DIMSZ
Direkt és Interaktív Marketing Szövetség

FEDMA

Az EU Általános Adatvédelmi Rendelete

Mítosz és Valóság

& GYIK

Federation of European Direct and Interactive Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

1. Mítosz: A GDPR csak nagyvállalatoknak kötelező – nem csak nagyvállalatoknak!

A GDPR általánosságban alkalmazandó a személyes adatok kezelésére függetlenül attól, hogy az adatokat kis vagy nagy szervezetek kezelik. Az új szabályozás ezért a direkt és interaktív marketing iparág minden szereplőjére kötelező, nagyokra és kicsikre egyaránt. A túlszabályozás elkerülése érdekében a GDPR a KKV-k számára rugalmasabb szabályokat tartalmaz. Nem kötelező számukra például az adatkezelésekről való belső nyilvántartás vezetése, kivéve ha az adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár.

2 Mítosz: A GDPR csak az Európában letelepedett szervezeteknek kötelező – nem csak az Európában letelepedett szervezetekre!

A GDPR az Európai Gazdasági Térségben (az Európai Unió 27 tagállamán kívül Izland, Liechtenstein és Norvégia - a továbbiakban: Európai Unió) tevékenységi hellyel rendelkező direkt és interaktív marketing tevékenységet folytató cégre vonatkozik még akkor is, ha az adatkezelésre az Európai Unión kívül kerül sor. A GDPR ezen kívül azokra a szervezetekre is alkalmazandó, amelyek nem az Európai Unióban rendelkeznek letelepedési hellyel, de az adatkezelésük áruknak vagy szolgáltatásoknak az Európai Unióban történő nyújtásához kapcsolódik (ideértve az ingyenes árukat és szolgáltatásokat), vagy ha ezek a szervezetek egyének viselkedését figyelik meg sütik vagy ahhoz hasonló technológiák segítségével.

3 Mítosz: A GDPR csak az online adatkezelést érinti – nem csak az online adatkezelést!

A GDPR technológia-semleges és széles körben alkalmazandó. Az új szabályok alkalmazandók a személyes adatoknak mind az offline (pl. papíralapú nyilvántartó rendszer), mind az online kezelésére.

4. Mítosz: Mi csak B2B (vállalkozások között) kezelünk adatokat, ezért a GDPR nem vonatkozik ránk – téves!

A GDPR átfogóan vonatkozik a személyes adatok kezelésére, és nem tesz különbséget a B2B (vállalkozások közötti) és a B2C (vállalkozások és fogyasztók közötti) kapcsolatokból származó személyes adatok között. A B2B szektorban személyes adat például a munkahelyi e-mail cím, a munkahelyi telefonszám, a név, a beosztás, és a munkahely irányítószám is, mivel ezekkel az adatokkal egyértelműen azonosítani lehet egy élő személyt.

5. Mítosz: Mi nem végzünk automatizált adatkezelést, a GDPR nem vonatkozik ránk – téves!

A GDPR minden automatizált (pl. profilalkotás), illetve részben automatizált vagy egyéb módon (manuálisan, emberi beavatkozás által) végzett adatkezelésre vonatkozik.

6. Mítosz: A GDPR-nak való megfeleléshez csak át kell néznünk az adatvédelmi szabályzatainkat és az adatvédelmi tájékoztatóinkat – téves!

A GDPR növeli a hatályos adatvédelmi kötelezettségek szintjét, például a hozzájárulást egyértelműen kell megadni, és a szervezeteknek adatkezeléseikkel kapcsolatosan részletesebb tájékoztatást kell adniuk az érintett személyeknek. Az új jogszabály a direkt és interaktív marketing tevékenységet folytató cégek számára újfajta kötelezettségeket is megállapít. Ilyen például az adatvédelmi incidensek bejelentése, az adatvédelem beépítése a projektekbe már az induláskor (beépített adatvédelem), és annak biztosítása, hogy a kiindulási adatvédelmi beállítások blokkolják a kapcsolatfelvételt (alapértelmezett adatvédelem); valamint néhány új jogot az érintett személyek számára, például arra nézve, hogy információt vigyenek át az egyik szolgáltatótól a másikhoz (adathordozhatósághoz való jog).

Az adatvédelmi *szabályzatok* egy szervezetnek az általa végzett adatkezelést részletező belső dokumentumai, míg az adatvédelmi *tájékoztatók* az érintett személyek számára a személyes adataik gyűjtésével és kezelésével kapcsolatosan szükséges információkat tartalmazó külső dokumentumok. Az adatvédelmi szabályzatok és tájékoztatók átnézése biztosítja a megfelelést a szervezet számára irányadó új tájékoztatási követelményeknek, de ez csak egy az új jogszabálynak való megfeleléshez szükséges előkészületek közül. Új belső eljárásokat kell kidolgozni. Ezen túlmenően a rendelet által bevezetett elszámoltathatósági alapelv arra bátorítja a szervezeteket, hogy mindennapi adatkezeléseik során új, proaktív adatvédelmi megközelítést válasszanak annak érdekében, hogy a GDPR szabályainak való megfelelésüket bármikor képesek legyenek igazolni a nemzeti adatvédelmi hatóságoknak.

7. Mítosz: Már megszereztük az érintettek hozzájárulását ahhoz, hogy használhassuk az adataikat, ezért nem kell megfelelnünk a GDPR-nak – téves

A GDPR növeli a hatályos adatvédelmi kötelezettségek szintjét, így például az adatkezeléshez való hozzájárulásnak egyértelműnek kell lennie. A hozzájárulást félreérthetetlenül kell megadni - nem lehet csupán hallgatólagos. A direkt és interaktív marketing tevékenységet folytató cégeknek ezért felül kell vizsgálniuk az érintett személyektől kapott (marketing célú) hozzájárulások gyűjtésének módját. Ettől függetlenül a GDPR tartalmaz más jogalapokat is az adatkezeléshez (lásd a GYIK „Hogyan kezelhetünk személyes adatokat?" kérdését). Az érintett cégeknek a GDPR összes többi rendelkezésének is meg kell felelniük.

8. Mítosz: A sütik elfogadására vonatkozó banner bevezetésével a weboldalunkon már meg is feleltünk a GDPR-nak – téves

A sütik elfogadására vonatkozó banner független a GDPR-tól. Az érintett személyektől való hozzájárulás gyűjtése és tájékoztatásuk a weboldalon a süti használatról (például banner formájában) az Elektronikus Hírközlési Adatvédelmi Irányelvnek való megfeleléshez szükséges. A GDPR nem törli el a szervezeteknek azt a kötelezettségét, hogy a sütik elfogadásához hozzájárulást kérjenek, azonban új tájékoztatási követelményeket is tartalmaz, amelyeket a szervezeteknek biztosítaniuk kell az érintettek számára, amikor személyes adatokat gyűjtenek be tőlük. Ez az esetben is alkalmazandó, amikor egy szervezet sütik használatához kapcsolódó hozzájárulást kap. A direkt és interaktív marketing tevékenységet folytató cégeknek ezért felül kell vizsgálniuk a sütik használatához való hozzájárulások gyűjtése során adott tájékoztatásaikat. Az Elektronikus Hírközlési Adatvédelmi Irányelv még 2016 folyamán kerül felülvizsgálatra annak érdekében, hogy harmonizálják a GDPR-ral.

9. Mítosz: „Félszemélyes" cégként nincs szükségünk adatvédelmi tisztviselőre – téves

Az adatvédelmi tisztviselő kötelező alkalmazása nem a szervezet méretétől, hanem a tevékenységétől függ. Ha egy szervezet alaptevékenysége „az érintettek nagymértékű, rendszeres és szisztematikus nyomon követését" foglalja magában vagy „az adatok különleges kategóriáinak (különleges adatok) nagymértékű kezelésével jár", a szervezetnek adatvédelmi tisztviselőt kell kineveznie. A fenti követelmények értelmezéséhez várhatóan a nemzeti adatvédelmi hatóságok adnak majd iránymutatást (lásd a GYIK „Mik az adatvédelmi tisztviselőre vonatkozó követelmények? kérdését)

GYIK

Mi az a GDPR?

Az általános adatvédelmi rendelet („a Rendelet”) egy új EU-s rendelet, amelyet 2016 második negyedévében fogadtak el, és felváltja *a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról* szóló 95/46 Irányelvet („az Irányelv”).

A direkt és interaktív marketing tevékenységet folytató cégek számára lényeges, hogy megértések és betartsák a Rendeletet, mivel ez határozza meg a személyes adatok kezelésének szabályait, valamint az érintett személyek adatvédelmi jogait. A Rendelet az adatvezérelt marketing iparágban használt legtöbb adatra nézve irányadó.

Mi az új a GDPR-ban?

A Rendelet a jelenleg is hatályos adatvédelmi alapelveken alapul, de sokkal részletesebb, mint az Irányelv:

- A Rendelet tárgyi és földrajzi hatálya szélesebb. A személyes adatok meghatározása is bővült. Így több adatkezelési művelet tartozik a Rendelet hatálya alá (lásd: GYIK – „Mi a személyes adat?” lent). A szélesebb földrajzi hatálynak köszönhetően a Rendelet több EU-n kívüli szervezetre alkalmazandó (lásd a GYIK „Kikre vonatkozik a GDPR?” kérdését).
- A Rendelet új jogokat biztosít az érintett személyeknek, például szolgáltatóváltás esetén jogot a személyes adatok továbbvitelére (az adathordozhatósághoz való jog), valamint új kötelezettségeket határoz meg az adatkezeléshez kapcsolódóan, például:
    - az adatvédelmi incidensek bejelentése;
    - az adatvédelem beépítése a projektekbe már az induláskor (beépített adatvédelem);
    - annak biztosítása, hogy már a kiindulási adatvédelmi beállítások blokkolják a kapcsolatfelvételt (alapértelmezett adatvédelem);
    - az új termékeknek és szolgáltatásoknak az érintett személyek adatvédelmi jogaira gyakorolt hatásának vizsgálata (adatvédelmi hatásvizsgálat).
- A Rendelet nagyon részletesen kiterjeszti és pontosítja a szervezetek és az egyének adatvédelmi jogaira vonatkozó jelenlegi kötelezettségeket, például:

- a hozzájárulás egyértelmű kell, hogy legyen, a szervezetek szélesebb körű tájékoztatást kell, hogy adjanak az érintett személyeknek;
- az érintettek „elfeledtetéshez" való joga, ami azt jelenti, hogy szélesebb körben jogosultak személyes adataikat töröltetni).

Az Irányelvvel ellentétben, amely csak elérendő célokat fogalmaz meg a tagállamok számára, így a jogszabály szövegét a tagállamok helyi törvények formájában kellett, hogy átültessék a nemzeti jogba, a Rendelet közvetlenül alkalmazandó az EU minden tagállamában (azaz nincs szükség külön helyi törvényekre az alkalmazásához).

A szervezeteknek 2 éves átmeneti időszak alatt kell biztosítaniuk a Rendeletnek való megfelelést mielőtt az 2018. május 25-ét követően kötelező lesz. A szakmának azonban nem szabad vesztegetnie az időt, és már most el kell kezdenie a munkát a megfelelés érdekében, mivel néhány változás végrehajtása akár a teljes rendelkezésre álló 2 évet is igénybe veheti.

Kikre vonatkozik a GDPR?

A Rendelet az alábbi szervezetekre vonatkozik:

- Az Európai Unióban tevékenységi hellyel rendelkező szervezetekre. Abban az esetben is, ha az adatkezelés az Európai Unión kívül történik, vagy ha a személyes adat nem az Európai Unióban élő személyhez kapcsolódik.
- Az Európai Unióban tevékenységi hellyel nem rendelkező szervezetre akkor is, ha az adatkezelés áruknak vagy szolgáltatásoknak az Európai Unióban való nyújtásához kapcsolódik (ideértve az ingyenes árukat és szolgáltatásokat is), vagy ha ezek a szervezetek egyének viselkedését figyelik meg.

Ennek következtében bármely, az Európai Unióban tevékenységi hellyel rendelkező, vagy az EU-ban árukat vagy szolgáltatásokat kínáló, vagy az EU-ban egyének viselkedését megfigyelő direkt és interaktív marketing tevékenységet folytató cég a GDPR hatálya alá tartozik.

Mit kell tennünk?

A szervezetnek 2 évük van arra, hogy biztosítsák a Rendeletnek való megfelelést. A Rendelet 2018. május 25-ét követően lesz alkalmazandó. A FEDMA azonban azt tanácsolja, hogy a szervezetek a megfeleltetési folyamatokat olyan hamar kezdjék el, amennyire csak lehetséges, mert a Rendelet alapján szükséges egyes változtatások végrehajtásához akár 2 évre is szükségük lehet.

A Rendelet által bevezetett új jogi kötelezettségeknek meg kell felelni, és azok általános gyakorlattá kell, hogy váljanak. A megfelelési folyamat lépései:

- Az adatvédelmi szabályzatok és adatvédelmi tájékoztatók, valamint a szerződéses feltételek felülvizsgálata és frissítése;
- Új technikai és szervezési folyamatok bevezetése (pl. adatvédelmi incidensek kötelező bejelentéséhez);
- A meglévő adatbiztonsági intézkedések felülvizsgálata;
- Az adatkezelési szerződések, valamint az adatfeldolgozókkal, partnerekkel és ügyfelekkel való egyéb megállapodások felülvizsgálata;
- Az Európai Unión kívüli országokba történő nemzetközi adattovábbítások jogalapjának felülvizsgálata.

Az új Rendelet bevezeti ezen kívül az elszámoltathatóság fogalmát is. Ennek alapján a szervezeteknek képeseknek kell lenniük arra, hogy a nemzeti adatvédelmi hatóságoknak bizonyítsák a jogszabályi előírásoknak való megfelelést. A megfelelés az alapelvnek több kötelezettséggel is jár, úgymint:

- A szervezet tevékenysége során az adatvédelem beépítése a projektekbe már az induláskor (beépített adatvédelem);
- Annak biztosítása, hogy már a kiindulási adatvédelmi beállítások blokkolják a kapcsolatfelvételt (alapértelmezett adatvédelem);
- Az adatvédelmi szabályzatok és eljárások dokumentálásának kötelezettsége.

Mi a személyes adat?

A Rendelet úgy határozza meg a személyes adatot, mint *„azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható”.*

A Rendelet megállapítja, hogy egyes „online” adatok személyes adatnak minősülhetnek, például az online azonosítók, helymeghatározó adatok, azonosító számok (pl. eszközazonosítók, süti azonosítók, IP-címek és rádiófrekvenciás azonosító címkék). Az új Rendelet szövegének fényében jogi szempontból először azt kell megvizsgálni, hogy a digitális formában kezelt adatok személyes adatnak minősülnek-e. Egyértelmű például, hogy az internetszolgáltatók által tárolt statikus IP-cím személyes adat, mert alkalmas az érintett azonosítására. Az

azonban csak a későbbi joggyakorlatból derül majd ki, hogy a böngészők vagy eszközök által használt azonosítók személyes adatnak minősülnek-e, ha egy azonos érdeklődési körrel rendelkező csoport tagjaként azonosítanak egy érintett személyt, de őt magát egyértelműen nem.

Mit jelent a személyes adatok álnevesítése?

A Rendelet új koncepcióként vezeti be az álnevesítést. Az adatok álnevesítése csökkenti az egyének számára az adatvédelmi kockázatot, mivel ennek során a személyes adatokat adatbiztonságot fokozó technikákkal kezelik (pl. egy irányú kivonatolás), így az egyén többé már nem azonosítható kizárólag a létrejött adathalmazból. Az álnevesített adat kiegészítő információ – mint például egy kulcs – segítségével újra azonosíthatóvá válik.

Bár még mindig a személyes adat egyik formájaként, de a Rendelet rugalmasabban kezeli az álnevesített adatot. Álnevesített adatok használatával a direkt és interaktív marketing tevékenységet folytató cégek például könnyebben végezhetnek profilalkotást, valamint rugalmasabban határozhatják meg, használható-e az adat az adatgyűjtés céljától eltérő célra. Az adatvédelemnek a projektbe már az induláskor való beépítésével (beépített adatvédelem), továbbá már a kiindulási adatvédelmi beállítások kapcsolatfelvétel blokkolása céljából való meghatározásával (alapértelmezett adatvédelem) kapcsolatos kötelezettségeknek történő megfelelés során az álnevesítést figyelembe kell venni. A FEDMA ezért arra ösztönzi tagjait, hogy ahol ez megvalósítható, vizsgálják meg, tudják-e álnevesíteni az általuk kezelt személyes adatokat, és ha igen, használják ki a Rendelet által az álnevesített személyes adatok kezelésével kapcsolatban biztosított előnyöket.

Mik az adatvédelmi alapelvek?

A Rendelet a személyes adatok kezeléséhez kapcsolódóan alapelveket határoz meg, amelyek nagyon hasonlóak az Irányelvben foglaltakhoz.

Ezek szerint:

(1) a személyes adatok kezelését jogszerűen, tisztességesen és az egyének számára átlátható módon kell végezni (**jogszerűség, tisztességes eljárás és átláthatóság**);

(2) a személyes adatok gyűjtése meghatározott egyértelmű és jogszerű célból kell, hogy történjen, és nem kezelhetők ezekkel a célokkal össze nem egyeztethető módon (**célhoz kötöttség**);

(3) a személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk (**adattakarékosság**);

(4) a személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük (**pontosság**);

(5) a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé (**korlátozott tárolhatóság**);

(6) a személyes adatok kezelését úgy kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítani lehessen a személyes adatok megfelelő biztonságát (**integritás és bizalmas jelleg**).

Hogyan kezelhetünk személyes adatokat?

A direkt és interaktív marketing tevékenységet folytató cégek akkor gyűjthetnek és kezelhetnek személyes adatokat, ha az adatkezelést a Rendeletben leírt jogalapok valamelyike alapján végzik. A Rendelet ugyanazt a 6 jogalapot határozza meg, mint az Irányelv.

Ezek a jogalapok a következők:

- az érintett hozzájárulása,
- az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél,
- az adatkezelés a szervezetre vonatkozó Európai Uniós jogból vagy tagállami jogból származó kötelezettség teljesítéséhez szükséges,
- az adatkezelés az érintett létfontosságú érdekeinek védelme miatt szükséges,
- az adatkezelés közérdek vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges,
- az adatkezelés az adatkezelő vagy harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

Az adatvezérelt marketingtevékenységek során a személyes adatok kezelésére a leginkább alkalmazható és a legtöbbet használt jogalap az érintett személy hozzájárulása, illetve az adatkezelő vagy harmadik fél jogos érdekeinek érvényesítése.

Mi jelent érvényes hozzájárulást a személyes adatok gyűjtéséhez?

A Rendelet alapján a hozzájárulásnak:

- **önkéntesnek,**
- **konkrétnak,**
- **megfelelő tájékoztatáson alapulónak**
- **és egyértelműnek**

kell lennie.

A hozzájárulás fogalma majdnem teljesen azonos alapelvekre épül, mint az Irányelvben, a Rendelet azonban tisztázza, hogy mi számít *érvényes* hozzájárulásnak. Az egyéneknek nyilatkozattal vagy a megerősítést félreérthetetlenül kifejező cselekedet útján kell kifejezniük akaratukat.

A direkt és interaktív marketing tevékenységet folytató cégek rugalmasak kell, hogy maradjanak a hozzájárulások gyűjtésekor, azonban nem szabad szem elől téveszteniük azt a jogszabályi követelményt, hogy adatkezelési tevékenységükről már az adatok gyűjtése során elegendő információt kell, hogy biztosítsanak az érintettek számára. A tájékoztatási követelmények a Rendelet III. fejezetének 2. szakaszában kerültek meghatározásra, és attól függően változnak, hogy a személyes adatot az érintett személytől közvetlenül vagy nem közvetlenül gyűjtötték-e. A tájékoztatást tömör, átlátható és érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell nyújtani.

Az elszámoltathatóság alapelvének részeként a direkt és interaktív marketing tevékenységet folytató cégeknek bármikor képeseknek kell lenniük a Rendeletnek való megfelelés igazolására a nemzeti adatvédelmi hatóságok felé. A bizonyítási terhet a szervezetek viselik, és ha a személyes adatok kezelésének jogalapja a hozzájárulás, akkor megfelelő bizonyítékot kell szolgáltatniuk a hozzájárulás megszerzésére.

A Rendelet megerősíti a gyermekek jogainak védelmét. Az adatvezérelt direkt és interaktív marketing tevékenységet folytató cégeknek igazolniuk kell, hogy ésszerű erőfeszítéseket tettek annak ellenőrzése érdekében, hogy a hozzájárulást a 13 és 16 év közötti gyermek esetében a felette szülői felügyeleti jogot gyakorló adta meg. Az egyes tagállamok az erre vonatkozó szabályozásban 16 évnél alacsonyabb, de 13 évnél nem alacsonyabb életkort is meghatározhatnak.

Lehet-e adatokat kezelni marketing céllal a szervezet jogos érdeke alapján (leiratkozás, opt-out)?

A személyes adatok kezeléséhez a direkt és interaktív marketing tevékenységet folytató cégek számára a Rendelet alapján rendelkezésre áll egy másik jogalap is: a jogos érdek. Az Irányelv alapján ezt a jogalapot a cégek a postai úton történő direkt marketing céljából alkalmazzák. A Rendelet egyértelművé teszi azt, hogy a „személyes adatok közvetlen üzletszerzési célú kezelése szintén jogos érdeken alapulónak tekinthető".

A direkt és interaktív marketing tevékenységet folytató cégeknek mérlegelniük kell a személyes adatok kezeléséhez kapcsolódó érdekeiket és az érintett személyeknek a Rendelet alapján fennálló jogait. Az érdekmérlegelési teszt eredménye határozza meg, hogy kezelhető-e a személyes adat hozzájárulás nélkül. A jelenlegi Irányelv alapján fennálló gyakorlat azt valószínűsíti, hogy az érintett személyek jogai biztosíthatók a direkt marketing küldeményekről történő – az adat gyűjtésének időpontjában gyakorolható – leiratkozási (opt-out) jogaik postai úton történő lehetővé tételével, valamint annak ellenőrzésével, hogy az érintett korábban megtiltotta-e adatai kezelését, vagy szerepel-e valamilyen Robinson listán.

A direkt és interaktív marketing tevékenységet folytató cégeknek más csatornákon keresztül történő marketingtevékenység megkezdése előtt egyéb jogszabályok általános rendelkezései – például az Elektronikus Hírközlési Adatvédelmi Irányelv – szerint is be kell szerezniük az érintett személy hozzájárulását. Az Elektronikus Hírközlési Adatvédelmi Irányelv például általánosságban megköveteli a direkt és interaktív marketing tevékenységet folytató cégektől, hogy direkt marketing célú email kiküldése előtt szerezzék meg az érintett hozzájárulását. A Rendelet ezeken a specifikus szabályokon nem változtat.

A fentieken túlmenően a direkt és interaktív marketing tevékenységet folytató cégek a személyes adatoknak a Rendeletben meghatározott különleges kategóriáit, melyeket az Irányelv különleges adatnak nevez (például politikai véleményekre, faji vagy etnikai hovatartozásra és egészségi állapotra vonatkozó adatok) kizárólag az egyén kifejezett hozzájárulásával kezelhetik.

Milyen tájékoztatást kell adni az érintett számára?

Az érintett személyek adatai kezelésével kapcsolatos átláthatóság növelése érdekében a GDPR előírja, hogy a szervezetek személyes adatok gyűjtésekor milyen információkról kötelesek az érintett személyeket tájékoztatni.

A szervezeteknek tájékoztatniuk kell az érintett személyeket a Rendelet III. fejezetének 2. szakaszában meghatározott információkról. Az érintett személyek számára rendelkezésre bocsátott információkkal kapcsolatos követelmények attól függően változnak, hogy a személyes adatokat közvetlenül az érintettől gyűjtötték-e vagy nem. A tájékoztatást az adatgyűjtés időpontjában vagy az első adattovábbításkor kell megadni az érintett részére. A GDPR megállapítja, hogy a tájékoztatásnak könnyen hozzáférhetőnek és közérthetőnek kell lennie, de nem tér ki arra, hogy milyen formában kell az információt rendelkezésre bocsátani. Ezzel kapcsolatban további iránymutatásra számítunk a nemzeti adatvédelmi hatóságok részéről.

Az adatvédelmi értesítésnek az alábbi **információkat** kell tartalmaznia:

- a direkt és interaktív marketing tevékenységet folytató cég **kiléte**, elérhetőségi adatokkal és az adatkezelés **céljával és jogalapjával**,
- információt az **érintett jogairól** (helyesbítéshez való jog, törléshez való jog, tiltakozáshoz való jog, adathordozhatósághoz való jog),
- azon **címzettek** vagy címzettek kategóriái, akikkel a személyes adatokat közölték,
- ha az adatkezelés a szervezet jogos érdekein alapszik, melyek ezek a **jogos érdekek**,
- ha az adatkezelés kifejezett hozzájáruláson alapszik, az egyének azon joga, hogy **visszavonhatják a hozzájárulást**,
- információ a **nemzetközi adattovábbításról**, ideértve a megfelelően nyújtott garanciákat,
- a személyes adatok tárolásának **időtartama**,
- a felügyeleti hatósághoz címzett **panasz** benyújtásának joga,
- **automatizált döntéshozatal** ténye (profilalkotás),
- a személyes adatok gyűjtésének eredeti céljától eltérő célból történő **további adatkezelés** szándéka.

Ha egy szervezet nem közvetlenül az érintettől szerzi meg a személyes adatot, a fenti információkon túl az érintettet tájékoztatni kell a kezelt adatok kategóriájáról és az adatok forrásáról – ésszerű határidőn belül vagy legalább az érintettel való első kapcsolatfelvétel alkalmával.

Fontos, hogy az adatvédelmi tájékoztató naprakész és könnyen hozzáférhető legyen. Az online adatvédelmi tájékoztatóra mutató linknek mindenhol elérhetőnek kell lennie, ahol az adatkezelő adatot gyűjt, például belépő oldalakon, online regisztrációs nyomtatványokon, stb.

Mi az adattörléshez való jog („az elfeledtetéshez való jog")?

A Rendelet lehetővé teszi az érintett személyek számára, hogy meghatározott esetekben kérjék adataik törlését. Az adattörléshez való jog, más néven az elfeledtetéshez való jog a Rendelet III. fejezetének 3. szakaszában felsorolt helyzetekben és korlátozásokkal alkalmazandó. A direkt és interaktív marketing tevékenységet folytató cégeknek nem kell törölniük a személyes adatokat, ha azokat nyilvántartási célokból meg kell őrizniük, például könyvviteli, adózási vagy más külső szabályozási követelmények miatt.

A direkt és interaktív marketing tevékenységet folytató cégeknek alaposan meg kell fontolniuk, hogy a személyes adatot törlik, vagy megőrzik saját belső Robinson-listájukon. Ha az érintett személy kéri a személyes adatainak törlését, mert a továbbiakban nem szeretne direkt marketing üzenetet kapni a szervezettől, a személyes adatok törlése helyett a szervezetnek inkább hozzá kell adnia az érintett személy kapcsolattartási adatait a saját belső Robinson-listájához. Ha a szervezet teljesen törli az érintett személy személyes adatait, akkor fennáll annak a veszélye, hogy a jövőben újabb direkt marketing üzenetet küld, pedig az érintett éppen ezt nem szerette volna. Ha azonban az érintett személyek adatai a szervezet saját belső Robinson listájára kerülnek, akkor a szervezet a jövőben nem fog semmilyen egyéb direkt marketing üzenetet küldeni az érintett személyek számára. A Rendelet szerint a szervezetek jogosultak a fentiek szerint eljárni.

A szervezetek meg kell, hogy tegyék az ésszerűen elvárható lépéseket annak érdekében, hogy tájékoztassák azokat a harmadik feleket, amelyeknek a személyes adatok átadásra kerültek. A direkt és interaktív marketing tevékenységet folytató cégeknek csak akkor kell tájékoztatniuk a harmadik feleket az érintett személyek adattörlési kérelméről, ha ez az elérhető technológia és a megvalósítás költségeinek figyelembevételével ésszerűen elvárható, és a cég nem felelős azért, hogy a harmadik fél szervezet törli-e az adatokat vagy sem.

Ha a személyes adatokat anonimizálták, az érintett személy nem jogosult kérni a korábban hozzá kapcsolt adatok törlését.

Mi az adathordozhatósághoz való jog?

A Rendelet új jogot biztosít az érintett személyek számára: az adathordozhatósághoz való jogot. Eszerint az érintett személy jogosult megkapni azokat az adatait, amelyek szolgáltatóváltásához szükségesek, különösen az online világban.

A szervezetnek az érintett kérésére át kell adnia az érintett számára „a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat". A személyes adatokat „tagolt, széles körben használt, géppel olvasható formátumban" kell átadni. Ezért az érintett személy kérheti, hogy személyes adatai közvetlenül egy másik szervezetnek kerüljenek továbbításra.

Az adathordozhatósághoz való joghoz két korlátozás kapcsolódik:

- csak olyan személyes adatra vonatkozik, amelyet automatizált módon kezelnek,
- csak akkor alkalmazandó, ha a személyes adatok kezelése a felhasználó hozzájárulásán vagy a szerződés teljesítése érdekében történik. Ennek következtében az adathordozhatósághoz való jog nem vonatkozik a „jogos érdek" alapján személyes adatokat kezelő direkt és interaktív marketing tevékenységet folytató cégekre.

Mi a tiltakozáshoz való jog (a leiratkozáshoz való jog / opt-out)?

A Rendelet biztosítja az érintett személyek számára a jogot, hogy tiltakozzanak a személyes adataik kezelése ellen, vagyis hogy leiratkozási (opt-out) jogaikat gyakorolják adataik felhasználásával kapcsolatban. Ez a jog már a jelenlegi Irányelv alapján is létezik. A Rendelet azonban az érintett személyek számára megkönnyíti a tiltakozáshoz való jog gyakorlását.

Ha a személyes adatot direkt marketing célokra használják, az érintett személyeknek joguk van tiltakozni a személyes adataik ilyen célú kezelése ellen. A Rendelet kifejezetten rögzíti, hogy a tiltakozáshoz való jog direkt marketing tevékenységekhez kapcsolódó profilalkotási tevékenységekre is vonatkozik. Ha az érintett személyek leiratkoznak (opt-out jogaikat gyakorolják) a direkt marketinggel kapcsolatban, a direkt és interaktív marketing tevékenységet folytató cégnek abba kell hagynia a direkt marketing célokra történő adatkezelést, és az egyén elérhetőségeit hozzá kell adnia saját, belső Robinson-listájához.

A szervezeteknek, különösen a direkt és interaktív marketing tevékenységet folytató cégeknek tájékoztatniuk kell az érintetteket a személyes adataik kezeléséhez kapcsolódó tiltakozási jogukról. A tiltakozási jogra vonatkozó

tájékoztatásnak egyértelműnek és a szervezetek által az érintett személyeknek nyújtott más információktól elkülönültnek kell lennie.

Mik a profilalkotásra vonatkozó új szabályok?

A Rendelet bevezet néhány újdonságot a profilalkotással kapcsolatosan, miközben megtartja a korábbi alapelvet: az érintett személyek számára meg kell adni a lehetőséget, hogy tiltakozzanak a profilalkotással szemben, azaz az erről való leiratkozással (opt-outtal).

A Rendelet a profilalkotást személyes adatok automatizált kezeléseként határozza meg, amely személyes jellemzők kiértékelésére szolgál, különösen, ha az érintett személy személyes jellemzőinek elemzésére vagy előrejelzésére kerül sor. Adatvezérelt marketing során minden bizonnyal profilalkotásnak minősül egy algoritmus adatelemzési célú használata, ha célja annak megállapítása, hogy egy érintett személy vagy érintett személyek kategóriája egyes terméktípusok vagy szolgáltatástípusok iránt érdeklődik-e, hajlandó-e egy bizonyos terméket megvásárolni, bizonyos módon viselkedik-e, vagy meghatározott helyeken tartózkodik-e. Adatvezérelt marketing során az érintett személynek joga van kérni a direkt marketing célokból történő profilalkotás megszüntetését.

Amikor egy szervezet a direkt marketing célú profilalkotási tevékenységen túlmenően profilalkotási tevékenységet végez, figyelembe kell vennie a profilalkotás alapján hozott döntésének az egyénre kifejtett hatását. Ha a profilalkotás alapján hozott döntés „joghatással bír”, vagy „jelentős mértékben érint” egyes személyeket, az érintett személynek joga van a profilalkotás megszüntetését kérni (opt-out jogait gyakorolni). Az érintett személyek nem jogosultak erre, ha:

(1) a profilalkotás az érintett és a szervezet közötti szerződés megkötése vagy teljesítése érdekében szükséges,

(2) a profilalkotást Európai Uniós jog vagy tagállami jog lehetővé teszi,

(3) a profilalkotás az érintett kifejezett hozzájárulásán alapul.

A Rendelet az érintett személyekre joghatással bíró vagy jelentős mértékben érintő tevékenységekre példaként egy online hitelkérelem automatikus elutasítását vagy emberi beavatkozás nélkül folytatott online munkaerő-toborzást említi.

A profilalkotás szabályainak véglegesítésére a Rendelet elfogadásának egyik utolsó lépéseként került sor, ezért a „joghatással bír” és „jelentős mértékben érint” kifejezések jelentésének értelmezéséhez a nemzeti adatvédelmi hatóságok iránymutatására lesz szükség.

Mit mond a Rendelet az adatvédelmi hatásvizsgálatról?

Személyes adatok kezelésének megkezdése előtt az adatkezelő szervezetnek meg kell határoznia, hogy az adatkezelés az érintett személyek számára mikor járhat valószínűsíthetően magas kockázattal. Ha a szervezet az adatvédelmi hatásvizsgálat elvégzését követően úgy véli, hogy az adatkezelés magas kockázattal jár, akkor az adatkezelés megkezdését megelőzően egyeztetnie kell a nemzeti adatvédelmi hatósággal. A nemzeti adatvédelmi hatóság az adatkezeléssel kapcsolatban konzultál az adatkezelővel.

A Rendelet tisztázza, hogy az érintett személyekre joghatással járó profilalkotás, valamint a személyes adatok különleges kategóriáinak (melyeket az Irányelv különleges adatnak nevez) nagy számban történő kezelése nagy kockázattal járó adatkezelésnek tekintendők, és ilyenkor az adatvédelmi hatásvizsgálat elvégzése kötelező. A nemzeti adatvédelmi hatóságok listát készítenek a magas kockázatúnak minősülő adatkezelési tevékenységekről.

A Rendelet az adatvédelmi hatásvizsgálat elemeit az alábbiak szerint határozza meg:

- a tervezett adatkezelési műveletek módszeres leírása és az adatkezelés céljainak ismertetése;
- az adatkezelés céljait figyelembe véve az adatkezelési műveletek szükségességének és arányosságának vizsgálata;
- az érintett személyeket érintő kockázatok vizsgálata;
- a szervezetnek az érintett személyeket érintő adatkezelési tevékenységgel okozott adatvédelmi kockázatok csökkentésére vonatkozó javaslata (pl. további adatbiztonsági intézkedések a kezelt személyes adatok védelme érdekében).

Mik az adatvédelmi tisztviselőre vonatkozó követelmények?

A Rendelet egyes szervezetek számára kötelezően előírja az adatvédelmi tisztviselő (*Data Protection Officer* – „*DPO*”) kinevezését.

A szervezetnek adatvédelmi tisztviselőt kell kineveznie, ha fő tevékenységei „érintettek rendszeres és szisztematikus, nagymértékű megfigyelését” vagy „adatok különleges kategóriáinak nagy számban történő kezelését” foglalják magukban. Az Irányelv az utóbbiakat különleges adatnak nevezi (faji, etnikai hovatartozásra, politikai véleményre, vallási vagy lelkiismereti meggyőződésre, szakszervezeti tagságra vonatkozó adatok, valamint genetikai adatok stb.). A DPO

lehet az adatkezelő vagy az adatfeldolgozó alkalmazottja, illetve szolgáltatási szerződés keretében is elláthatja a feladatait. Adatvezérelt marketinggel kapcsolatos tevékenységekkel összefüggésben a nagy fogyasztói adatbázissal rendelkező direkt és interaktív marketing tevékenységet folytató cégek valószínűsíthetően ki fognak nevezni DPO-t. Az „érintettek rendszeres és szisztematikus, nagymérték megfigyelésének" fogalom értelmezéséhez várhatóan a nemzeti adatvédelmi hatóságok adnak iránymutatást.

„Az adatvédelmi jog és gyakorlat szakértői szintű ismeretével" rendelkező DPO mind európai, mind nemzeti szinten felelős a Rendeletnek való megfelelésért, tájékoztatja a szervezetet a Rendelet szerinti kötelezettségeiről, tájékoztatást ad az adatvédelmi hatásvizsgálat elvégzésének időpontjáról és módjáról, valamint a nemzeti adatvédelmi hatóságoktól érkező megkeresések, illetve az érintett személyektől érkező megkeresések és adathozzáférési kérések esetén a szervezet kapcsolattartójaként szolgál.

A DPO vagy a szervezet alkalmazottja (két évre kell kinevezni és ez alatt az idő alatt felmondási tilalom védi) vagy külső szolgáltató (tanácsadó, ügyvédi iroda). A DPO rendelkezik „a feladat végrehajtásához szükséges forrásokkal" és „közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének tartozik felelősséggel".

Ha a szervezetnek a Rendelet szerint nem kötelező DPO-t kineveznie, a Rendeletnek való megfelelési kötelezettség teljesítésének segítése érdekében önkéntesen is kinevezhet egyet.

Mi az az „Egyablakos Ügyintézés"?

Az „Egyablakos Ügyintézés" koncepciója lehetővé teszi az egy vagy több tagállamban létrehozott szervezetek számára, hogy legyen egy fő felügyeleti hatóságuk, amely elsődlegesen eljár velük kapcsolatosan. A fő felügyeleti hatóság azon ország adatvédelmi hatósága, ahol a szervezet marketing tevékenységét végzi.

Például ha egy páneurópai szervezet marketing tevékenységét az Egyesült Királyságból végzi, akkor a szervezet marketing tevékenységeit illetően az Egyesült Királyság adatvédelmi hatósága lehet a fő felügyeleti hatóság. Ha az Egyesült Királyságbeli szervezet marketing anyagokat küldött egy francia állampolgárnak és a francia állampolgár szerint ez a Rendeletbe ütközik, akkor a francia állampolgár panasszal élhet a francia nemzeti adatvédelmi hatóságnál. A francia nemzeti adatvédelmi hatóság a panaszt továbbítja az Egyesült Királyság nemzeti adatvédelmi hatóságának. A francia nemzeti adatvédelmi hatósággal való egyeztetést követően a panasszal kapcsolatos végleges döntést az Egyesült Királyságbeli nemzeti adatvédelmi hatóság hozza meg. Ha a panasz a Rendelet szerint egy átfogóbb jogi kérdést érint, akkor az Egyesült Királyság nemzeti

adatvédelmi hatósága az ügyet az egyes nemzeti adatvédelmi hatóságok képviselőiből álló Európai Adatvédelmi Testülethez utalhatja.

A többi ország nemzeti adatvédelmi hatóságaival való egyeztetést, az Európai Adatvédelmi Testülethez fordulást, valamint az egyes nemzeti adatvédelmi hatóságok közötti véleménykülönbség feloldását összetett eljárásrend szabályozza. Ez a Rendelet VII. fejezetében részletezett ún. egységességi mechanizmus.

Milyen új szabályok vonatkoznak a nemzetközi adattovábbításokra?

A személyes adatok Európai Unión belüli továbbításával szemben a Rendelet nem támaszt többletfeltételt. Az Irányelvhez hasonlóan a Rendelet lehetővé teszi az adatok az Európai Unión kívüli harmadik országokba történő továbbítását is, feltéve, hogy a személyes adatokat megkapó országban biztosítják a személyes adatok védelmének megfelelő szintjét.

Az Európai Bizottság jogosult eldönteni, hogy egy Európai Unión kívüli harmadik ország mikor biztosítja a személyes adatok védelmének megfelelő szintjét. A Bizottság azt is eldöntheti, hogy „a harmadik ország valamely területe, illetve egy vagy több meghatározott ágazata" megfelelő adatvédelmi szintet biztosít-e.

Az Irányelv szerint a Bizottság jelenleg 11 országban minősítette az adatvédelmet valamilyen módon megfelelőnek.

A Bizottság megfelelőségi döntése hiányában a Rendelet megfelelő garanciák ellenében engedélyezi az adatok nemzetközi továbbítását, „de csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre" az Európai Unión kívüli harmadik országban.

A Rendelet számos megoldást elismer az Európai Unión kívüli nemzetközi adattovábbítások esetében, például:

- Nemzeti adatvédelmi hatóságok jóváhagyásához kötött, kötelező erejű vállalati szabályok. Ezek csak nagy szervezetek részére megfelelőek, mivel a jóváhagyási folyamatuk jogi és adminisztrációs szempontból egyaránt összetett, és akár 2 évig is eltarthat.
- Általános adatvédelmi klauzulák, más néven általános szerződési feltételek / adattovábbítási modellszerződések (SCCk). Ezek váltják fel az Irányelv szerinti Adattovábbítási Modellszerződéseket (*Model Contract Clauses*). Annak ellenére, hogy a Bizottság korábbi határozataiban már engedélyezte az Adattovábbítási Modellszerződések használatát, az Irányelv alapján néhány nemzeti adatvédelmi hatóság ragaszkodott az Adattovábbítási Modellszerződések jóváhagyásához, mielőtt az adott cég azokat az EU-n kívüli harmadik országokba való adattovábbítás alapjaként használta volna. A Rendelet szerint azonban az SCCk használatához nem szükséges a nemzeti adatvédelmi hatóságok előzetes jóváhagyása.
- Jóváhagyott magatartási kódex vagy jóváhagyott tanúsítási mechanizmus – a személyes adatokat az EU-n kívüli harmadik országokban megkapó szervezet kötelező és kikényszeríthető kötelezettségvállalásával.

A Bizottság megfelelőségi döntésének vagy megfelelő garanciák hiányában egy szervezet továbbra is továbbíthat személyes adatot egy harmadik országban lévő szervezet részére az alábbi feltételek szerint:

- Az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő esetleges kockázatokról.
- Az adattovábbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges.
- Az adattovábbítás az adatkezelő és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges.
- Egyszeri vagy nem rendszeres adattovábbítás történhet az EU-ban letelepedett szervezet jogos érdeke alapján, amíg az adattovábbítás nem ismétlődő, csak korlátozott számú érintettre vonatkozik és megfelelő garanciák kerültek alkalmazásra. Ilyen jellegű adattovábbítás esetén az EU-ban letelepedett szervezetnek tájékoztatnia kell a saját nemzeti adatvédelmi hatóságát az adattovábbításról.

Mik az új adatbiztonsági kötelezettségek?

A Rendelet a jelenlegi Irányelvhez hasonló adatbiztonsági követelményeket tartalmaz. „A szervezeteknek és a kiszervezett szolgáltatást nyújtóknak a kockázat mértékének megfelelő szintű adatbiztonság biztosítása érdekében megfelelő technikai és szervezési intézkedéseket kell végrehajtaniuk.” A Rendelet lehetővé teszi a szervezetek számára, hogy a szükséges biztonsági intézkedések előzetes felmérése során figyelembe vegyék „a tudomány és technológia állását és a megvalósítás költségeit”, valamint a kockázat alapú megközelítés részeként az adatkezeléshez kapcsolódó szempontokat. Az Irányelvben előírtakhoz hasonlóan a direkt és interaktív marketing tevékenységet folytató cégeknek biztosítaniuk kell a személyes adatok kezelésének védelme érdekében megfelelő adatbiztonsági intézkedéseket. Az adatbiztonsági intézkedéseknek az adatkezelés során az érintett személyekkel kapcsolatban esetlegesen felmerülő kockázat szintjével arányosnak kell lenniük.

A Rendelet számos adatbiztonsági intézkedés foganatosítását javasolja:

- a személyes adatok álnevesítését és titkosítását;
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenállóképességét;

- fizikai vagy műszaki incidens esetén a képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen állítani;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárások alkalmazását.

A Rendelet adatbiztonsági megközelítése összekapcsolódik az új kötelezettségekkel, melyek célja az adatvédelem beépítése a projektekbe már az induláskor (beépített adatvédelem), továbbá annak biztosítása, hogy a kiindulási adatvédelmi beállítások blokkolják a kapcsolatfelvételt (alapértelmezett adatvédelem), valamint annak biztosítása, hogy új projektek az érintett személyek adatvédelmi jogaira gyakorolt hatásának felmérésére hatásvizsgálatokat végezzenek (adatvédelmi hatásvizsgálat).

Az adatkezelési tevékenységekkel kapcsolatban mind a szervezeteket, mind a kiszervezett szolgáltatást nyújtókat adatbiztonsági kötelezettségek terhelik. A Rendelet egyértelművé teszi, hogy a „az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak megfelelő technikai és szervezési intézkedések végrehajtására”. Ezek a jelenlegi Irányelvhez hasonló követelmények.

Mik az új szabályok adatvédelmi incidens esetén?

A Rendelet az adatvédelmi incidens fogalmát meglehetősen széles körűen határozza meg („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 incidens meghatározása nem veszi figyelembe, hogy az incidens maga kárt okozott-e az egyénnek vagy nem.

Adatvédelmi incidens esetén a szervezeteknek tájékoztatniuk kell saját nemzeti adatvédelmi hatóságukat indokolatlan késedelem nélkül, de legkésőbb 72 órával azután, hogy az adatvédelmi incidens ténye a tudomásukra jutott. Ha a szervezet a megadott határidőn belül nem jelenti be az adatvédelmi incidenst a nemzeti adatvédelmi hatóságnak, akkor az esetleges bejelentés alkalmával a bejelentéshez mellékelni kell a késedelem igazolására szolgáló indokokat is. A Rendelet meghatározza, hogy a szervezeteknek milyen tájékoztatást kell adniuk a nemzeti adatvédelmi hatóságok számára adatvédelmi incidens esetén.

A szervezeteknek „indokolatlan késedelem nélkül” tájékoztatniuk kell az adatvédelmi incidenssel érintett személyeket az incidensről, „ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve”. A tájékoztatásban „világosan és közérthetően

ismertetni kell az adatvédelmi incidens jellegét" és tartalmaznia kell az alábbi információkat:

(1) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit, ahol az érintett további információkat tud szerezni az incidensről;

(2) ismertetni kell az adatvédelmi incidensből eredően valószínűsíthető következményeket;

(3) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő, az érintett egyénekre hatással lévő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

A szervezetnek *nem* kell tájékoztatnia az érintett személyeket, ha:

- a szervezet megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre az adatvédelmi incidens által érintett adatok tekintetében, mint például titkosítás alkalmazása;
- a szervezet az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az említett magas kockázat a továbbiakban valószínűsíthetően ne valósuljon meg;
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosság útján kell tájékoztatni, például hirdetés formájában.

Mit jelent az elszámoltathatóság alapelve?

Az új Rendelet bevezeti az elszámoltathatóság alapelvét, ami elvárja a szervezetektől, hogy a nemzeti adatvédelmi hatóságok felé bármikor képesek legyenek igazolni a Rendeletnek való megfelelésüket. Például a Rendelet eltörli az Adatvédelmi Nyilvántartásba való bejelentkezés kötelezettségét, de a szervezeteknek a Rendelet értelmében továbbra is meg kell őrizniük az Adatvédelmi Nyilvántartásba való bejelentkezési kötelezettségek teljesítése során a nemzeti adatvédelmi hatóságoknak korábban elküldött dokumentumok másolatait. A nemzeti adatvédelmi hatóság bármikor betekintést kérhet ezekbe a dokumentumokba.

Külön köszönet

- FEDMA Data Protection Working Group
- Mr. Olivier Proust (Fieldfisher) – az Általános Adatvédelmi Rendelet szerinti profilalkotás koncepciójához fűzött észrevételéért
- CMS Cameron McKenna LLP Magyarországi Fióktelepe: Domokos Márton és Seres Márk – a magyar fordításért és szakmai lektorálásért