Szilágyi Szabolcs 2018.02.01.

Megkezdődött a visszaszámlálás a GDPR bevezetéséig!

Nem egészen négy hónap maradt az új, európai uniós szintű adatvédelmi szabályozás bevezetéséig. Itt az idő foglalkozni a kérdéssel!

Tavaly májusban a *Gartner* meglehetősen lesújtó képet festett a vállalatok GDPR-felkészültségi szintjéről: a piackutató előrejelzése szerint az érintett szervezetek fele még 2018 végén sem fog megfelelni a 2018. május 25-én életbe lépő *General Data Protection Regulation* irányelveinek. Pedig a szabályok be nem tartása esetén a hatóságok 20 millió euró vagy a jogsértés előtti pénzügyi év teljes világpiacon szerzett árbevételének 4 százalékát kitevő is a nyakukba varrhatnak.

Az új adatvédelmi törvényt minden szervezetnek alkalmazni kell, amely az Európai Unió – így Magyarország – területén személyes adatokat kezel. Márpedig ez minden cégre igaz. Itt vannak tehát az utolsó pillanatok, amikor még büntetés nélkül lehet korrigálni az elmaradást.

Az adatkezelés feltételei

Bár lapunkban is rengeteget foglalkoztunk a témával, érdemes újra és újra átismételni, hogy ki vagy mi minősül adatkezelőnek. A rendelet betűje szerint az a természetes személy vagy szervezet, aki vagy amely az adatkezelés célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza, adatkezelőnek minősül. Egy adatbázist több adatkezelő közösen is kezelhet.

A személyes adatok bármilyen jellegű kezelése tekintetében az adatkezelő hatáskörét és felelősségét szabályozni kell. Az adatkezelő kötelezett a megfelelő és hatékony intézkedések végrehajtására, valamint, hogy igazolja az adatkezelési tevékenységek és hatékonyságuk GDPR-nak való megfelelését. Ennek keretei között minimálisra kell csökkenteni a személyes adatok kezelését, a lehető leghamarabb álnevesíteni kell azokat, biztosítani kell átláthatóságukat, valamint azt, hogy az érintett nyomon követhesse az adatkezelést, az adatkezelő pedig biztonsági elemeket hozhasson létre és továbbfejleszthesse azokat.

Az adatkezelő köteles nyilvántartást vezetni a hatásköre alapján végzett adatkezelési tevékenységekről, melynek tartalmaznia kell többek között a (közös) adatkezelő nevét és elérhetőségét, valamint természetesen az adatkezelés céljait. Emellett köteles a felügyeleti hatósággal együttműködni és ezeket a nyilvántartásokat kérésre hozzáférhetővé tenni az ellenőrzés érdekében.

A GDPR azt az esetet is tisztázza, amikor az adatkezelést az adatkezelő nevében más végzi. Ilyen esetben az adatkezelő kizárólag a megfelelő garanciákat nyújtó adatfeldolgozókat vehet igénybe.

De hol vannak az adatok?

Gyakran elkövetett hiba, hogy a szervezet az általa kezelt adatok felmérése során csak az olyan triviális ügyfélinformáció-forrásokat veszi figyelembe, mint például a CRM- vagy a marketingrendszerek. Ennél ugyanakkor jóval sokrétűbbek lehetnek az adattárolási források. Gondoljunk például az okostelefonokra, mobil adattárolókra (pendrive-ok, külső merevlemezek), hálózati mappákra, archivált postafiókokra, közösségi hálózatokon tett megosztásokra, felhőben tárolt adatokra, leselejtezett IT-eszközökre, kinyomtatott dokumentumokra – a sor még sokáig folytatható.

Noha az új uniós rendelet nem szabályozza explicit módon az adattárolás technikáját, azt előírja, hogy az alkalmazott módszerek az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig tegyék lehetővé. A GDPR teljesítéséhez viszont módszertől függetlenül gondoskodni kell a személyes adatok megfelelő biztonságáról, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („integritás és bizalmas jelleg").

Biztonság: általános elvek, nem konkrétumok

Az adatkezelőnek az előírás szerint megfelelő technikai és szervezési intézkedéseket kell végrehajtani annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja. Ezt nem csak a személyes adatok álnevesítése és titkosítása során szükséges megtenni, hanem gondoskodni kell a rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosításáról is.

Értékelni kell az adatkezelés természetéből fakadó kockázatokat, és az e kockázatok csökkentését szolgáló intézkedéseket, például titkosítást alkalmazni. Ezek meghatározásakor figyelembe kell venni a személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből eredő kockázatokat is.

Az új adatbiztonsági szabályozás az adatvesztés esetére is kitér. Incidens bekövetkezte után az adatokhoz való hozzáférést „kellő időben" vissza kell állítani, áll a GDPR leírásában. Ezen túlmenően az adatkezelőnek gondoskodnia kell a létrehozott adatvédelmi megoldás rendszeres teszteléséről, értékeléséről. Így biztosított ugyanis, hogy nem csupán egyszer megugrandó akadály lesz a GDPR bevezetése, hanem a rendelkezés betartása folyamatos feladattá válik.

Egyszerre fogalmaz világosan és homályosan az európai uniós rendelkezés abban a tekintetben, hogy milyen eszközöket kell a feltételek biztosításának szolgálatába állítani. Konzekvensen a "tudomány és technológia állását figyelembe vevő" megoldásokat ír elő a reguláció, ami hátrány abban a tekintetben, hogy nem ad konkrét fogódzót az alkalmazandó eljárásokról és termékekről. Másrészt viszont előny is, mert nem szabályozza tételesen a felhasználható eszközök listáját, ennek hiánya pedig kellő szabadságot és rugalmasságot biztosít a GPDR technikai oldalról való betartásához.

Forrás: **http://bitport.hu/mar-csak-par-honap-a-gdpr-bevezeteseig**

Válogatta: Fonyó Istvánné