FELKÉSZÜLÉSI ÚTMUTATÓ AZ EU ADATVÉDELMI RENDELETNEK VALÓ MEGFELELŐSÉGHEZ

Környei Mátyás

2017

arsboni

TARTALOMJEGYZÉK:

KÖRNYEI MÁTYÁS BEMUTATÁSA

Ügyvédjelölt, a Budapesti Ügyvédi Kamara Ügyvédjelölti Tagozatának Elnökségi Tagja. Társasági és kereskedelmi jogban, banki, tőkepiaci és finanszírozási jogban, IT/IP és adatvédelmi területen valamint vitarendezési ügyekben szerzett tapasztalatokat. Elhivatott a modern technológiák vizsgálata és az üzleti, gazdasági megközelítés alkalmazása iránt.

FELKÉSZÜLÉSI ÚTMUTATÓ AZ EU ADATVÉDELMI RENDELETNEK VALÓ MEGFELELŐSÉGHEZ

Tavaly májusban lépett hatályba az új Uniós Általános Adatvédelmi Rendelet (GDPR), amely jelentős mértékben átalakítja a személyes adatok kezelésére vonatkozó Uniós szabályozást. A természetes személyeknek személyes adataikkal való rendelkezésük tekintetében jóval erősebb jogosultságaik lesznek, a vállalatoknak az eddigieknél jóval átláthatóbban és átfogóbban szabályozott módon kell az adatkezelést végezniük, míg az Uniós adatvédelem valamelyest megújuló hatósági kereteket kap, amellyel együtt némileg megváltoznak a hatósággal történő kapcsolattartás módjai.

A vállalatoknak kicsivel több mint fél év áll a rendelkezésükre a GDPR szabályainak kötelező alkalmazásáig, így adatkezelési gyakorlatuknak a GDPR-nak megfelelő átalakításáig. Ahogy azt majd a jelen összefoglalóban is láthatjuk, a GDPR-nak való megfelelés a vállalkozások kiemelt feladata lesz az elkövetkezendő években, hiszen nem csupán az adatvédelmi standardok szigorodása, de pl.: az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-ig vagy EUR 20 millió összegig terjedően] kiszabható bírság összeg okán is.

E felkészülés keretében, jelen összefoglaló bemutatja az adatvédelem eddigi rendszeréhez képest a legfontosabb változásokat, illetve az adatvédelem új standardjait, továbbá – ahol szükséges - meghatározza azokat a legfontosabb felkészülési feladatokat, amelyek elvégzése mindenképpen szükséges lesz a GDPR szabályainak való megfelelés érdekében.

IRÁNYELV HELYETT RENDELET

Idáig, és a GDPR szabályainak alkalmazásának időpontjáig az adatvédelem szabályozása Uniós szinten a 95/46/EK irányelv keretei között valósult meg. Az irányelv meghatározza az adatvédelem minden tagállamban érvényesülést követelő minimum standardjait, de nem határozza meg az azok érvényesülését garantáló konkrét szabályokat, jelenleg tehát a tagállami szabályozások feladata az Uniós adatvédelmi céloknak megfelelő szabályozás kialakítása. Magyarországon ezt a szerepet a 2011. évi CXII. tv. (**„Info tv.”**) tölti be.

Azzal, hogy a GDPR hatályon kívül helyezi az irányelvet és rendeleti formában került megalkotásra, az abban foglalt szabályok közvetlenül alkalmazandóvá váltak mindenki számára és a rendeleti jelleg okán, a GDPR rendelkezési elsőbbséget éveznek a tagállami szabályokkal, így hazánkban az Info tv. szabályaival szemben is. 2018. május 25-től tehát, az adatkezelésre vonatkozó szabályoknak való megfelelőség során már nem az Info tv. rendelkezésiből, hanem a GDPR szabályaiból kell kiindulnunk. Ebből a szempontból lényeges még, hogy mind a 28 tagállam területén ugyanazok a szabályok alkalmazandóak, jóllehet a GDPR több helyen is megnyitja az utat a nemzeti szabályozás előtt (pl.: speciális adatkezelési helyzetek, kiskorú hozzájárulásának feltételei stb.)

A rendeleti jellegből adódó felkészülési feladatok:

Jogalkotói feladat: Mivel az adatvédelem és a személyes adatok kezelésének szabályai rendeleti formát kaptak, és az Uniós jog értelmében egy tagállam nem alkothat olyan kérdésre vonatkozóan jogot, melyet az EU rendeleti szinten szabályozott, az egyes tagállamoknak (így Magyarországnak is) hatályon kívül kell helyeznie azokat a hazai szabályokat, melyek a GDPR keretein belül már szabályozást nyertek. Ezen felül, a GDPR keretében adott felhatalmazások alapján jogalkotási kötelezettsége is van a jogalkotónak.

Jogalkalmazói feladat: Minden vállalatnak, vállalkozásnak, amely természetes személyek személyes adatait kezeli, valamint a hatóságoknak is részletesen keresztül kell menniük a GDPR szövegén, meg kell érteniük annak logikáját és működését, továbbá az adatkezelőknek telje-

sen felül kell vizsgálniuk az adatkezelésüket a GDPR szempontjából és biztosítaniuk kell az abban foglaltaknak való megfelelést.

A TERÜLETI HATÁLY KITERJESZTÉSE

A GDPR szabályait kell majd alkalmaznia minden az EU-ban tevékenységi hellyel rendelkező adatkezelőnek vagy adatfeldolgozónak függetlenül attól, hogy az adatkezelés az Unió területén történik-e vagy sem. E szabály alapján bárki, aki az EU-ban valamilyen tevékenységet végez (és megállapítható, hogy tevékenységi hellyel rendelkezik), és e tevékenységével összefüggésben személyes adatokat kezel a GDPR szabályait kell majd alkalmaznia.

A GDPR szabályai lesznek alkalmazandóak továbbá az EU-ban tartózkodó érintettek személyes adatainak kezelésére is, amennyiben az adatkezelési tevékenységek áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért, vagy az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve, hogy az Unió területén belül tanúsított viselkedésükről van szó.

A KITERJESZTETT TERÜLETI HATÁLYBÓL ADÓDÓ FELKÉSZÜLÉSI FELADATOK:

a) A vállalkozásoknak meg kell bizonyosodniuk arról, hogy rendelkeznek-e tevékenységi hellyel az EU-ban vagy sem;
b) Ha az adott vállalkozás megállapítja, hogy az EU-n belül tevékenységi hellyel rendelkezik, akkor meg kell állapítania, hogy ahhoz kapcsolódó tevékenységével összefüggésben kezel-e személyes adatokat;
c) Amennyiben az a) és b) pontok pozitív eredményt mutatnak, a vállalkozásnak alkalmaznia kell a GDPR szabályait.

1) A vállalkozásoknak meg kell állapítaniuk, hogy nyújtanak-e az EU-ban tartózkodó érintettek számára valamilyen szolgáltatást vagy értékesítenek-e árut a részükre;
2) A vállalkozásoknak meg kell állapítaniuk, hogy ezzel kapcsolatban kezelnek-e személyes adatokat;
3) Amennyiben az 1) és 2) pontok pozitív eredményt mutatnak, a vállalkozásnak alkalmaznia kell a GDPR szabályait.

I) A vállalkozásoknak meg kell állapítaniuk, hogy végeznek-e olyan személyes adatkezelést, amely az érintettek viselkedésének megfigyeléséhez kapcsolódik;
II) A vállalkozásoknak meg kell állapítaniuk, hogy a megfigyelt érintetti viselkedés az Unión belül tanúsított viselkedés-e;
III) Amennyiben az I) és II) pontok pozitív eredményt mutatnak, a vállalkozásnak alkalmaznia kell a GDPR szabályait.

AZ ADATVÉDELEMBEN FELBUKKANÓ ÚJ FOGALMAK

A GDPR a személyes adatok körében új típusú adatfajtákat definiál. Ezek a helymeghatározó adat, online azonosító (pl.: IP cím), genetikai adat, biometrikus adat. A genetikai és a biometrikus adat egyben különleges adatnak minősül és így szigorúbb adatkezelési szabályok vonatkoznak rájuk.

A modern adatkezelési módszerek alkalmazásának lehetőségét teremtik meg a profilalkotás és az álnevesítés fogalmai.

- Profilalkotás a személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.

- Az álnevesítés a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.
  A GDPR alkalmazásában kiemelkedően fontos lesz az adatkezelő tevékenysége központja helyének meghatározása (pl.: one stop shop] [ld. később]), ennek megfelelően a Rendelet meghatározza a tevékenységi központ fogalmát.

Tevékenységi központ:

a) olyan adatkezelő esetében, amely több EU országban is működik, a tevékenységi központja az a hely, ahol az EU-n belüli központi ügyvitelének a helye található. Abban az esetben azonban, ha az adatkezelésre vonatkozó döntések meghozatala és végrehajtása az előbbitől eltérő helyen történik, a tevékenységi központnak a döntéshozatal helyét kell tekinteni.

vagy

b) az egynél több tagállamban tevékenységi hellyel rendelkező adatfeldolgozó esetében az EU-n belüli központi ügyvitelének helye, vagy olyan adatfeldolgozó esetében, amely nem rendelkezik központi ügyviteli hellyel az EU-ban, az a hely, ahol az adatfeldolgozó tevékenységi helyén folytatott tevékenységekkel összefüggésben végzett fő adatkezelési tevékenységek zajlanak, amennyiben az adatfeldolgozóra a GDPR szerint meghatározott kötelezettségek vonatkoznak.

A megjelenő új fogalmakkal kapcsolatos felkészülési feladatok:

a) A vállalkozásoknak meg kell állapítaniuk, hogy kezelnek a személyes adatok körébe újonnan bevont adatokat (pl.: IP cím) és amennyiben igen, úgy alkalmazniuk kell a GDPR szabályait;
b) vállalkozásoknak meg kell állapítaniuk, hogy végeznek-e profilalkotásnak, automatizált döntéshozásnak vagy álnevesítésnek megfelelő tevékenységet és amennyiben igen, úgy alkalmazniuk kell a GDPR vonatkozó szabályait;
c) A vállalkozásoknak (adatvédelmi, adatkezelési stratégiai célból is) meg kell határozniuk a GDPR szerinti tevékenységi központjuk helyét.

ALAPELVEK ÚJ KÖNTÖSBEN

A GDPR újrafogalmazza az adatkezelésre vonatkozó legfontosabb szabályokat, melyek a:

jogszerűség, tisztességes eljárás és átláthatóság
célhoz kötöttség
adattakarékosság
pontosság
korlátozott tárolhatóság
integritás és bizalmas jelleg.

Új alapelv, hogy az adatkezelőnek nem csak biztosítani kell az alapelvek megtartását, de képesnek kell lennie a megfelelés igazolására is (elszámoltathatóság). Ennek jelentős szerepe lesz az újonnan bevezetett tanúsítási rendszer vonatkozásában.

Az újragondolt alapelvekkel kapcsolatos felkészülési feladatok:

a) A vállalkozásoknak meg kell vizsgálniuk az adatkezelési gyakorlatukat és azt megfelelő tervezést és előkészítést követően az újrafogalmazott alapelveknek is megfelelő módon kell majd módosítaniuk;
b) Az elszámoltathatóság alapelvének való megfelelés érdekében a vállalkozásoknak megfelelő adatvédelmi és adatkezelési dokumentációt kell készíteniük. Ez jelenti a belső szabályzatok és iránymutatások, az adatkezelési rendszerek megalkotását és írásba foglalását.

A HOZZÁJÁRULÁS

Hozzájáruláson alapuló adatkezelés esetében, az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult. Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni. Az érintett hozzájárulását tartalmazó ilyen nyilatkozat bármely olyan része, amely sérti a GDPR rendelkezéseit, kötelező erővel nem bír.
A hozzájárulás bármikor visszavonható, mégpedig ezt ugyanolyan egyszerű módon kell biztosítani, mint a hozzájárulás megadását (pl.: ha checkbox-al ad hozzájárulást az érintett, akkor hasonló egy kattintásos módszerrel kell lehetővé tenni a visszavonást is). A hozzájárulás önkéntessége körében vizsgálni kell azt is, hogy a szerződés teljesítésének feltételéül határoztak-e meg olyan adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.

A GDPR fontos újítása, hogy kitér a gyermekek által adható hozzájárulásra is. Ha az adatkezelés közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatásokkal kapcsolatos akkor a 16. életévét betöltött gyermek hozzájárulhat a személyes adatainak kezeléséhez. Minden egyéb esetben az adatkezelés akkor jogszerű, ha a hozzájárulást a szülői felügyeletet gyakorló szülő adta meg, vagy ő engedélyezte.

A tagállamok, a fenti célokból jogszabályban ennél alacsonyabb, de a 13. életévnél nem alacsonyabb életkort is megállapíthatnak. Az adatkezelőnek ésszerű erőfeszítéseket kell tennie annak érdekében, hogy ellenőrizze, hogy a hozzájárulást a gyermek feletti szülői felügyeleti jog gyakorlója adta meg, illetve engedélyezte. Ezek a rendelkezések azonban nem érintik a tagállami szerződési jogot, így a szerződések érvényességének megtámadása nem alapozható majd a GDPR-nak nem megfelelő hozzájáruláson. A hozzájárulás szabályai csupán az adatkezelés jogszerűségére vonatkoznak.

A különleges adatok kezelése általános szabály szerint tilos, kivéve a GDPR-ban felsorolt okok esetén. Ilyen ok többek között az érintett kifejezett hozzájárulása egy vagy több konkrét célból történő adatkezeléshez.

A hozzájárulással kapcsolatos felkészülési feladatok:

Jogalkotói feladatok: A jogalkotónak meg kell határoznia, hogy el kíván-e a térni a GDPR-nak, a gyermekek hozzájárulásával kapcsolatban megállapított korhatártól és amennyiben igen, úgy hány évnél húzza meg a határt, amikor a gyermek még hozzájárulhat személyes adatainak a kezeléséhez. Ezt a jogalkotási folyamatot érdemes figyelnie az olyan vállalkozásoknak is, amelyek kiskorúak számára nyújtott szolgáltatások keretében kezelik azok adatait.

Jogalkalmazói feladatok: A vállalkozásoknak felül kell vizsgálniuk az eddigi hozzájárulás-kérési gyakorlatukat és ki kell alakítaniuk egy olyan jogi és technológiai rendszert, amely biztosítja, hogy:

a) A hozzájárulás megadását a vállalkozás később is igazolni tudja majd;

b) Az érintettek ugyanolyan egyszerűen visszavonhassák a hozzájárulásukat, mint ahogy azt megadták.

1) A vállalkozásoknak meg kell vizsgálniuk, hogy nem kérnek-e be olyan adatot, amely nem szükséges a szerződés teljesítéséhez;

2) A vállalkozásoknak ki kell alakítaniuk majd olyan mechanizmusokat, amelyek keretében ellenőrzik, hogy a(z önálló hozzájárulás adásra nem jogosult) gyermek adatainak kezeléséhez történő hozzájárulást a szülői felügyeletet gyakorló szülő adta meg, vagy ő engedélyezte.

EROSEBB ÉRINTETTI JOGOSULTSÁGOK

Átlátható tájékoztatás és kommunikáció

Az adatkezelőknek, az adatkezelés megkezdése előtt, illetve az érintett kérelmére, tömör, átlátható, érthető, könnyen hozzáférhető módon kell az érintetteket tájékoztatnia az adatkezelésről és az érintetti jogok gyakorlásáról. Ez a tájékoztatás, valamint az érintett hozzáférési jogán alapuló kérelme szerinti tájékoztatás az érintett kérésére, szóban is megadható, amennyiben más módon igazolták az érintett személyazonosságát.

Az előzetes tájékoztatást pl. szabványosított ikonokkal is ki lehet egészíteni annak érdekében, hogy a tervezett adatkezelésről az érintett jól látható, könnyen érthető és jól olvasható formában kapjon általános tájékoztatást. Ezekre az ikonokra vonatkozóan az Európai Unió Bizottsága fogja megalkotni a vonatkozó szabályozást.

Az előzetes tájékoztatási kötelezettség kibővül, így többek között ezentúl a következő információkat is közölni kell az érintettel:

- ha van ilyen, az adatvédelmi tisztviselő elérhetőségeiről,
- az EU Bizottságának megfelelőségi határozata (ld. később)

- az automatizált döntéshozatalról, ideértve a profilalkotást is.

Az utóbbi esetben érthető módon tájékoztatni kell az érintettet, legalább az alkalmazott logikáról és az arra vonatkozó információkról, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

A felejtéshez való jog

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 a GDPR-ban meghatározott indokok valamelyike fennáll. Ha az adatkezelő nyilvánosságra hozta, vagy továbbította a személyes adatot, és azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével meg kell tennie minden ésszerűen elvárható lépést – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

Az adathordozhatóság joga

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 hozzájáruláson vagy szerződésen alapul; és
b) az adatkezelés automatizált módon történik.

Az adatok hordozhatóságához való jog során az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását. Az adathordozhatósághoz való jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges.

Az érintetti jogok gyakorlásának korlátai

Bizonyos érintetti jogok nem gyakorolhatóak, ha az adatkezelő – abból az okból, hogy azok az adatkezelési célok, amelyek alapján az adatkezelés történik, nem vagy már nem teszik szükségessé az érintettek adatkezelő általi azonosítását - bizonyítani tudja, hogy nincs abban a helyzetben, hogy azonosítsa az érintettet. Amennyiben az érintett kérelme egyértelműen megalapozatlan vagy túlzó (ilyen a különösen ismétlődő jelleg is), az adatkezelő a kérelem teljesítéséért díjat számíthat fel, vagy megtagadhatja az intézkedést. Ennek bizonyítása azonban az adatkezelőt terheli.

Az erősebb érintetti jogosultsággal kapcsolatos felkészülési feladatok

a) A vállalkozásoknak el kell készíteniük a GDPR rendelkezéseinek megfelelő adatkezelési tájékoztatójukat;
b) Létre kell hozniuk olyan mechanizmusokat, amelyek szerint költséghatékony módon lesznek képesek eleget tenni a felejtés jogával kapcsolatos érintetti igényeknek;
c) Létre kell hozniuk olyan mechanizmusokat, amelyek szerint költséghatékony módon lesznek képesek eleget tenni az adathordozhatósággal kapcsolatos érintetti igényeknek;
d) Fel kell készülniük az egyéb érintetti jogosultságok gyakorlásából eredő kötelezettségek teljesítésére (pl.: tájékoztatáshoz való jog szerinti tájékoztatás, adatkezeléssel szembeni tiltakozással kapcsolatos feladatok stb.).

AZ AUTOMATIZÁLT DÖNTÉSHOZATAL SZABÁLYOZÁSA

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, kivéve, ha a döntés:
a) az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges,
b) meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít, vagy
c) az érintett kifejezett hozzájárulásán alapul.

Az a) és c) eseteiben az érintettnek joga van, hogy az adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be. Az automatizált döntéshozatal és a profilalkotás főszabály szerint nem alapulhat a különleges adatokon.

Az automatizált döntéshozatallal kapcsolatos felkészülési feladatok:

a) Az automatizált döntéshozatalt (pl.: profilalkotást) is alkalmazó vállalkozásoknak ki kell alakítaniuk azokat a gyakorlatokat, amelyek során biztosítják, hogy az érintettek tiltakozhassanak az automatizált adatkezelésen alapuló döntések rájuk vonatkozó meghozatala ellen;
b) Meg kell adniuk az érintetteknek az automatizált döntéshozatalról szóló előzetes tájékoztatást;
c) Továbbá, a vállalkozásoknak, a fenti döntéshozatalra vonatkozóan biztosítaniuk kell majd az emberi beavatkozás lehetőségét.

AZ ADATKEZELŐK KÖTELEZETTSÉGEI

Privacy by Design & Privacy by Default

A GDPR alapján az adatkezelőnek az adatkezelés módjának meghatározásakor és az adatkezelés során olyan technikai és szervezési intézkedéseket kell alkalmaznia, amelyek biztosítják a GDPR-ban foglalt alapelveknek, szabályoknak való megfelelést és az érintetti jogok védelmét, továbbá azt, hogy az adatkezelő alapértelmezés szerint kizárólag azokat az adatokat kezelje, amelyek az adatkezelési cél érdekében feltétlenül szükségesek. E célok elérése érdekében, be kell építeni a szükséges garanciákat az adatkezelés folyamataiba.

A Privacy by Default kötelezettség azt jelenti, hogy az adatkezelőnek mindig a legmagasabb fokú adatvédelmi beállításokat kell alapértelmezettként nyújtania. Ezeket az érintett természetesen enyhítheti, de az lapértelmezett beállításnak a legszigorúbb adatvédelmi szintnek kell megfelelnie.

A fenti két kötelezettség különösen az új szolgáltatások fejlesztése és bevezetése során lesz fontos, amikor is a fejlesztőknek és a vállalkozásoknak a fenitek szerint kell tervezniük és bevezetniük az adatkezeléssel is járó szolgáltatást.

Unión kívüli vállalatok adatvédelmi képviselője.

Azon adatkezelőknek, akik nem rendelkeznek tevékenységi hellyel az Unióban, ki kell jelölniük egy képviselőt. A képviselőnek tevékenységi hellyel kell rendelkeznie az egyik olyan tagállamban, ahol azon érintettek tartózkodnak, akiknek személyes adatait áruknak vagy szolgáltatásoknak a részükre történő nyújtása során kezelik vagy akiknek a magatartását megfigyelik. Az adatkezelő vagy az adatfeldolgozó által a képviselő számára adott megbízásnak ki kell terjednie arra, hogy az adatkezeléssel összefüggő minden ügyben, az e rendeletnek való megfelelés biztosítása érdekében – különösen a felügyeleti hatóságok és az érintettek megkeresésére – az adatkezelő vagy az adatfeldolgozó helyett vagy mellett a képviselő járjon el. Nem szükséges képviselőt kijelölni, ha az adatkezelés alkalmi jellegű és nem vonatkozik különleges adatokra, illetve, ha azt közhatalmi vagy egyéb közfeladat ellátó szerv végzi.

Az új adatkezelői kötelezettségekkel kapcsolatos felkészülési feladatok:

a) A vállalkozásoknak felül kell vizsgálniuk az adatkezelési gyakorlatukat és ha szükséges azt oly módon kell módosítaniuk, hogy megfeleljenek a Privacy by Design & Privacy by Default elvéből fakadó kötelezettségeknek;

b) Ennek során a vállalkozásoknak szorosan együtt kell működniük az adatkezelésben érintett szervezeti döntéshozókkal, valamint az IT fejlesztőkkel;

c) Az Unión kívüli vállalatoknak ki kell nevezniük az adatvédelmi képviselőt.

AZ ADATFELDOLGOZÓK KÖTELEZETTSÉGEI

Az egyik legfontosabb változás, hogy a GDPR bevezeti az adatfeldolgozóknak az érintettekkel szembeni kártérítési felelősségét, illetve, mivel a GDPR már konkrét kötelezettségeket állapít meg az adatfeldolgozók részére, így ők is bírságolhatóvá válnak a Rendeletben foglalt szabályok be nem tartásáért.

Az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés a GDPR követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására. A GDPR meghatározza az adatkezelő és az adatfeldolgozó közötti szerződés egyes tartalmi elemeit, továbbá felhatalmazást ad a Bizottságnak és a felügyeleti hatóságoknak arra, hogy az adatkezelők és adatfeldolgozók közötti szerződésekre általános szerződési feltételeket határozzon meg. Az adatfeldolgozási szerződéseket írásba kell foglalni.

A 250 főnél nem kevesebb személyt foglalkoztató adatkezelőnek és adatfeldolgozóknak vagy a képviselőiknek, írásban adatkezelési nyilvántartást kell vezetnie, amelyet a felügyeleti hatóság kérésére rendelkezésre kell bocsátani. A nyilvántartás tartalmát a GDPR határozza meg. 250 főnél kevesebb személyt foglalkoztató vállalkozásoknak is nyilvántartást kell vezetniük, ha adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár, ha az adatkezelés nem alkalmi jellegű, vagy ha az adatkezelés különleges vagy bűnügyi adatokat is érint.

Az adatfeldolgozói kötelezettségekkel kapcsolatos felkészülési feladatok:

a) A vállalkozásoknak értékelniük kell, hogy a megbízott adatfeldolgozó nyújtja-e a GDPR-nak megfelelő garanciákat;
b) A vállalkozásoknak felül kell vizsgálniuk az adatfeldolgozásra adott megbízási szerződéseiket a fent említett felelősségi szituációk változására tekintettel, valamint abból a szempontból, hogy azok megfelelnek a GDPR követelményeinek;
c) A vállalkozásoknak meg kell alkotniuk és vezetniük kell majd az adatkezelési nyilvántartást.

ADATVÉDELMI INCIDENS

A GDPR bevezeti az adatvédelmi incidens fogalmát és meghatározza azt a protokollt, amelyet egy ilyen helyzetben követnie kell az adatkezelőnek. Az 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.

Az adatvédelmi incidenst az adatkezelőnek indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, be kell jelentenie az illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Az adatfeldolgozónak az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül be kell jelentenie az adatkezelőnek. Az adatkezelőnek nyilvántartást kell vezetnie az adatvédelmi incidensekről, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelőnek indokolatlan késedelem nélkül tájékoztatnia kell az érintettet az adatvédelmi incidensről. Nem kell az érintetteket tájékoztatni, ha az adatkezelő megfelelő védelmi intézkedéseket tett, amelyek biztosítják, hogy az előbb említett magas kockázat nem valósul meg, vagy a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Utóbbi esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását. Ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja az előbb felsorolt feltételek valamelyikének teljesülését.

Az adatvédelmi incidens szabályozásával kapcsolatos felkészülési feladatok:

a) A vállalkozásoknak ki kell alakítaniuk a szervezeten belül azt a mechanizmust, amely szerint az adatvédelmi incidensek esetén, a GDPR szabályainak megfelelően járnak el;
b) Ahogy korábban említettük, az elszámoltathatóság elvével kapcsolatban, létre kell hozniuk egy az adatvédelmi incidensek kezelésére vonatkozó belső szabályzatot;
c) A vállalkozásoknak létre kell hozniuk az adatvédelmi incidensek nyilvántartását.

AZ ADATVÉDELMI HATÁSVIZSGÁLAT

Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelőnek az adatkezelést megelőzően hatásvizsgálatot kell végeznie arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Ha van kijelölt adatvédelmi tisztviselő, az adatkezelőnek az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő szakmai tanácsát ki kell kérnie.
Adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

- profilalkotáson és automatizált adatkezelésen alapuló személyes jellemzők értékelése;
- különleges adatok és bűnügyi adatok nagy számban történő kezelése;
- nyilvános helyek megfigyelése.

Az adatvédelmi hatásvizsgálatnak legalább a következőket kell tartalmaznia:

• a tervezett adatkezelési műveletek módszeres leírása és az adatkezelés céljainak ismerteté-

se, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálata;
- a potenciálisan magas kockázattal járó adatkezelésekre vonatkozóan, az érintett jogait és szabadságait érintő kockázatok vizsgálata; és
- a kockázatok kezelését célzó intézkedések bemutatása, ideértve a személyes adatok védelmét és a GDPR-al való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciák, biztonsági intézkedések és mechanizmusok.

A felügyeleti hatóságnak össze kell állítania és nyilvánosságra kell hoznia az olyan adatkezelési műveletek típusainak a jegyzékét, amelyekre vonatkozóan adatvédelmi hatásvizsgálatot kell végezni. Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az adatkezelőnek konzultálnia kell a felügyeleti hatósággal.

Az adatvédelmi hatásvizsgálattal kapcsolatos feladatok:

a) A vállalkozásoknak értékelnie kell, hogy az adatkezelés magas kockázattal jár-e;
b) A vállalkozásoknak értékelni kell egy új technológia vagy adatkezelés alkalmazása, bevezetése előtt, hogy az valószínűsíthetően magas adatvédelmi kockázattal jár-e;
c) A vállalkozásoknak az új technológia alkalmazása előtt meg kell terveznie majd el kell végeznie a hatásvizsgálatot, az adatvédelmi tisztviselő bevonásával;
d) A hatásvizsgálatot követően, amennyiben valamilyen ún. reziduális kockázat azonosításra került, a vállalkozásoknak konzultálniuk kell majd a hatósággal.

AZ ADATVÉDELMI TISZTVISELŐ

A GDPR alapján adatvédelmi tisztviselőt kell kijelölni, ha:
a) az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat;
b) az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé;
c) az adatkezelés különleges adatok vagy bűnügyi adatok nagy számban történő kezelését foglalják magukban.

Az adatkezelőnek és az adatfeldolgozónak biztosítania kell, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon. Az adatkezelőnek és az adatfeldolgozónak biztosítania kell, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. Az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének tartozik felelősséggel. Az adatvédelmi tisztviselő más feladatokat is elláthat. Az adatkezelő vagy az adatfeldolgozó biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

A vállalkozáscsoport közös adatvédelmi tisztviselőt is kijelölhet, ha az adatvédelmi tisztviselő valamennyi tevékenységi helyről könnyen elérhető.

Az adatvédelmi tisztviselő kijelölésével kapcsolatos felkészülési feladatok:

a) A vállalkozásoknak meg kell vizsgálniuk, hogy a GDPR-ban meghatározott adatkezelés esetükben fennáll-e (vállalkozások esetében ez jellemzően a b) esetben történhet meg);
b) Amennyiben az szükséges ki kell választaniuk a megfelelő szakértelemmel rendelkező adat-

védelmi tisztviselőt. Ez különös jelentőséggel bír, hiszen a GDPR alapján, az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a GDPR-ban említett adatvédelmi tisztviselői feladatok ellátására való alkalmasság alapján kell kijelölni. Az adatvédelmi tisztviselő nem csupán az adatkezelő vagy az adatfeldolgozó alkalmazottja lehet, de szolgáltatási szerződés keretében is elláthatja a feladatait;

c) A vállalkozásoknak közzé kell majd tenniük az adatvédelmi tisztviselő nevét és elérhetőségét, továbbá közölnie kell az előbbieket a felügyeleti hatósággal is.

A TANÚSÍTÁSI RENDSZER

A tagállamok, a felügyeleti hatóságok, a Testület, valamint a Bizottság – különösen uniós szinten – ösztönzik olyan adatvédelmi tanúsítási mechanizmusok, valamint adatvédelmi bélyegzők, illetve jelölések létrehozását, amelyek bizonyítják, hogy az adatkezelő vagy adatfeldolgozó által végrehajtott adatkezelési műveletek megfelelnek e rendelet előírásainak. Az adatkezelő vagy adatfeldolgozó részére a tanúsítványt legfeljebb hároméves időtartamra lehet kiállítani, amely azonos feltételek mellett a tanúsítvány megújítható, feltéve, hogy a vonatkozó követelmények továbbra is teljesülnek.

A SZEMÉLYES ADATOK HARMADIK ORSZÁGOKBA VAGY NEMZETKÖZI SZERVEZETEK RÉSZÉRE TÖRTÉNŐ TOVÁBBÍTÁSA

Személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására akkor kerülhet sor, ha a Bizottság megállapította, hogy a harmadik ország, a harmadik ország valamely területe, vagy, egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít. Az ilyen adattovábbításhoz nem szükséges külön engedély. A Bizottság az Európai Unió Hivatalos Lapjában és annak honlapján közzéteszi az olyan harmadik országok, harmadik országon belüli területek és meghatározott ágazatok, valamint nemzetközi szervezetek jegyzékét, amelyek esetében úgy ítélte meg, hogy biztosítják, vagy többé nem biztosítják a megfelelő védelmi szintet.

A fent említett határozat hiányában az adatkezelő vagy adatfeldolgozó csak abban az esetben továbbíthat személyes adatokat harmadik országba vagy nemzetközi szervezet részére, ha az adatkezelő vagy adatfeldolgozó a GDPR-ban meghatározott, megfelelő garanciákat nyújtott, és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.

Valamely harmadik ország bíróságának bármely olyan ítélete, illetve közigazgatási hatóságának bármely olyan döntése, amely valamely adatkezelő vagy adatfeldolgozó számára személyes adatok továbbítását vagy közlését írja elő, kizárólag akkor ismerhető el vagy hajtható bármely módon végre, ha az az adatok megismerését igénylő harmadik ország és az Unió vagy egy tagállama között létrejött, hatályos nemzetközi megállapodáson, például kölcsönös jogsegélyszerződésen alapul, az adattovábbítás e fejezet szerinti egyéb módozatainak sérelme nélkül.

A nemzetközi adattovábbítással kapcsolatos felkészülési feladatok:

a) A vállalkozásoknak meg kell vizsgálniuk, hogy pontosan milyen országokba, milyen szervezetek számára továbbítanak adatot;
b) Ezt követően a vállalkozásoknak fel kell mérniük, hogy az adott adattovábbítás olyan területre vagy szervezet részére történik, amely szerepel a Bizottság által összeállított jegyzéken;
c) Amennyiben az adattovábbítás olyan területre vagy szervezet részére történik, amely nem szerepel a Bizottság jegyzékén, úgy a vállalkozásoknak meg kell vizsgálniuk, hogy az adattovábbítás címzettje nyújtja-e a GDPR-nak megfelelő garanciákat és hogy biztosított-e a jogorvoslat lehetősége.

ONE STOP SHOP

Az adatkezelő vagy az adatfeldolgozó tevékenységi központja vagy egyetlen tevékenységi helye szerinti felügyeleti hatóság jogosult fő felügyeleti hatóságként eljárni az említett adatkezelő vagy az adatfeldolgozó által végzett határokon átnyúló adatkezelés tekintetében. A fő felügyeleti hatóság az adatkezelő vagy adatfeldolgozó egyetlen kapcsolattartója az általuk végzett, határokon átnyúló adatkezeléssel kapcsolatban. A fő felügyeleti hatóság, konszenzusra törekedve együttműködik a többi érintett felügyeleti hatósággal. A fő felügyeleti hatóság és az érintett felügyeleti hatóságok minden releváns információt kicserélnek egymással.

A one stop shop-al kapcsolatos felkészülési feladatok:

a) A vállalkozásoknak a tevékenységi központjuk kiválasztása során a jövőben figyelembe kell venniük majd az adott területen fő felügyeleti hatóságként eljáró hatósággal való kapcsolatukat és a hatóság adatvédelmi gyakorlatát. Ez a jövőben kiemelten fontos lesz, hiszen az adott vállalat a fő felügyeleti hatósággal fog kommunikálni az Unió egész területére kiterjedő adatkezelésével kapcsolatban, így kiemelt feladat lesz az is, hogy az illetékes hatósággal jó kapcsolatot alakítson ki az adott vállalkozás.

AZ EURÓPAI ADATVÉDELMI TESTÜLET

A GDPR létrehozza az Európai Adatvédelmi Testületet, melynek fő feladata a GDPR egységes alkalmazásának biztosítása. A Testület minden tagállam egy felügyeleti hatóságának vezetőjéből és az európai adatvédelmi biztosból vagy azok képviselőiből áll.

SZANKCIÓK ÉS FELELŐSSÉG

Minden olyan személy, aki a GDPR megsértésének eredményeként vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért az adatkezelőtől vagy az adatfeldolgozótól kártérítésre jogosult. Az adatkezelésben érintett valamennyi adatkezelő felelősséggel tartozik minden olyan kárért, amelyet a GDPR-nak nem megfelelő adatkezelés okozott. Az adatfeldolgozó csak abban az esetben tartozik felelősséggel az adatkezelés által okozott károkért, ha nem tartotta be a GDPR-ban meghatározott, kifejezetten az adatfeldolgozókat terhelő kötelezettségeket, vagy ha az adatkezelő jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el.

Az adatkezelő, illetve az adatfeldolgozó mentesül a felelősség alól, ha bizonyítja, hogy a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség. Ha több adatkezelő vagy több adatfeldolgozó vagy mind az adatkezelő mind az adatfeldolgozó érintett ugyanabban az adatkezelésben, minden egyes adatkezelő vagy adatfeldolgozó az érintett tényleges kártérítésének biztosítása érdekében egyetemleges felelősséggel tartozik a teljes kárért.

A GDPR alapján a kiszabható adatvédelmi **bírság 20 000 000 euróig vagy az előző év globális forgalmának 4%-ig is terjedhet.** Nagyon fontos figyelembe venni, hogy a két összeg közül a magasabbat kell majd kiszabni.

Meg kell említenünk azonban, hogy a fenti bírságplafon az adatkezelés alapelveinek megszegése esetén alkalmazandó, míg létezik egy alacsonyabb bírságplafon is, mely az alacsonyabb szintű, adminisztratív jellegű szabályok megsértése esetén alkalmazandó. Ez az alacsonyabb bírság **10 000 000 euróig vagy az előző év globális forgalmának 2%-ig terjedhet.**

A szigorúbb felelősségi szabályokkal kapcsolatos felkészülési feladatok:

a) A vállalkozásoknak fel kell mérniük az adatkezelési folyamataikat és azonosítaniuk kell az

abban rejlő megfelelőségi kockázatokat;

b) A vállalkozásoknak szükség esetén meg kell változtatniuk az adatkezelési gyakorlatukat, oly módon, hogy az általuk meghatározott adatkezelési célokat a lehető legkisebb megfelelőségi kockázat mellett tudják elérni;

c) A vállalkozásoknak fel kell készülniük a jelentősen megemelt szankciók miatti követeléskezelésekre és vitarendezésekre, ki kell alakítaniuk a megfelelő érdekérvényesítő és vitarendezési mechanizmusokat.

+1) A vállalkozásoknak a pénzügyi tervezés folyamán is számításba kell venniük a jelentősen megemelt szankciós kitetettséget, valamint azt, hogy az adatkezelési megfelelőség napi szintű költségei jelentősen megemelkednek

AZ ADATKEZELÉS SPECIÁLIS ESETEI

A GDPR bizonyos rendelkezéseitől eltérési lehetőséget enged a tagállamoknak annak érdekében, hogy a személyes adatok védelméhez való jogot össze lehessen egyeztetni a véleménynyilvánítás szabadságához és a tájékozódáshoz való joggal.

A közérdekű feladat teljesítése céljából közhatalmi szervek, vagy egyéb, közfeladatot ellátó szervek, illetve magánfél szervezetek birtokában lévő hivatalos dokumentumokban szereplő személyes adatokat az adott szerv vagy szervezet az uniós joggal vagy a szervre vagy szervezetre alkalmazandó tagállami joggal összhangban nyilvánosságra hozhatja annak érdekében, hogy a hivatalos dokumentumokhoz való nyilvános hozzáférést összeegyeztesse a személyes adatok e rendelet szerinti védelméhez való joggal.

A tagállamok jogszabályban vagy kollektív szerződésekben pontosabban meghatározott szabályokat állapíthatnak meg annak érdekében, hogy biztosítsák a jogok és szabadságok védelmét a munkavállalók személyes adatainak a foglalkoztatással összefüggő kezelése tekintetében, különösen a munkaerő-felvétel, a munkaszerződés teljesítése céljából, ideértve a jogszabályban vagy kollektív szerződésben meghatározott kötelezettségek teljesítését, a munka irányítását, tervezését és szervezését, a munkahelyi egyenlőséget és sokféleséget, a munkahelyi egészségvédelmet és biztonságot, a munkáltató vagy a fogyasztó tulajdonának védelmét is, továbbá a foglalkoztatáshoz kapcsolódó jogok és juttatások egyéni vagy kollektív gyakorlása és élvezete céljából, valamint a munkaviszony megszüntetése céljából.

A személyes adatok közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból folytatott kezelését a GDPR-al összhangban az érintett jogait és szabadságait védő megfelelő garanciák mellett kell végezni. E garanciáknak biztosítaniuk kell, hogy olyan technikai és szervezési intézkedések legyenek érvényben, melyek biztosítják különösen az adattakarékosság elvének betartását. Ezen intézkedések közé tartozhat az álnevesítés, amennyiben az említett célok ily módon megvalósíthatók. Amennyiben e célok megvalósíthatók az adatok oly módon történő további kezelése révén, amely nem vagy már nem teszi lehetővé az érintettek azonosítását, a célokat ilyen módon kell megvalósítani.

A tagállamok egyedi szabályokat fogadhatnak el annak érdekében, hogy meghatározzák a felügyeleti hatóságok hatáskörét olyan adatkezelőkre vagy adatfeldolgozókra vonatkozóan, amelyek az uniós vagy a tagállami jog alapján, vagy az illetékes nemzeti szervek által alkotott szabályok alapján szakmai titoktartási kötelezettség vagy azzal egyenértékű egyéb titoktartási kötelezettség hatálya alá tartoznak, ha ez szükséges és arányos a személyes adatok védelméhez való jog és a titoktartási kötelezettség összeegyeztetése érdekében.
Ha egy tagállamban egyház, illetve vallási szervezet vagy közösség a GDPR hatálybalépésének időpontjában átfogó szabályokat alkalmaz a természetes személyek személyes adatok kezelése tekintetében történő védelme vonatkozásában, e szabályok tovább alkalmazhatók, ha a GDPR-al összhangba hozzák őket.

A RENDELETBEN FOGLALTAK ALKALMAZÁSÁNAK KEZDŐ IDŐPONTJA

A Rendeletben foglaltakat 2018. május 25-től kell alkalmazni. Addig a továbbiakban is a 95/46/EK irányelv, illetve az Info tv. az irányadóak.

KONKLÚZIÓ

Ahogy azt az összefoglalóban láthattuk a GDPR-nak való megfelelőségre való felkészülés jelentős kihívások és sok feladat elé állítja a vállalkozásokat, továbbá igen komoly szankcióval fenyegeti azokat, akik nem tartják be a GDPR-ban foglalt szabályokat és az adatkezelésüket nem hozzák összhangba az abban foglalt előírásokkal.
Különösen a jelentősen megnövekedett adatvédelmi felelősség, valamint a szigorúbb adatkezelési és adatfeldolgozási előírásokra tekintettel a vállalkozásoknak a hátralévő időben meg kell tenniük mindent, hogy készen álljanak az új európai adatvédelmi rezsimnek való megfelelésre. A vállalkozásoknak és az adatkezelőknek ezt a felkészülést – amennyiben eddig még nem kezdték volna el - indokolt minél hamarabb elkezdeni, hiszen egy rendkívül bonyolult, időigényes és drága megfelelőségi folyamatot kell viszonylag rövid időn belül végrehajtani.

Köszönöm az anyag elkészítését meglátásaikkal és szerkesztői munkájukkal segítők, így Hodák Vencel, Németh Márton, Molnár Benedek, Gyarmati Dorottya, Gönczi Gergely és Schmidt Cecília munkáját.