Amit a GDPR-ról tudni kell

2018. május 25-én életbe lép az Európai Unió új adatvédelmi rendelete (GDPR – General Data Protection Rules), amely a nemzeti jogszabályokat felülírva egységesíti az uniós tagállamok adatkezelési szabályait. A magánszemélyek nagyobb betekintést és jogokat kapnak az adataik kezelésével kapcsolatban, ezzel párhuzamosan a cégek ez irányú kötelezettségeit növekednek, a mulasztásokat pedig minden eddiginél nagyobb pénzbüntetéssel sújtják.

Az új, egységes európai szabályozás jövő év május 25-én lép hatályba, s bár ez még távolinak tűnhet, a változások olyan sok mindenre kiterjednek, hogy ez a bő félév biztosan kell a felkészülésre, amit ideje a cégeknek haladéktalanul elkezdeni. A rendelet ugyanis nemcsak a nagyvállalatokat érinti, hanem minden, adatot kezelő vállalkozást, legyen az családi cég vagy kis- és középvállalkozás (kkv).

Ráadásul a rendelet nemcsak a digitálisan tárolt személyes adatokra vonatkozik, hanem a papíralapúakra is, amennyiben azok valamilyen nyilvántartási rendszer részét képezik vagy fogják képezni. Mivel a nyilvántartási rendszer nem jelent mást, mint meghatározott ismérvek alapján hozzáférhető adatokat, ezért nagy az esélye, hogy az iratkezelések túlnyomó többsége a rendelet hatálya alá esik, így azokra ugyanolyan szigorúan szabályozás fog vonatkozni a kezeléstől a tároláson át a szakszerű iratmegsemmisítésig, mint a digitálisan tárolt személyes adatokra.

GDPR közérthetően

Forrás: GDPR Info
https://www.gdpr.info.hu/blog

Egyre többször merül fel kérdésként a GDPR-al kapcsolatban, hogyan is kell értelmezni a rendelet alkotói által létrehozott, gyakran babilóni körmondatokban megfogalmazott kötelezettségeket.

Alkalmazási terület

A rendeletet személyes adatok automatizált módon történő kezelésekor, valamint akkor kell alkalmazni, ha személyes adatokat valamely nyilvántartási rendszerben kezelnek. A rendeletnek mind a tárgyi (mikor kell alkalmazni), mind a területi (hol kell alkalmazni) hatálya szélesebb a korábbi adatvédelmi jogszabályokénál.

Tárgyi hatály: A rendeletet mind az adatkezelők, mind azadatfeldolgozók tevékenységére alkalmazni kell. A rendeletet nem kell alkalmazni, ha a személyes adatok kezelése személyes vagy ott honi tevékenység során történik.

Területi hatály: a rendeletet alkalmazni kell az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett adatkezelésre illetve az Unióban tartózkodó érintettek személyesadatainak az Unióban tevékenységi hellyel nemrendelkező adatkezelő vagy adatfeldolgozó általvégzett kezelésére, ha 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.

Teendők

1. a kezelt személyes adatok számbavétele, az adatregiszter és az adattérképek elkészítése
2. az EU-ban lévő, személyes adatokat kezelő tevékenységi helyek feltérképezése
3. Európán kívüli adatkezelők esetén annak megállapítása, hogy áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához vagy viselkedésüknek a megfigyeléséhez kapcsolódóan milyen adatkezelés történik
4. annak meghatározása, hogy az adatkezelés adatkezelőként vagy adatfeldolgozóként történik
5. annak eldöntése, hogy szükséges-e uniós képviselőt kijelölni

Az adatkezelés jogalapja

A magyar jogalkalmazók számára a legszembetűnőbb változás az, hogy a rendelet az adatkezelő jogos érdekét is a jogalapok között nevesíti. Ennek a jogalapnak az alkalmazásakor fontos feladat lesz az érdekmérlegelési teszt elkészítése.

1. A személyes adatok kezelése akkor jogszerű, amennyiben legalább az alábbiak egyike teljesül:
2. az érintett hozzájárulását adta személyes adatainak kezeléséhez
3. az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél
4. az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges
5. az adatkezelés az érintett létfontosságú érdekeinek védelme miatt szükséges
6. az adatkezelés közérdekű feladat végrehajtásához szükséges

A hozzájáruláson alapuló adatkezelés során az adatkezelőnek bizonyítania kell tudnia, hogy az érintett szabadon adta meg a hozzájárulását, a hozzájárulás iránti kérelmet más ügyektől egyértelműen megkülönböztethető módon kell előadni.
A jogos érdekre történő hivatkozásnál az adatkezelő érdekeit és az érintett jogait érdekmérlegelési teszt elvégzésével kell összevetni, illetve az érintettet tájékoztatni kell arról, hogy az adatkezelés az adatkezelő jogos érdekén alapul. Az érdekmérlegelési teszt lényegében annak írásbeli dokumentálása, hogy a munkáltató által tervezett ellenőrzésre miért van szükség, hogyan is végezné azt, és milyen – a munkavállalók érdekeit védő – garanciákat épített be az adatkezelés folyamatába. A rendelet meghatározza a kritériumokat, hogy mikor megengedett az adatoknak az eredeti céljától eltérő egyéb célból történő kezelése.

Teendők

1. az adatkezelések jogalapjának vizsgálata
2. annak felülvizsgálata, hogy az érintett hozzájárulása érthető, könnyen hozzáférhető formában, világos és egyszerű nyelvezettel történik-e
3. érdekmérlegelési teszt elvégzése, ha a jogos érdek az adatkezelés jogalapja
4. az eredeti céltól eltérő, egyéb cél esetén dokumentálni az adatkezelés indokát

Az érintettek jogai

Az adatkezelők tevékenységének transzparensebbnek kell lennie az érintettek számára, akik többlet jogokat kapnak az adataik feletti közvetlenebb rendelkezés révén, a hozzáférési jogon, a helyesbítési és a törlési jogon keresztül.

Átlátható tájékoztatás
A természetes személyek jogosultak a személyes adatik kezeléséről tömör, átlátható és könnyen hozzáférhető formában, világosan és közérthetően tájékoztatást kapni, így különösen:

- az adatkezelő kilétéről és elérhetőségéről
- az adatvédelmi tisztviselő elérhetőségeiről
- a személyes adatok tervezett kezelésének céljáról, valamint az adatkezelés jogalapjáról
- a „jogos érdeken" alapuló adatkezelés esetén ezen jogos érdekekről
- a személyes adatok címzettjeiről
- az EU-n kívülre történő adattovábbítás esetén a megfelelő garanciákról
- az adatkezelés tervezett időtartamáról
- az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról
- a felügyeleti hatósághoz címzett panasz benyújtásának jogáról
- arról, hogy a szerződés kötésének előfeltétele-e az adatok megadása, illetve milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása
- az esetleges automatizált döntéshozatalról, ideértve a profilalkotást is.

Hozzáférési jog
Az adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát ingyenesen köteles az érintett rendelkezésére bocsátani. 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. Mindez nem érintheti hátrányosan mások jogait és szabadságait.

A helyesbítéshez való jog
Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat.

A törléshez való jog
Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, ha

- a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték
- az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja
- az érintett tiltakozik az adatainak kezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre
- a személyes adatokat jogellenesen kezelték.

Az adatkezelés korlátozásához való jog
Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha

- az érintett vitatja a személyes adatok pontosságát
- az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését
- az adatkezelőnek már nincs szüksége a személyes adatokra, de az érintett igényli azokat jogi igények érvényesítéséhez.

Az adathordozhatósághoz való jog
Az érintett jogosult arra, hogy a rá vonatkozó, általa az adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, ha az adatkezelés hozzájáruláson vagy szerződésen alapul és az adatkezelés automatizált módon történik.

Automatizált adatkezelés
Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely őt jelentős mértékben érintené.

Teendők

- az adatvédelmi nyilatkozatok áttekintése
- megvizsgálni az üzleti folyamatokat az érintettek hozzáférési joga szempontjából
- az adathordozhatósághoz és az adatkorlátozáshoz való jognak történő megfelelés vizsgálata
- az informatikai rendszereknek a törléshez való jog szerinti átalakítása, különös tekintettel a biztonsági mentésekre.

Adatvédelmi irányítási rendszer

A rendelet által bevezetett új kötelezettséget jelent, hogy az „elszámoltathatóság" elvének megfelelően az adatkezelő nemcsak, hogy felelős a GDPR-nak való megfelelésért, hanem képesnek kell lennie e megfelelés igazolására is. Mindez elképzelhetetlen megfelelő adatvédelmi irányítási rendszer bevezetése nélkül.

Megfelelő technikai és szervezési intézkedések
Az adatkezelőnek megfelelő technikai és szervezési intézkedéseket kell végrehajtania annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a rendelettel összhangban történik:

- belső adatvédelmi szabályzatok
- magatartási kódexhez való csatlakozás
- tanúsítási mechanizmushoz való csatlakozás útján.

Beépített és alapértelmezett adatvédelem
A beépített adatvédelem (Privacy by design) elve értelmében az adatvédelmet és az adatbiztonságot a tervezéskor kell beépíteni – pl. álnevesítés, titkosítás révén – az üzleti folyamatokba, műszaki termékekbe. Az alapértelmezett adatvédelem (Privacy by default) elve arra ad biztosítékot, hogy a szolgáltatás nyújtásához, termék igénybevételéhez minimálisan szükséges személyes adatot kezelik a vállalkozások.

Adatvédelmi hatásvizsgálat
Ha az adatkezelés magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve (pl. profilalkotáson alapuló döntéshozatal, különleges adatok nagy számban történő kezelése), akkor az adatkezelőnek az adatkezelést megelőzően hatásvizsgálatot köteles végeznie.

Adatvédelmi tisztviselő
Az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt köteles kijelölni, ha fő tevékenységeik olyan adatkezelési műveleteket foglalnak magukban, amelyek az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését vagy különleges adatok nagy

mértékű kezelését teszik szükségessé. A fentieken túl adatvédelmi tisztviselőt bármelyik vállalkozás kinevezhet vagy külsős szolgáltatóként megbízhat.

Adatregiszter, adattérkép
Minden adatkezelőnek kötelessége adatkezelési tevékenységeiről nyilvántartást vezetni. A nyilvántartás minimálisan az adatkezelő nevét és elérhetőségét, az adatkezelés céljait, a személyes adatok kategóriáit, a tervezett törlési határidőket és az olyan címzettek kategóriáit tartalmazza, akikkel a személyes adatokat közlik. Az adattérkép a bonyolultabb adatkezelési folyamatok vizuális áttekintését segítheti.

Teendők

- a management GDPR tudatosságának elérése
- a megfelelő személyi és anyagi erőforrások biztosítása az adatvédelmi irányítási eszközök létrehozására
- a felelősségi körök megállapítása
- annak megvizsgálása, hogy kötelező-e vagy szükséges-e adatvédelmi tisztviselőt kinevezni vagy megbízni
- meglévő adatvédelmi, információbiztonsági irányítási eszközök áttekintése és egybevetése az üzleti folyamatokkal
- ha szükséges, az üzleti folyamatok átalakítása

Adatvédelmi incidensek

Szigorú szabályokat és határidőket állapít meg a rendelet az adatvédelmi incidensek kezelésére. Az adatkezelők fontos feladata az adatvédelmi incidensek megfelelő időben való észlelése, annak megállapítása, hogy pontosan mi történt, az incidens milyen súlyú, milyen hatással lehet az érintettekre. Az incidensek észlelésére, értékelésére, jelentésére, és enyhítésére tett nem megfelelő intézkedések esetén a legmagasabb összegű bírságokat helyezi kilátásba a GDPR.

Adatvédelmi incidens fogalma
Az adatvédelmi incidens alatt a biztonság olyan sérülését értjük, amely a személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az adatvédelmi hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Az adatvédelmi incidensről szóló bejelentésben legalább:

- ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát
- közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket
- ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az EU szakosított ügynöksége, az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) módszertani útmutatójában ajánlást fogalmazott meg arra vonatkozóan, hogy milyen módszerrel állapíthatjuk meg az adatvédelmi incidens súlyosságát.

Teendők

- az adatvédelmi incidensek észlelésére, értékelésére, bejelentésére megfelelő intézkedési terv készítése az adatkezelőnél
- a munkavállalók képzése a szűk határidők miatt kiemelten fontos
- biztosítani a megfelelő eljárásrendet az adatfeldolgozónál is

Adatfeldolgozói szerződések

Elsőként némi fogalommagyarázattal kezdve tisztázzuk, mi a különbség adatkezelő és adatfeldolgozó között. 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. Adatfeldolgozó pedig az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel (például egy informatikai szolgáltatás üzemeltetője). A GDPR új kötelezettségeket állapít meg az adatfeldolgozók számára. A rendelet meghatározza az adatkezelők és az adatfeldolgozók között a személyes adatok kezelésére kötött szerződések kötelező tartalmielemeit.

Az adatkezelők és az adatfeldolgozók közötti szerződések

Az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik megfelelő garanciákat nyújtanak a GDPR rendelkezései szerinti, megfelelő technikai és szervezésiintézkedések végrehajtására. Az adatkezelő és az adatfeldolgozó között olyan írásbeli szerződést kell kötni, amely minimálisan az alábbiakra tér ki:

- 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
- segíti az adatkezelőt a kötelezettségeinek a teljesítésében
- 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 vagy a tagállami jog az személyes adatok tárolását írja elő
- lehetővé teszi és elősegíti az adatkezelő általvagy az általa megbízott más ellenőr általvégzett auditokat, beleértve a helyszínivizsgálatokat is.

Ha az adatfeldolgozó további adatfeldolgozó szolgáltatásait is igénybe veszi, a további adatfeldolgozóra is ugyanazokat az adatvédelmi kötelezettségeket kell telepíteni, mint amelyek az adatkezelő és az adatfeldolgozó között létrejött szerződésben vannak. Az adatfeldolgozók számára a következő kötelezettségeket írja elő a rendelet:

- az adatvédelmi hatóság részére bemutatható módon kell nyilvántartást vezetnie az adatkezelő nevében végzett adatkezelési tevékenységéről
- az adatvédelmi incidenst, az arról való tudomásszerzést követően haladéktalanul jelentenie kell az adatkezelőnek
- ha azt a rendelet előírja, adatvédelmi tisztviselőt jelöl ki vagy bíz meg

Teendők

- az adatkezelőnek biztosítania kell, hogy valamennyi adatfeldolgozóval kötött szerződése megfelel a rendelet rendelkezéseinek
- adatkezelési tevékenységek nyilvántartásának elkészítése az adatfeldolgozónál
- az adatfeldolgozónak megfelelő technikai és szervezési intézkedéseket kell bevezetnie, ideértve az adatvédelmi incidensek esetén alkalmazandó eljárásrendet
- annak eldöntése, hogy adatvédelmi tisztviselő kinevezése vagy megbízása kötelező-e vagy szükséges-e?

A személyes adatok EU-n kívülre történő továbbítása

A GDPR alapelvként rögzíti, hogy a személyes adatoknak az Unión kívülre történő továbbítása esetén sem sérülhet a természetes személyeknek az EU-ban biztosított védelem szintje. Az adattovábbítás csak megfelelő jogi garanciák megléte esetén jogszerű.
Személyes adatok EU-n kívülre történő továbbítására akkor kerülhet sor, ha a Bizottság megállapította, hogy a harmadik ország megfelelő védelmi szintet biztosít. Az ilyen adattovábbításhoz nem szükséges külön engedély. Ilyen döntés nyomán továbbítható személyes adat az Egyesült Államokba (Privacy Shield, korábban Safe Harbor). A biztonságos országok listája a Bizottság honlapján megtalálható. A fenti döntés hiányában személyes adat akkor továbbítható az Unión kívülre, ha

- az Európai Bizottság által elfogadott általános adatvédelmi szerződéses kikötéseket alkalmazzák a felek
- olyan kötelező erejű vállalati szabályokat (BCR) vezet be egy vállalkozás, amelyet azadatvédelmi hatóság jóváhagyott
- jóváhagyott magatartási kódexhez csatlakozott vállalkozásnak kerül továbbításra
- jóváhagyott tanúsítási mechanizmussal rendelkező vállalkozásnak továbbítják.

A fenti garanciák hiányában az Unión kívülre akkor lehet személyes adatot továbbítani, ha

- az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról
- az adattovábbítás szerződés teljesítéséhez szükséges
- az adattovábbítás fontos közérdekből szükséges
- az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges
- az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására
- a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja.

Teendők

- az EU-n kívülre továbbított adatok feltérképezése
- az adattovábbítások jogalapjának felülvizsgálata
- a bizottsági megfelelőségi döntések folyamatos nyomon követése

Jogorvoslat, kártérítés, bírság

A GDPR megfelelő alkalmazását biztosítandó a rendelet garanciális szabályokat állít a jogszabály megsértése esetére. A jogorvoslati lehetőség, a kártérítéshez való jog és a mamut méretű bírságok mind ezt a célt szolgálják.

Jogorvoslatok

- Minden érintett jogosult arra, hogy panaszt tegyen az adatvédelmi hatóságnál – különösen a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban –, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti a rendeletet.
- Minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben.
- Minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak a GDPR-nak nem megfelelő kezelése következtében megsértették a rendelet szerinti jogait.

Felelősség és kártérítés

- Minden olyan személy, aki a rendelet megsértésének eredményeként vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért az adatkezelőtől vagy az adatfeldolgozótól kártérítésre jogosult.
- Ha több adatkezelő vagy több adatfeldolgozó érintett ugyanabban az adatkezelésben, és felelősséggel tartozik az adatkezelés által okozott károkért, minden egyes adatkezelő vagy adatfeldolgozó az érintett tényleges kártérítésének biztosítása érdekében egyetemleges felelősséggel tartozik a teljes kárért.

Bírságok

- Az adatvédelmi bírság mértékét a GDPR-ban lefektetett szabályok mentén, a jogsértés típusától függően határozza meg az adatvédelmi hatóság.
- A rendelet szabályainak megsértői maximálisan 20 millió eurót vagy a vállalkozás előző pénzügyi év teljes éves világpiaci forgalmának 4 %-át kitevő összeggel sújthatóak, azzal, hogy a kettő közül a magasabb összeget kell kiszabni.
- Az adatvédelmi jogsértések esetén a tagállamok jogosultak további, így például büntetőjogi szankciókat alkalmazni.

Teendők

- az eljáró hatóságnak és az alkalmazandó jognak a meghatározása
- az adatkezelői, adatfeldolgozói szerződések felelősségi szabályainak felülvizsgálata, különös figyelemmel a felelősséget korlátozó vagy kizáró rendelkezésekre
- az adatvédelmi hatóság által az egyes ügyekben kiszabható bírságok mértékének megvizsgálása

Adatvédelmi hatóság

A természetes személyek alapvető jogainak és szabadságainak a személyes adataik kezelése tekintetében történő védelme, valamint a személyes adatok Unión belüli szabad áramlásának megkönnyítése érdekében minden tagállamban a rendelet alkalmazásának ellenőrzéséért egy vagy több független, szélesellenőrzési és bírságolási hatáskörrel rendelkező adatvédelmi hatóság felel.

Egyablakos rendszer

Több tagállamban tevékenységet folytató vállalatok esetében a tevékenységi központ helye szerinti felügyeleti hatóság jogosult fő felügyeleti hatóságként eljárni. Az adatvédelmi hatóságok joggyakorlatuk kialakítása során szorosan együttműködnek egymással és az Európai Bizottsággal. Az Európai Adatvédelmi Testület, amely jogi személyiséggel rendelkező uniós szerv a W29 Munkacsoport hatáskörét fogja átvenni. A Testület minden tagállam adatvédelmi hatóságának vezetőjéből és az európai adatvédelmi biztosból vagy azok képviselőiből áll. A Testület biztosítja a GDPR egységes alkalmazását, melynek keretében:

- ellenőrzi és biztosítja a rendelet helyes alkalmazását
- iránymutatásokat, ajánlásokat és legjobb gyakorlatokat bocsát ki
- véleményt bocsát ki az Európai Bizottság számára a valamely harmadik országban biztosított védelmi szint megfelelőségének megítéléséhez.

Teendők

- multinacionális vállalatok esetében az illetékes adatvédelmi hatóság meghatározása
- az adatvédelmi hatóság iránymutatásainak nyomon követése
- az Európai Adatvédelmi Testület legjobb gyakorlatának, iránymutatásainak nyomon követése