A GDPR ÉS AZ IT-SZEKTOR

ÚJ SZINTEKEN AZ ADATVÉDELEM

Két éve lépett hatályba az Európai Unióban a személyes adatok védelméről szóló rendelet, amelyet 2018. május 25-étől kezdve az EU teljes területén alkalmazni kell. A GDPR (General Data Protection Regulation) néven ismert, az Unióban kötelezően érvényes jogszabály alapján nemcsak a határnaptól kezdődő, hanem az alkalmazás időpontja előtt megkezdett adatkezelést is összhangba kell hozni az előírásokkal. A komplex feladat az IT-szektor szereplőit szokatlanul nagy kihívások elé állítja.

A globalizáció és a folyamatosan gyorsuló technológiai fejlődés egyre nehezebbé teszi a személyes adatok védelmét, mivel ezen adatok gyűjtésének és megosztásának jelentős mértékű emelkedésével párhuzamosan az emberek kiszolgáltatottsága is növekszik. Az adatvédelmi rendeletben az EU döntéshozói kinyilvánították, hogy a személyes adatok védelme alapvető jog, ezért a természetes személyek számára biztosítani kell a saját személyes adataik feletti önrendelkezést. Mint minden szabadságjog, ez is csak bizonyos korlátozásokkal érvényes: a rendelet hangsúlyozza, hogy a személyes adatok kezelését az emberiség szolgálatába kell állítani, és léteznek olyan társadalmi érdekek, amelyek elsőbbséget élveznek az egyéni szabadságjogokkal szemben.

Néhány fontos meghatározás

Tisztázzuk először az „érintett" fogalmát. Mindenkinek vannak rá jellemző személyes adatai, de a rendelet szempontjából egy *természetes személy akkor válik érintetté*, ha bármilyen személyes adata alapján őt – akár közvetlenül, akár közvetve – azonosítani lehet.

Személyes adat a név, a születési adatok, a különböző azonosító jelek, a helymeghatározó adat, az online azonosítók, továbbá a testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális adottságokra vonatkozó adatok. A GDPR szerint „a természetes személyek összefüggésbe hozhatók az általuk használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítókkal, például IP-címekkel és cookie-azonosítókkal".

A GDPR hat olyan jogalapot nevez meg, amely jogszerűvé teszi a személyes adatok kezelését: *az érintett hozzájárulása* (ezt az érintett bármikor visszavonhatja); *szerződéses jogviszony* (ha az érintett az egyik szerződő fél); az adatkezelőre vonatkozó *jogi kötelezettség; közérdek;* jogos érdek (ez esetben érdekmérlegelési teszt és írásbeli nyilatkozat kell); *létfontosságú érdekek védelme.*

A személyes adatok kezelése során az alábbi feltételek mindegyikének együttesen kell érvényesülnie: az eljárás csak *jogszerű, tisztességes, átlátható és célhoz kötött* lehet, fontos követelmény *az adattakarékosság, a pontosság, a korlátozott tárolhatóság, az integritás és a bizalmas jelleg biztosítása,* továbbá az *elszámoltathatóság.*

Az alapvető jogok gyakorlására vonatkozó szabályok egységes és következetes alkalmazását egyöntetűen kell biztosítani az Európai Unió területén.

Adatkezelés, adatfeldolgozás

Adatkezelő és adatfeldolgozó pozíciók között a GDPR funkcionális, függőségi és felelősségi viszonyokat állapít meg. Az adatkezelő határozza meg az adatkezelés céljait és eszközeit, ő hozza meg az adatkezeléssel kapcsolatos érdemi döntéseket, ő kezeli (gyűjti, rögzíti, tárolja stb.) ténylegesen a személyes adatokat, amelyeket az *adatfeldolgozó* az adatkezelő nevében, az ő megbízásából kezel valamilyen konkrét, meghatározott céllal. Az adatfeldolgozónak az adatkezelő utasítása alapján kell eljárnia, nem dönthet önállóan az adatkezelés tárgyát képező személyes adatokról. Az adatfeldolgozó által végzett adatkezelésről a két félnek írásbeli szerződésben kell megállapodnia.

Az adatkezelő és az adatfeldolgozó közötti tipikus feladatmegosztás, hogy ez utóbbi kezeli az előbbi honlapját, könyveli bevételeit stb. A GDPR szerint: ha az adatkezelést az adatkezelő nevében más végzi, az adatkezelő *kizárólag* olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek *megfelelő garanciákat* nyújtanak arra, hogy az adatkezelés megfelel a rendelet követelményeinek, és arra alkalmas technikai, szervezési intézkedések biztosítják az érintettek jogainak védelmét. Az adatfeldolgozónál a személyes adatok kezelésére feljogosított személyeknek titoktartási kötelezettséget kell vállalniuk.

Kikerülhetetlen lépések

A szervezetben legelőször át kell tekinteni az összes olyan folyamatot, ahol személyes adatokat kezelnek. A rendelet kötelezi az adatkezelőket és az adatfeldolgozókat a részletesen előírt tartalmú *adatkezelési nyilvántartás* vezetésére. (A rendelet megfogalmaz a 250 főnél kisebb létszámú szervezetekre vonatkozó kivételeket, köztük az alkalmilag történő adatkezelést, de nehéz elképzelni, hogy egy vállalkozás a munkavállalóinak az adatait csak alkalmilag kezelné…) A nyilvántartásban rögzíteni

kell a kezelt személyes adatok kategóriáit, az adatkezelés jogalapját, a személyes adatok manuális és/vagy informatikai feldolgozásának módját, tárolásának idejét, az adatok szervezeten belüli áramlását, az esetleges adattovábbítás tényét stb.

Az „adatleltár" elkészítése után fel kell mérni a kockázatokat, majd górcső alá kell venni a rendelkezésre álló feltételeket, különösen az *információbiztonságra vonatkozó technológia szintjét és megfelelőségét*. Az ISO/IEC 27001 szabvány szerinti tanúsítással rendelkező szervezetek nagy valószínűséggel megfelelnek a rendelet ez irányú követelményeinek.

Ki kell jelölni az adatkezeléssel ténylegesen foglalkozó munkatársakat, akiket föl kell készíteni a rendelet alkalmazására; számukra *adatvédelmi oktatást*, tréninget kell tartani. A rendelet által előírt tartalommal kell elkészíteni az új *adatkezelési tájékoztatót*, a különböző *nyilatkozatokat*, a *sütikezelési tájékoztatót* stb.

Következik az *adattisztítás* kényes, nehéz feladata. A személyes adatokat tartalmazó, digitálisan és/vagy papíron tárolt dokumentumokat, fájlokat át kell nézni, és *törölni* vagy *selejtezni* azokat, amelyekre nézve nincs jogosultság. A célhoz kötötten őrzött állomány *biztonságos tárolását* meg kell oldani.

Külön szólunk a törlésről, amely nemcsak a már meglévő, hanem a jövőbeni adatokra is igaz. Amennyiben a természetes személy hozzájárulás alapján adta meg az adatait, bármikor kérheti azok törlését. A törlésre olyan technikai megoldást kötelező választani, amely lehetetlenné teszi a személyes adatok visszaállíthatóságát, és ezt az adatkezelő hitelt érdemlően tudja bizonyítani.

A kellő jogalap birtokában tárolt adatok esetén a rendelet szól az *álnevesített*, illetve az *anonim* adatokról, amelyek között alapvető különbség van. A rendelet kifejezetten ajánlja az álnevesítést, ha az adatkezelés az érintettekre nézve vélhetően magasabb kockázattal jár. A feltételek azonban szigorúak: az adatkezelőnek megfelelő technikai és szervezési intézkedéseket kell hoznia, és biztosítania kell, hogy azokat az információkat, amelyek birtokában az álnevesített adatokat egy adott érintetthez lehet kapcsolni, elkülönítve tárolják. Az adatkezelő szervezeten belül ki kell jelölni a feladatra feljogosított személyeket. Az anonimizált adatokra a rendelet nem vonatkozik.

Ki kell nevezni egy *belső adatvédelmi felelőst* – vagy bizonyos esetekben *adatvédelmi tisztviselőt* –, akinek az elérhetőségét közzé kell tenni a nyomtatott és online adatkezelési tájékoztatókban. Bármilyen adatkezelési probléma esetén haladéktalanul értesíteni kell az adatvédelmi felelőst, mert ő köteles bejelenteni az illetékes hatósághoz az *adatvédelmi incidenst*.

A kockázatelemzés során meg kell jelölni a kritikus folyamatokat: az érintettek tájékoztatását, az adatigénylések kezelését, az adatok tárolásának módját és idejét, a törléshez („elfeledtetéshez") való jog biztosítását, az adattovábbítás feltételeit és körülményeit.

Hatásvizsgálat és biztonság

A rendelet által meghatározott esetekben, az adatkezelést megelőzően az adatkezelőnek *adatvédelmi hatásvizsgálatot* kell lefolytatnia. Az eljárás során az adatkezelő áttekinti a tervezett adatkezelési műveletek szükségességét és arányosságát, megvizsgálja az adatkezelésnek az érintettekre gyakorolt esetleges hatását, felméri a kockázatokat és azok

GDPR-KOMPATIBILIS ADATKEZELÉS A SZIGET FESZTIVÁLON

Érdekes ügy olvasható a Nemzeti Adatvédelmi és Információs Hatóság (NAIH) 2017. évi beszámolójában. Többen kifogásolták, hogy a Sziget és a VOLT Fesztiválra beléptetés során a szervezők beszkennelik a vendégek fényképes személyazonosító igazolványát, és az érintetteket nem tájékoztatják arról, milyen célból, mennyi ideig kezelik az adataikat.

A vizsgálat során megállapították, hogy az igazolvány beszkennelése a részvétel előfeltétele volt: a szervező rögzítette a látogatók személyes adatait, majd hozzárendelte azokat a belépésre jogosító karszalaghoz. A szervező a terrorcselekmények elleni védelemmel indokolta az intézkedését, így akarván biztosítani a fesztivállátogatók élethez való jogát, és megakadályozni a visszaéléseket.

A NAIH a fesztivállátogatók biztonságának garantálását fontos és elfogadható célnak tekintette, amelyben egyszerre van jelen a közérdek, az érintettek biztonsága és a rendezvényszervező gazdasági érdeke, ugyanakkor megállapította, hogy a hozzájárulás nem megfelelő jogalap, ha nélküle nem valósul meg a fizetség ellenében igénybe vehető szolgáltatás, továbbá, ha az érintettnek nincs valódi választási lehetősége a beléptetéssel összefüggő adatkezelés során. A NAIH sem a választott eszközt, sem a módszert nem tartotta alkalmasnak és arányosnak.

A hatóság utalt arra, hogy jellemzően állami feladat annak megállapítása és kimondása, hogy a fesztiválátogatók biztonságának garantálása közérdek, és az államnak kell gondoskodnia a védelem megfelelő szintjét biztosító intézkedésekről. A jogalkotónak kellene megfelelően szabályoznia a kérdést, és törvényes jogalapot teremteni a cél eléréséhez szükséges adatok kezeléséhez.

kezelésének módját, bizonyítja a rendeletnek való megfelelést, és mindezt dokumentálja.

A következő körülmények fennállásakor kell elvégezni az előzetes adatvédelmi hatásvizsgálatot: vagy *magas kockázatú adatkezelési műveletek esetén*, vagy ha *nagy mennyiségű személyes adat kezelése* várható, vagy ha *kiszolgáltatott személyek*, például *gyermekek adatait* szándékoznak kezelni. Kötelező a vizsgálat akkor is, ha egyes személyes jellemzők *automatizált adatkezelésen, profilalkotáson* alapuló értékelése történik, és erre a természetes személy tekintetében joghatással bíró, vagy a természetes személyt jelentős mértékben érintő döntések épülnek. Ugyanezen kritériumok érvényesek a *nyilvános helyek nagymértékű, módszeres megfigyelése*, továbbá a *különleges adatok kezelése* során.

Számos olyan vállalkozás, intézmény van, ahol eddig is maximálisan gondoskodtak az IT-biztonságról, de az ő számukra sem fölösleges áttekinteni, „GDPR-kompatibilis-e" az informatikai rendszer működése.

Az első lépés lehet a *kétlépcsős azonosítás* bevezetése, amely két, egymástól fizikailag elkülönített eszközt használ a belépéskori autentikációhoz. Jó megoldás a személyes adatokat tartalmazó állományok *titkosítása* valamennyi adathordozón, tárolóeszközön. Kötelezettségként elő lehet írni, de még jobb automatikusan beállítani a *munkaállomások zárolását*, néhány perc inaktivitás után. Léteznek olyan megoldások, amelyek zárolják az okostelefonnal Bluetooth-on keresztül párosított számítógépet, ha a mobil eszköz hatótávon kívül kerül.

Ismert, széles körben alkalmazott megoldás a VPN-kapcsolat, az interneten keresztül működő „virtuális magánhálózat". Az újabb mobileszközök képesek *VPN-kapcsolat* létrehozására, amely a személyes adatok védelmét is segíti, mert ez esetben a védett belső hálózatról nem kell kivinni semmilyen adatot. A VPN további előnye, hogy a Wifi-hálózatok használata során jelentősen megnehezíti az adathalászok dolgát.

Kódexek, szabályok

Végül egész röviden érintünk néhány további fontos elemet. A GDPR szerint az adatkezelő nemcsak önállóan járhat el. A rendelet bevezeti a *közös adatkezelő* fogalmát, mely szerint a közös adatkezelők átlátható módon, a közöttük létrejött megállapodásban határozzák meg a kötelezettségek teljesítéséért fennálló felelősségük megoszlását.

A rendelet szorgalmazza a *magatartási kódexek* kidolgozását annak érdekében, hogy az egy szakterületen dolgozó adatkezelők vagy adatszolgáltatók pontosítsák a rendelet alkalmazását. A magatartási kódexeket a felügyeleti hatóság hagyja jóvá. A rendelet ösztönzi továbbá olyan adatvédelmi *tanúsítási mechanizmusok, adatvédelmi bélyegzők, jelölések* létrehozását, amelyek azt bizonyítják, hogy az adatkezelő vagy adatfeldolgozó adatkezelési műveletei megfelelnek a rendelet előírásainak.

A *felhőszolgáltatókra* vonatkozó szabályok legfontosabb elemei: a felhőszolgáltatást nyújtó jogilag adatfeldolgozónak minősül, tehát vonatkoznak rá a fent leírt garanciális feltételek. Gyakran azonban nehéz megállapítani, hol működik a felhőszolgáltató – holott a GDPR szempontjából perdöntő, hogy az Unió területén, vagy azon kívül zajlik-e az adatkezelés. A jogi megfelelőséghez és annak bizonyításához szükséges megoldások kialakítása elengedhetetlen, és hasznos, ha a felhőszolgáltató rendelkezik a nemzetközi információbiztonsági szabványok auditjával. A legnagyobb felhőszolgáltatók már kialakítottak néhány magatartáskódexet, amelyhez auditált módon lehet csatlakozni, és ezzel bizonyítani a GDPR-megfelelőséget.

Végezetül meg kell említeni a *kötelező erejű vállalati szabályok* alkalmazását, amely főleg azoknak a vállalkozáscsoportoknak fontos, amelyek egyes tagjai az EU-n kívül olyan országokban működnek, amelyek tekintetében nincs elfogadott megfelelőségi határozat. A kötelező erejű vállalati szabályok alkalmazására csak akkor kerülhet sor, ha azt előzőleg az illetékes felügyeleti hatóságok – az egységességi mechanizmus keretében – jóváhagyták.

A rendelet tisztázza az adatkezelésben érintettek szerepét és felelősségi viszonyait. Bármilyen nehéznek tűnik némelyik előírás betartása, hosszú távon előnyt jelent a világos szabályozottság. A személyes adatok kezelésével foglalkozó szervezeteket összefogásra, integrációra készteti, és minden eddiginél erőteljesebben kikényszeríti a négy nagy szegmens: az üzleti, a jogi, az informatikai és az információbiztonsági területek együttműködését.

Tószegi Zsuzsanna