- meg kell szövegezni egy hozzájáruló nyilatkozatot, amelynek általános, állandó része felhasználható az eltérő adatkezelési célok és más változó adatoknál pedig behelyettesítjük a behelyettesítendőket.

- tájékoztatni kell az érintetteket a jogorvoslati lehetőségekről

  A jogokkal kapcsolatos eljárási szabályokat is be kell írni az adatkezelési tájékoztatóba. Ha valakinek kifogása van, akkor elsősorban a társaságnál megbízott adatvédelmi felelőst keresse meg, és ha itt nem vezet eredményre az ügye, inkább a bírósághoz fordulás előnyeit kell az ügyfél figyelmébe ajánlani, ami a lakóhelye szerinti illetékességű bíróság, illetékmentes és soron kívüli. Az adatvédelmi hatóság nemcsak a bírság miatt veszélyes, hanem a teljes adatkezelésünk törlését is elrendelheti. A bíróság ilyet nem tehet, mert ő csak a panaszos adatainak törlését rendelheti el.

- Az adatvédelmi tájékoztató végén célszerű feltüntetni, hogy annak tartalmát az adatkezelő folyamatosan felülvizsgálja és a jogszabályi változások figyelembevételével módosítja, kiegészíti. Ez azért fontos, mert a jelenlegi hazai szabályozás még nincs meg, holott az EU-s rendelet számtalan helyen hivatkozik arra, hogy az egyes tagországi belső szabályozás további részletszabályokat határozhat meg. Az infotörvénynek már készült egy módosító javaslata, vélhetően az új országgyűlés elé kerül hamarosan, és talán az ágazati szabályozás is megszületik, hiszen az egészségügyben keletkező személyes adatok speciális szabályozást igényelnek, amelyet ugyan tartalmaz az EU-s rendelet, de nyilvánvalóan ennél sokkal részletesebb belső szabályozásra van szükség.

- Fontos, hogy az adatvédelmi tájékoztató az adatalanyok nyelvén készüljön, fogyasztóbarát, testreszabott, neki szóló legyen az információ.