ABT Adatbiztonsági Tanácsadó Kft.

H-1037 Budapest Montevideo u. 3/A
Tel.: +36 1 430-3400 Fax: +36 1 430-3402
abt@abt.hu www.abt.hu

Új időszámítás a vállalkozások életében: 2018. május 25-én életbe lép az EU Adatvédelmi Rendelete

Tartalomjegyzék

Jelentős terhet ró a hazai vállalkozásokra a tavasszal hatályba lépő európai adatvédelmi rendelet. Egyre növekszik azon vállalkozások száma, amelyek megkövetelik a beszállítóiktól a rendeletnek való megfelelőségük bizonyítását. Ezen felül példátlan, 6 milliárd forint mértékű bírság fenyeget. A KKV-k, sőt a mikró vállalkozások sem kivételek. Aki nem lép időben, könnyen lemaradhat. Aki viszont hatékonyan alkalmazkodik az új körülményekhez, a versenytársai elé kerülhet! 30 lépésben konkrét útmutatót adunk a cikkünkben.

Az *arany* és az *olaj* után az adat vált a gazdaság legjelentősebb erőforrásává. A világ öt legértékesebb tőzsdén jegyzett vállalata adatokkal gazdálkodik. Nem mindegy tehát, hogy a vállalkozások a kincsüket hol és milyen körülmények között kezelik. 2018. május 25-e új időszámítás az adatvédelemben. Ekkortól alkalmazandó kötelezően az Európai Unió Általános Adatvédelmi Rendelete, angol nevén a General Data Protection Regulation, rövidítve GDPR. A jogszabály már kötelező alkalmazása előtt jelentős hatást gyakorol a világ adatvédelmi rezsimjeire is. A GDPR-t kell ugyanis alkalmazni akkor is, ha ugyan a szolgáltatást nyújtó vállalat nem az EU területén működik, de a kínált szolgáltatás vagy termék Európában tartózkodó személyek számára is elérhető.

Az adatvédelmi rendeletnek való megfelelés a legtöbb vállalkozásnál jelentős anyagi és személyi erőforrást igényel. Alábbiakban foglaljuk össze az új jogszabály legfontosabb rendelkezéseit, pontokba szedve a mérföldköveket, amelyeket követve a vállalkozások felkészülhetnek a rendelet alkalmazására.

A tét nem kicsi, ha nem tudjuk a megfelelőségünket a piaci résztvevők felé bizonyítani, *elveszíthetjük az ügyfeleinket.* Egyre több cég várja el ugyanis a beszállítóitól, hogy a GDPR megfelelőségüket igazolják.

Ezen felül az új rendelet horrorisztikus, akár 20 millió eurót vagy a vállalkozás előző pénzügyi év teljes éves világpiaci forgalmának 4%-át elérő bírságokat helyez kilátásba azok számára, akik nem az új jogszabály szerint kezelik mások személyes adatait. Röviden: nem lehet a továbbiakban a laza adatvédelmi gyakorlat veszélyét az üzleti folyamatokban beárazni.

A megfelelésnek nincs alternatívája a saját jövőjét felelősséggel építő vállalkozások körében. Másik oldalról persze a jogszabályi rendelkezésektől függetlenül látjuk, hogy az adatszivárgások, illetve a jogszerűtlen adatkezelések felmérhetetlen reputációs károkat okoznak a vállalkozásoknak. Nemrégiben a Yahoo esetében találkozhattunk azzal, hogy egy adatvédelmi incidens napvilágra kerülése után mennyit esett a cég piaci értéke.

De nézzük meg az előttünk álló feladatok pozitív oldalát: egy vállalkozás komoly versenyelőnyre tehet szert, ha az EU új adatvédelmi rendeletére való felkészülése során áttekinti üzleti folyamatait, körültekintető adatvédelmi stratégiát készít, szigorú adatvédelmi szabályokat vezet be, és az adatvédelmi megfelelőségét a külvilág felé bemutatja.

1. Miért volt szükség egy új adatvédelmi rendeletre?

A jelenleg hatályban lévő irányelvvel szemben, amelyet 28 különböző tagállami adatvédelmi jogszabály ültetett a nemzeti jogba, a hamarosan életbelépő rendeletet nem kell a tagállami jogrendszerekbe átültetni, az közvetlenül alkalmazandó és hivatkozható az EU minden tagállamban. A rendelet egységesíti a 28 uniós tagállam adatvédelmi jogszabályait, ettől kezdve a vállalkozásoknak minden uniós országban ugyanazokat a rendelkezéseket kell betartaniuk és ugyanazokkal a jogkövetkezményekkel számolhatnak, ha ennek nem tesznek eleget.

Mindannyian tudjuk, hogy a jogszabályi elvárások és a mindennapi gyakorlat sokszor nincsenek teljesen harmóniában. Más szóval egy dolog, hogy mit kér egy jogszabály és egy másik, hogy ebből mit tartanak be a vállalkozások. Talán nincsen még egy jogterület, ahol a jogalkotó által felmutatott célok, jogelvek olyan messze kerültek volna a valós gyakorlattól, mint az adatvédelem.

Egyik oldalról az adatvédelemhez, a magánszféra védelméhez való jog egy alkotmányos jog, amit már 1948-ban az ENSZ Emberi Jogok Egyetemes Nyilatkozata is védeni rendelt. Másik oldalról a technika rohamos fejlődésével (vénaszkenner, drónok, IoT, Facebook, profilozás, gépelésdinamika alapján történő azonosítás stb.) egyre több szolgáltatás, mindinkább intim magánszféránkhoz tartozó személyes adatokat használ üzleti célokból. A *magánszféránk sérülékenyebbé vált* mint valaha, a személyes adatok piaci értéke pedig soha nem látott magasságokban jár.

Napjainkra a szakadék a piaci szereplők gyakorlata és a jogalkotó elvárásai, a valóság és az emberi jogok patetikus jogelvei, elvárásai között áthidalhatatlanná nőtt. Ezt a szakadékot kívánja a jogalkotó a kilátásba helyezett példátlan mértékű, 20.000.000 euró összegű bírsággal és a – későbbiekben tárgyalt - elszámoltathatóság elvének bevezetésével május 25-tel áthidalni.

A GDPR-ban szereplő szabályok többségében semmi új nincsen. Az újdonság az, hogy ezeket a szabályokat ki is lehet majd kényszeríteni, a megfelelőségünket pedig dokumentáltan kell tudnunk bizonyítani. Nem elég ezentúl jogszerűen eljárnunk, a jogszerű működésünket dokumentumokkal *alá is kell tudnunk támasztani.* Ha valaki továbbra sem felel meg az adatvédelmi elvárásoknak, azt veszélyezteti, hogy a vállalkozása lehúzhatja a rolót. A vállalkozások egyszerűen nem engedhetik meg maguknak, hogy olyan partnerekkel dolgozzanak, akik nem tudják az adatvédelmi szabályokat bizonyítottan betartani. A bíróságok ugyanis olyan méretűre lettek szabva, hogy azok a vállalkozások méretétől függetlenül a jogszabályokra fittyet hányó cégek ellehetetlenítését hozzák magukkal.

Az egyeztetési mechanizmus, amit a nemzetállamok hatóságainak igénybe kell venniük, biztosítja azt, hogy a holland, a francia vagy a svéd hatóságok ugyanolyan összegű bírságot szabjanak ki, mint a magyar hatóság. A vállalkozás méretétől (egyéni vállalkozó vagy multinacionális cég) sem függhet az, hogy a bírság mekkora összegű lesz. Az egyetlen faktor az adatvédelmi szabálysértés súlya lesz.

Ahol jelenleg is komoly anyagi és személyi erőforrásokat vesznek igénybe az adatvédelmi megfelelés érdekében, ahol jelenleg is dolgozik adatvédelmi tisztviselő, vannak kidolgozott, naprakészen tartott adatvédelmi szabályzatok, amiket a munkavállalók ismernek, betartanak, a belső audit rendszeresen ellenőrzi a folyamatokat, ahol ezen felül rendelkeznek működő információbiztonsági irányítási rendszerrel (lsd. ISO 27001 tanúsítvány), ott csak fazonigazítást

kell elvégezniük a cégeknek. A fazonigazítás is eltarthat hónapokig, az adatvédelemmel mélységeiben nem foglalkozó vállalkozások pedig az anyagi, időbeli és személyi ráfordításokat tekintve lényegesen nagyobb kihívás előtt állnak.

A GDPR az uniós joganyagok között is a *nagy terjedelmű, bonyolult* és nehezen értelmezhető jogszabálynak számít. Ennek ellenére, ha átverekedtük magunkat a rendelet szövegének dzsungelén, még mindig csak az utunk elején járunk. Az adatvédelmi jog területén, mivel egy viszonylag fiatal jogterületről van szó, alapvetően fontos ismerni a hazai, a külföldi és az uniós hatóságok, intézmények és bíróságok jogértelmezését és joggyakorlatát. Mindezen tudás nélkül elképzelhetetlen felelős jogi tanácsadás.

A jogi szakértelmen kívül nélkülözhetetlen az informatikai, információbiztonsági szakismeret is. A jogi elvárásokat az *informatika* eszközeivel tudjuk a mindennapok részévé tenni.

A harmadik elem az üzleti folyamatok ismerete. Alapos ismeretekkel kell rendelkeznünk a *vállalkozás napi működését* illetően ahhoz, hogy az előttünk álló feladatokkal meg tudjunk birkózni.

A jogi, az informatikai és a közgazdaságtani ismeretekkel, szaktudással felvértezve tudunk csak a GDPR-ra felkészülni. Nyilvánvalóan mindez az ismeret nem lehet meg egy személyben. A polihisztorok kora lejárt. Ez egy igazi csapatjáték.

2. Hogyan kezdjünk neki a GDPR-ra való felkészülésnek?

A *vezetők elkötelezettsége* nélkül messzire nem jutunk, ezért fontos, hogy a vállalkozás döntéshozóit megismertessük az előttük álló feladatokkal, a jogszabályi megfelelés elmaradásának üzleti, jogi és pénzügyi kockázataival és nem utolsó sorban a megfelelés üzleti előnyeivel.

A jogszabályi elvárásoknak való megfelelés a legtöbb hazai vállalkozásnál komoly anyagi és személyi erőforrásokat fog igényelni. A szükséges erőforrások allokálása az egyik első lépésünk lesz.

A vállalkozásnál érdemes valakit kijelölni, aki az adatvédelmi felkészülést koordinálni fogja. Elengedhetetlen, hogy a felkészülést összefogó ember a vállalkozásnál működő különböző szakterületek legfőbb működési sajátosságaival tisztában legyen, megfelelő informatikai ismeretekkel rendelkezzen és ismerje az alapvető jogszabályi elvárásokat. Ideális esetben ez a személy a vállalkozás adatvédelmi tisztviselője lesz.

Ha a vállalkozás döntéshozói megismerték a GDPR által támasztott legfontosabb kihívásokat, elköteleződtek aziránt, hogy az adatvédelmi szabályoknak megfeleljenek, a szükséges anyagi és személyi erőforrásokat biztosították a projekthez, kinevezték a cég adatvédelemért felelős projektjének koordinátorát, a következő lépés, hogy egy projekt csapatot hozzunk létre. Az adatvédelemnek sajátja ugyanis, hogy a személyes adatok nem állnak meg a különböző csoportok, osztályok, igazgatóságok, üzletágak ajtajánál. A napi működés során természetes módon, sokszor észrevétlenül kezeljük, osztjuk meg, rögzítjük, tesszük mások számára elérhetővé vagy éppen töröljük a személyes adatokat. A sikeres GDPR felkészülés a vállalkozás valamennyi munkavállalójának szoros együttműködését feltételezi.

Lényeges, hogy a projektcsapatban a vállalkozás minden olyan részlege képviseltesse magát, amelyben személyes adatok kezelése történik. Bizonyosan a teamben lesz a helye a HR, az informatika (IT), a beszerzés, a jog, a risk & compliance és a belső audit képviselőjének.

3. De mi számít személyes adatnak?

Erre az elsőre triviálisnak tűnő kérdésre a válasz a gyakorlatban sokszor nem is olyan egyszerű. A rendelet értelmében személyes adatnak minősül „az azonosított vagy azonosítható természetes személyekre 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. Fontos tehát, hogy az azonosítás nem csak úgy képzelhető el, hogy tudom az illető lakcímét, anyja nevét, születési helyét és idejét. Azonosíthatok valakit úgy is, hogy annyit tudok róla, hogy a Kossuth utcában lakó szemüveges férfi. Az Egyesült Államokban a születési idő, a nem és az irányítószám alapján a lakosság 62%-át be lehet azonosítani. A fentiek alapján személyes adat lehet gyakorlatilag bármi, ami egy természetes személyhez köthető, így például a TAJ szám, az e-mail, az IP cím, a cookie (internetes süti), a biztonsági kamera felvétele, a GPS koordináták, a vércsoport, az irányítószám, az éttermi fogyasztás, az alkalmassági teszt eredménye, egy gépkocsi márka, vagy az autó fogyasztása is.

4. Mikor nem kell alkalmazni a rendelet szabályait?

A rendeletet nem kell alkalmazni, ha a személyes adatok kezelése személyes vagy otthoni tevékenység során történik. Nem kell továbbá alkalmazni, ha az adatok nem természetes személyekre, hanem jogi személyekre, cégekre vonatkoznak.

5. Mit jelent az adatkezelés?

A GDPR értelmében adatkezelés a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett *bármely művelet* vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés. Lényegében bármilyen cselekvés, ami a személyes adathoz köthető, még az is, ha ránézek vagy elolvasom azt.

6. Adatkezelő vagy adatfeldogozó vagyok?

A GDPR-ra való felkészülésünk fontos állomása az, hogy eldöntsük, hogy a személyes adatok kezelése során adatkezelőként vagy adatfeldolgozóként járunk-e el.

Adatkezelőnek kell tekinteni azt a természetes vagy jogi személyt, aki a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza. Adatfeldolgozó az a természetes vagy jogi személy lesz, aki az adatkezelő nevében személyes adatokat kezel. A kérdés eldöntése sokszor nem egyszerű, támpontot adhat ugyanakkor a nemzeti és az uniós hatóságok, illetve a tagállami és a közösségi bíróságok joggyakorlata. Az, hogy adatkezelő vagy adatfeldolgozó vagyunk-e részben az adminisztratív terheinkre lesz befolyással, részben pedig arra, hogy ki lesz felelős az adatkezelésből eredő incidensekért, károkért.

7. Az adatkezelés alapelvei

Ahhoz, hogy meg tudjuk állapítani, hogy az adatkezeléseink jogszerűek-e, elengedhetetlen, hogy tisztában legyünk a legalapvetőbb adatvédelmi jogi elvekkel. Az alábbiakban sorra vesszük az adatvédelem legfontosabb alapelveit.

A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni (*„jogszerűség, tisztességes eljárás és átláthatóság elve”*). Ennél az elvnél talán az átláthatóság fogalma igényel csak bővebb magyarázatot. Az átláthatóság azt jelenti, hogy az adatkezelés valamennyi stádiuma alatt (gyűjtés, kezelés, továbbítás, törlés stb.) minden fél számára (adatkezelő, érintett, hatóság stb.) világosnak és egyértelműnek kell lennie minden személyes adatra vonatkozó információnak (ki kezeli, milyen célból, milyen jogalappal, hol tárolja, hogyan védi, ki fér hozzá, mikor törli stb.).

A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, és azokat nem lehet ezekkel a célokkal össze nem egyeztethető módon kezelni (*„célhoz kötöttség elve”*).

Csak annyi személyes adatot kezeljünk, amennyire feltétlenül szükségünk van, ne raktározzunk adatokat abból a megfontolásból, hogy majdcsak jó lesz valamire. A személyes adatokhoz ne az férjen hozzá, akinek arra jogosultsága van, hanem az, akinek a munkája végzéséhez ehhez feltétlenül szüksége van (*„adattakarékosság”* vagy *„adatminimalizálás elve”*).

A személyes adatok pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék (*„pontosság elve*”).

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 elve*”).

A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az

adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve (*„integritás és bizalmas jelleg”*).

A GDPR legnagyobb újdonsága az *„elszámoltathatóság elvének”* a bevezetése. Ennek értelmében az adatkezelő felelős a fenti elveknek való megfelelésért, és ezt képesnek kell lennie dokumentumokkal alátámasztva igazolni. Ez egyfajta *fordított bizonyítási kényszer*t jelent. Nem az adatvédelmi hatóságnak, érintettnek, üzleti partnernek kell bizonyítania, hogy az adatkezelő nem jogszerűen járt el, hanem a vállalkozásoknak kell minden egyes adatkezelésükről dokumentálni és kérésre az adatvédelmi hatóságnak, beszállítónak átadni minden dokumentumot, amivel *bizonyítja a jogszabályi megfelelést*, különös tekintettel az adatkezelés jogalapjára, céljára, a címzettek körére, az alkalmazott konkrét, megfelelő technikai és szervezési védelmi intézkedésekre.

Az elszámoltathatóság elve a gyakorlatban azt jelenti, hogy egy aktában összekészítve át kell tudnunk adni a GDPR megfelelőségünket tanúsító szabályzatokat, jegyzőkönyveket, nyilvántartásokat, dokumentumokat úgy az ügyfeleink, az érintettek, mint az adatvédelmi hatóság részére.

8. 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 oly módon, hogy az adatvédelmi elvek a termék és a szolgáltatás teljes életciklusa alatt érvényesüljenek.

Az alapértelmezett adatvédelem (Privacy by default) elve arra ad biztosítékot, hogy a szolgáltatás nyújtásához, termék igénybevételéhez minimálisan szükséges személyes adatot kezelik a vállalkozások.

9. Az érintettek jogai

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

Átlátható tájékoztatás

A természetes személyek jogosultak a személyes adataik 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 estén annak okairól,
- 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.

Ha az adatkezelő a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő célról. Ha a személyes adatokat nem az érintettől szerezték meg, tájékoztatást kell adni a személyes adatok forrásáról, akkor is ha az adatok nyilvánosan hozzáférhető forrásokból származnak.

Hozzáférési jog

Az adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát (pl. feljegyzés a felvételi elbeszélgetés során vagy egy videó felvétel egy áruházban) 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, tehát másokra vonatkozó személyes adatokat ki kell maszkolni, azonosíthatatlanná kell tenni, törölni kell.

Ennek a jognak az újdonsága abban áll, hogy az érintettnek nemcsak arra van joga, hogy megtudja, hogy milyen adatot kezelnek róla (pl. képfelvétel), hanem konkrétan joga van megkapni a személyes adatát tartalmazó adathordozót, illetve annak másolatát.

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 egy 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.

10. 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.

11. Felelősség és kártérítés

Minden olyan személy, aki a GDPR 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.

12. Adatvédelmi tisztviselő kinevezése

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 fenti kötelezettségen túl természetesen adatvédelmi tisztviselőt bármelyik vállalkozás kinevezhet. Ha a vállalkozás – a jogszabályi kötelezettség vagy ennek hiányában az ebből fakadó üzleti előnyök, pénzügyi terhek megvizsgálása után – úgy dönt, hogy nem nevez ki adatvédelmi tisztviselőt, feltétlenül javasolt a döntés mögött álló tényeket, szempontokat, indokokat és az azokból levont következtetéseket papírra vetni, hogy mindez a hatóság kérésére bemutatható legyen. A korábban már tárgyalt elszámoltathatóság elvének így tudunk csak megfelelni.

13. Adatregiszter, adattérkép

Jó hír a vállalkozások számára, hogy az adatvédelmi rendelet hatálybalépésével megszűnik az adatkezelők azon kötelezettsége, hogy az adatkezelésüket be kell jelenteniük az adatvédelmi hatóságnál vezetett adatvédelmi nyilvántartásba.

A jövőben az adatvédelmi nyilvántartást minden adatkezelőnek saját magának kell vezetnie lényegesen kibővült tartalommal. Az új adatvédelmi rendeletre való felkészülés legfontosabb feladata annak feltérképezése, hogy a vállalkozásunk milyen személyes adatokat kezel, azokat milyen jogalap alapján, kitől, milyen célból szerzi be, kinek továbbítja, milyen szervezési és technikai eszközökkel védi, kinek továbbítja, mikor törli.

Sokan az adatregisztert és az adattérképet szinonimaként használják, pedig érdemes különbséget tennünk a két fogalom között. Az adatregiszternek vagy, ahogy a jogszabály nevezi az „adatkezelési tevékenységek nyilvántartásának” elkészítése jogszabályi kötelezettség, míg az adattérkép nem kötelező. Az adatregisztert egy excel táblázatban tudjuk vezeti, míg az adattérkép a bonyolultabb, nehezebben áttekinthető folyamatok vizuális megjelenítésére, a folyamatok egyes lépéseinek áttekinthető módon történő bemutatására szolgál.

14. Az adatkezelések jogalapja

Az adatkezeléshez minden esetben szükségünk lesz megfelelő jogalapra. Ha nincsen jogalapunk az adatkezelésre, az adatkezelést (pl. gyűjtést, betekintést) nem kezdhetjük meg. Ha megszűnik a jogalapunk, azonnal meg kell szüntetnünk az adatkezelést (pl. törölnünk kell a személyes adatot vagy meg kell fosztanunk annak személyes adat jellegétől, például anonimizálással).

A személyes adatok kezelése akkor jogszerű, amennyiben legalább az alábbiak egyike teljesül:

- az érintett **hozzájárulás**át adta személyes adatainak kezeléséhez;
- az adatkezelés olyan **szerződés** teljesítéséhez szükséges, amelyben az érintett az egyik fél;
- az adatkezelés az adatkezelőre vonatkozó **jogi kötelezettség** teljesítéséhez szükséges;
- az adatkezelés az érintett **létfontosságú érdek**einek védelme miatt szükséges;
- az adatkezelés **közérdekű feladat** végrehajtásához szükséges;
- az adatkezelő vagy harmadik fél **jogos érdeke** érvényesítéséhez szükséges.

Ha több jogalap alapján kezelhetjük az adatot, akkor választanunk kell a jogalapok közül. Az, hogy melyik jogalapot választjuk, lényeges hatással lehet az adatkezelésünkre. A hozzájárulásnak fontos eleme például, hogy azt bármikor egyoldalúan vissza lehet vonni, ez a szerződéses jogalapra viszont nem igaz.

Amennyiben az adatkezelő a *jogos érdekére* hivatkozva kezeli másnak a személyes adatát, többlet adminisztrációs terhet vállal magára. Ennek a jogalapnak az alkalmazásakor feladat lesz az érdekmérlegelési teszt elkészítése. Ennek része, hogy megvizsgáljuk, hogy a cél, aminek érdekében a személyes adatot kezelni kívánjuk jogszerű-e (*jogszerűség vizsgálata*). Amennyiben megállapítjuk, hogy az adatkezelés célja jogszerű, meg kell vizsgálnunk azt, hogy a jogszerű célunk eléréséhez ténylegesen szükségünk van-e az adatkezeléshez (*szükségesség vizsgálata*). Amennyiben nagyobb erőfeszítés, anyagi áldozat nélkül ez a célunk személyes adat kezelése nélkül is elérhető, abban az esetben megállapítható, hogy nem szükséges az adatkezelésünk, így már nem lesz jogszerű az adatkezelésünk a jogos érdek alapján. Ha az adatkezelés célja jogszerű, a jogszerű célunk eléréséhez szükséges az adatkezelés, azt kell megállapítanunk, hogy az adatkezelésünk jogi alapjául kitűzött jogi érdekünk milyen arányban áll az érintett személyes adatok védelméhez fűződő jogaival (*arányosság vizsgálata*). A jogos érdek jogalap választása a legnagyobb szabadságot adja az adatkezelőnek (hiszen nem függ az érintett hozzájárulásától, szerződés érvényességétől, hatályosságától vagy jogszabályi felhatalmazás meglététől), de komoly adminisztratív kötelezettséget ró a vállalkozásokra. Egy-egy vizsgálat akár több tíz oldalnyi, száz fölötti kérdés megválaszolásával, értékelésével végezhető el. Az adminisztratív terhek ellenére várható, hogy az egyik legnépszerűbb adatkezelési jogalap lesz a jogos érdek, ezért érdemes tisztában lenni ennek részletszabályozásával is, illetve a piacon kidolgozott és megosztott jó gyakorlatokkal.

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 rendelet meghatározza a kritériumokat, hogy mikor megengedett az adatoknak *az eredeti céljától eltérő* egyéb célból történő kezelése.

15. Direkt marketing, hírlevelek, weboldalak

Direkt marketingnek (DM) minősül minden olyan reklám, amelyet közvetlen megkeresés módszerével küldenek akár postai, akár elektronikus úton, de annak számít a telefonhívás is (legyen az manuális hívás vagy automatizált hívórendszer).

A DM ezen fajtáinak azért van jelentőségük, mert a közös szabályok mellett, speciális szabályok is vonatkoznak az egyes fajtákra.

A reklám címzettje az, aki felé a reklám irányul, illetve akihez a reklám eljut. Adatvédelmi szempontból ez a személy lesz az érintett, akinek személyes adatait pl. a webáruház/honlap üzemeltetője kezeli.

Főszabályként az érintett személyes adatait csak hozzájárulása alapján lehet kezelni. A hozzájárulásnak előzetesnek kell lennie (azaz pl. a hírlevél kiküldése előtt be kell szerezni). Követelmény az egyértelműség és az is, hogy a hozzájárulás kifejezett legyen: tevőleges, aktív magatartással kell megvalósítani a hozzájárulást (pl. checkbox kipipálása, megfelelő gombra kattintás stb.). A lényeg, hogy ráutaló magatartás vagy valaminek a meg nem tétele nem minősül hozzájárulásnak.

A hozzájárulásnak önkéntesnek és bármikor visszavonhatónak is kell lennie, tehát az érintettnek tényleges választási lehetőséget kell biztosítani, és a hozzájárulás nem lehet az adott szolgáltatás igénybevételének feltétele (kivéve, ha az szükséges a szolgáltatás nyújtásához, pl. egy ruházati webáruházban a vásárló nadrágjának mérete).

A hozzájárulásnak kifejezetten az adott szolgáltatásra kell vonatkoznia, nem lehet összekapcsolni más hozzájárulással (tehát ha pl. egy internetes ételrendelés kapcsán részt vehetek egy nyereményjátékban, az éttermi szolgáltató csak hozzájárulásommal továbbíthatja a személyes adataimat a nyereményjáték szervezőjének.)

A példánál maradva, ha enyém lesz a főnyeremény a nyereményjátékon, majd ezt követően visszavonom a hozzájárulásom, akkor emiatt nem érhet hátrány (tehát pl. nem kell visszaadnom a nyereményt).

A hozzájárulás visszavonásának ugyanolyan egyszerű feltételekkel kell megtörténnie, mint a hozzájárulásnak (nem lehet tehát pl. csak a debreceni ügyfélszolgálati irodában történő személyes lemondást előírni, ha a hozzájárulást e-mailen adta meg az érintett).

Fontos, hogy a lemondásról szóló tájékoztatásnak mindig kell egy e-mail és egy postai címet is tartalmaznia. Az adatkezelési tájékoztatónak a honlapon elkülönülten kell elérhetőnk lennie, vagyis nem lehet pl. az általános szerződési feltételek része.

A GDPR a fenti hozzájárulás mellett új joglapként megjeleníti a jogos érdeket is, mivel azt tartalmazza, hogy a személyes adatok közvetlen üzletszerzési célú kezelése jogos érdeken alapulónak tekinthető.

A személyes adatok közvetlen üzletszerzési célú kezelése kapcsán a jelenlegi magyar szabályozás meglehetősen szigorú, hiszen nem teszi lehetővé, hogy egy cég az ügyfelének vásárlást követően saját hasonló termékét vagy szolgáltatását direkt marketing útján reklámozza. Ezen lazítana az EU-ban majd közvetlen hatállyal bíró, jelenleg elfogadás alatt álló e-Privacy rendelet, amely a 2018. május 25-re tervezett elfogadását követően mindezt lehetővé tenné akkor, ha az ügyfél számára biztosított a leiratkozás lehetősége.

16. Az adatvédelmi tisztviselő jogállása

Az adatvédelmi tisztviselő személyét és feladatkörét szigorúan védi a GDPR. Az adatvédelmi tisztviselő teljes szakmai függetlenséget élvez, feladatai ellátásával kapcsolatban utasításokat senkitől nem fogadhat 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. Feladatai munkavállalóként és kiszervezett tevékenységként, vállalkozási szerződésben is elláthatóak.

17. Az adatvédelmi tisztviselő feladatai

Az adatvédelmi tisztviselő legalább a következő feladatokat látja el:

a.) tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére adatvédelmi kérdésekben;

b.) ellenőrzi a GDPR-nak, a belső adatvédelmi szabályzatnak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő munkavállalók tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;

c.) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;

d.) együttműködik a felügyeleti hatósággal;

e.) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

18. Az 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 adatkezelő az adatkezelést megelőzően hatásvizsgálatot köteles végezni.

19. Az 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 rendelet.

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:

- 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.

20. Adatvédelmi képzések

Elképzelhetetlen a hatékony adatvédelmi irányítási rendszer felépítése és működtetése anélkül, hogy a személyes adatokat kezelő munkatársak nincsenek tisztában az alapvető adatvédelmi fogalmakkal, saját felelősségükkel. Mindez pedig tudatosságnövelő előadások, tréningek, e-learning tananyagok, tesztek rendszeres használatával tartható csak naprakészen.

21. Mi a helyzet a felhőszolgáltatásokkal?

Mindennapjainknak egyre inkább részévé válnak a felhőalapú szolgáltatások. A felhő lehetővé teszi az igény szerinti hálózati hozzáférést megosztott, konfigurálható számítástechnikai erőforrásokhoz (például hálózatokhoz, szerverekhez, tárolókhoz, alkalmazásokhoz és szolgáltatásokhoz), melyeket gyorsan lehet allokálni és használatukat lezárni, minimális menedzsment ráfordítással vagy szolgáltatói közreműködéssel (The NIST, Definition of Cloud Computing). A felhők révén a vállalkozások komoly versenyelőnyre tehetnek szert a szolgáltatás rugalmassága, költséghatékonysága révén.

Mind a szolgáltatók, mind a felhőszolgáltatást igénybe vevők hajlamosak nagyvonalúan kezelni az adatvédelmet, úgy az IT biztonsági kérdéseket, mint a jogszabályoknak való megfelelést. Az informatikusok és a jogászok hagyományosan távolról szokták egymást méricskélni. Az informatikusoknak a felhőszolgáltatásokkal kapcsolatos kérdések túl jogiak, a jogászoknak túl informatikaiak. Az átlag cégvezető meg mind a jogi, mind az informatikai problémáktól idegenkedik. Ez a szakadék a rohamos ütemű technikai fejlődéssel csak nőni látszik.

De hogyan tud meggyőződni arról egy vállalkozás, hogy a felhőben a jogszabályoknak, különösen a GDPR-nak megfelelően kezelik az adatait? Másik oldalról hogyan tudja a felhőszolgáltató az ügyfeleinek bizalmát megszerezni, majd megtartani, s szükség esetén a jogi megfelelőségét a külvilág felé, elsősorban az illetékes hatóságok felé bizonyítani?

A felhőszolgáltatást igénybe vevő sem az ügyfelei, sem az illetékes hatóságok előtt nem takarózhat azzal, hogy a szolgáltató az *„eszi, nem eszi, nem kap mást”* vagy, ahogy az angolok mondják „take it or leave it” elv szerint működik. Ezért egyetlen adatkezelő sem engedheti meg magának, hogy bizonyos informatikai, *horribile dictu* IT biztonsági kérdésekben ne merüljön el. Adatkezelőként náluk marad a *felelősség*, hogy az adatok kezelése a felhőben a jogszabályok szerint történik-e. Az más kérdés, hogy a szolgáltatás elégtelenségére visszavezethető *adatvédelmi incidens* esetén az adatfeldolgozó felhőszolgáltató felelőssége is megállhat.

A Norvég Adatvédelmi hatóság ajánlásában egy ellenőrző lista elkészítésével segítette a szolgáltatást igénybe vevők döntését. Nemcsak a bankok számára, hanem valamennyi adatkezelőnek jó támpont lehet a **Magyar Nemzeti Bank** idén januárban a pénzügyi szervezeteknek kiadott **ajánlása** is. Ebben arra kaphatunk iránymutatást, hogy a jogszerű működés érdekében a felhőszolgáltatókkal kötendő szerződésben milyen technikai, szervezési kérdéseket vagyunk kötelesek tisztázni és adott esetben ellenőrizni.

22. Megfelelő technikai és szervezési intézkedések

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

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

23. Az adatkezelők és az adatfeldolgozók közötti szerződések

A rendelet meghatározza az adatkezelők és az adatfeldolgozók között a személyes adatok kezelésére kötött szerződések kötelező tartalmi elemeit. A GDPR új kötelezettségeket is megállapít az adatfeldolgozók számára. Az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik megfelelő garanciákat nyújtanak a GDPR rendelkezéseit követő, megfelelő technikai és szervezési intézkedések végrehajtására.

Az adatkezelő és az adatfeldolgozó között olyan írásbeli szerződést kell kötni, amely minimálisan az alábbiakra tér ki:

- 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 kockázat 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 által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

Ha az adatfeldolgozó további adatfeldolgozó szolgáltatásait is igénybe veszi, a további adatfeldolgozóra is ugyanazok az adatvédelmi kötelezettségeket kell telepíteni, mint amelyek az adatkezelő és az adatfeldolgozó között létrejött szerződésben.

24. A személyes adatoknak az EU-n kívülre történő továbbítása

A GDPR alapelvként rögzíti, hogy a személyes adatoknak az Európai Gazdasági Térségen (EGT) kívülre történő továbbítása esetén sem sérülhet a természetes személyeknek az EU-ban biztosított védelem szintje. Az adattovábbítás csak megfelelő jogi garanciák megléte esetén jogszerű. Ilyen új, a rendelet által bevezetett jogi garanciát jelenthet a magatartási kódex és a tanúsítvány.

Személyes adatok EGT-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, ugyanúgy kell tekinteni, mintha az EU-n belül maradna a személyes adat. A biztonságos országok listája a Bizottság honlapján megtalálható.

Hasonló döntés nyomán továbbítható személyes adat az Egyesült Államokba (Privacy Shield, korábbi nevén Safe Harbour megállapodás). Az USA-ba való adattovábbításhoz további feltételek teljesülésére van szükség. Csak a Privacy Shield megállapodásban lefektetett feltételek betartását vállaló vállalatnak továbbítható személyes adat.

A fenti döntés hiányában személyes adat akkor továbbítható az Unión kívülre, ha

- az Európai Bizottság által elfogadott általános adatvédelmi *szerződéses kikötések*et alkalmazzák a felek vagy;
- olyan *kötelező erejű vállalati szabályok*at (Binding Corporate Rules, BCR) vezet be egy vállalkozás, amelyet az adatvédelmi hatóság jóváhagyott vagy;
- jóváhagyott *magatartási kódex*hez csatlakozott vállalkozásnak kerül továbbításra vagy;
- jóváhagyott *tanúsítási mechanizmus*sal 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 vagy;
- az adattovábbítás *szerződés* teljesítéséhez szükséges vagy;
- az adattovábbítás fontos *közérdek*ből szükséges vagy;
- az adattovábbítás *jogi igény*ek előterjesztése, érvényesítése és védelme miatt szükséges vagy;
- az adattovábbítás az érintett vagy valamely más személy *létfontosságú érdekei*nek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására vagy;
- a továbbított adatok olyan *nyilvántartás*ból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja.

25. Mamut 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.

26. GDPR az információbiztonsági megfelelés tükrében

A GDPR megfelelés sikerének záloga a jogi, szervezeti/folyamati és információbiztonsági szakértők együttműködése.

Az információbiztonság területén a vállalatok eddig is számtalan szabályozói és piaci elvárással találkozhattak, elég csak az egyesült államokbeli Sarbanes-Oxley törvényre vagy különböző szabványok (COSO, COBIT, ISO27001, ISO30000, NIST 800-SP53 rev4 kontrollkatalógus) követelményeire gondolni. A GDPR léte erősíti ezeket az elvárásokat, ugyanis a rendelet előírásait lehetetlen szervezeti és technikai intézkedések (folyamatok, kontrollok) bevezetése és megvalósítása nélkül megoldani.

Ezen intézkedések foganatosítása jelentős mennyiségű erőforrás befektetést igényel, de bevezetésük már középtávon is pozitív hatásokkal, értékteremtő lehetőségekkel járhat a vállalat egészére nézve. A kockázatok tudatos kezelése és az információbiztonság nem önmagukban álló területek, hanem minden esetben szorosan összefonódnak a vállalat más – termelő és nem termelő jellegű – folyamataival. Ez egyúttal azt is jelenti, hogy azok a vállalatok, amelyek eddig kevés figyelmet fordítottak a megfelelési kérdésekre, most – a GDPR okán – kénytelenek lesznek foglalkozni azokkal, ezáltal viszont egyéb kockázataikat is csökkentik majd.

Például abban az esetben, ha egy kisvállalat május után gondot fordít arra, hogy az irodáiban csak arra jogosult személyek tartózkodjanak (a személyes adatokba való illetéktelen betekintés megakadályozása miatt ez nagyon fontos), egyúttal a lopásból és adatszivárgásból származó kockázatai is mérséklődnek. Egy DLP (Data Loss Prevention) adatszivárgási védelmi rendszer bevezetése nagyon sokat segít a személyes adatok kiszivárgásának megelőzésében, egyúttal azonban hatalmas segítség a kritikus üzleti adatok – árlisták, bérjegyzékek, szerződések, szellemi tulajdon, stb. – kikerülésének megakadályozásában is.

A folyamatok és az adatkezelési gyakorlat eltérései miatt szinte lehetetlen általánosságban meghatározni a technikai és szervezeti intézkedések azon csoportját, amely valamennyi vállalat esetében kötelező eleme lesz a GDPR megfelelésnek, léteznek azonban olyan alapvető intézkedések, amelyekre érdemes különös figyelmet fordítani. A legtöbb esetben az első lépések megtételéhez leginkább józan paraszti ész és valamennyi erőforrás mozgósítása szükséges.

Már önmagában az információbiztonsági szabályzat kialakítása vagy frissítése, benne a fizikai és logikai erőforrások használatára vonatkozó szabályokkal, jelentősen emeli egy szervezet információbiztonsági érettségi szintjét. Önmagukban azonban a szabályok kialakítása nem elegendő. Nagyon fontos az alapvető szabályok rendszeres, érthető kommunikálása, tudatosítása, elsősorban a munkavállalók, majd minden érintett felé.

További fontos lépés, hogy ha sikerül vállalati szinten elfogadtatni a fontos információk (pl. személyes és üzleti adatok) elzárását, és a tiszta asztal, tiszta képernyő politikát, mert ezzel csökken az esélye a jogosulatlan betekintéseknek is. Amennyiben emellett még belső körlevéllel és más kommunikációs csatornák használatával segítünk a munkatársaknak megérteni a rendelet követelményeit, akkor megakadályozhatunk egy sor könnyen elkerülhető incidenst, amely például abból adódik, hogy egy bérszámfejtő munkatárs jóhiszeműen nem biztonságos harmadik országba továbbít személyes adatokat vagy egyszerűen rákattint egy zsarolóvírus által küldött mellékletre.

Vannak emellett olyan intézkedések, amelyek pusztán a már meglévő infrastruktúra lehetőségeinek kiaknázását igénylik. A legtöbb – informatikai eszközöket aktívan használó – vállalat tartományba (domain) rendezi számítógépeit és mobil eszközeit, melyek felett a felügyeletet valamilyen központi szerver gyakorolja. Ha az eszközökre vonatkozóan sikerül bevezetni egy egységes szabályzatot, és kikényszeríteni azt csoport házirendeken vagy felügyeleti eszközökön keresztül, akkor elérhetjük például, hogy valamennyi számítógép és mobiltelefon megfelelő jelszavas védelemmel rendelkezzen, és a tárolóegységek titkosítva legyenek, a képernyők pedig automatikusan lezárásra kerüljenek, így csökkentve az adatszivárgás és jogosulatlan hozzáférés kockázatát.

Tapasztalatunk szerint azonban a teljes megfeleléshez az előzőeken túl gyakran szükséges bizonyos nagyobb összegű befektetést igénylő intézkedések megvalósítása, amelyek komoly terheket róhatnak a vállalkozásokra. Például egy adatszivárgási védelmi rendszer (DLP) kiépítése, esetleg már bevezetett (adott esetben nagyvállalati) informatikai rendszerek átalakítása vagy a saját fejlesztésű szoftverek újratervezése a „beépített adatvédelem” alapelv megvalósítása érdekében mind-mind olyan erőfeszítéseket igényelnek, amelyek próbára tehetik a vállalatok teljesítőképességét.

Az összes eddig példaként felsorolt lépést érdemes jól megtervezni, ütemezni, és valódi értékteremtő befektetésként tekinteni, amely hozzájárul a vállalat biztonságának növeléséhez, jó hírnevének, márkaértékének erősítéséhez, átláthatóvá teszi a folyamatokat, a bennük kezelt személyes adatokat, és ezért összességében versenyelőnyt biztosít a később ébredő vagy a rendeletet komolyan nem vevő vállalatokhoz képest.

27. GDPR felkészülés 30 lépésben - ellenőrző lista

1. A vállalkozás döntéshozói tisztában vannak a GDPR által támasztott elvárásokkal? Megfelelően elkötelezettek?

2. Különített el a vállalkozásom személyi és anyagi erőforrást a GDPR-ra való felkészülésre?

3. Megvizsgáltam, hogy köteles vagyok-e adatvédelmi tisztviselőt kinevezni? Rendelkezem adatvédelmi felelőssel a vállalkozásomban?

4. Felállítottam a GDPR projektcsapatot, amiben valamennyi személyes adatot kezelő részleg (HR, IT, jog, beszerzés, marketing, belső audit stb.) képviselteti magát?

5. Rendelkezem projekttervvel, amiben lefektettem a GDPR-ra való felkészülésem legfőbb feladatait és határidejét felelősökkel együtt?

6. Azonosítottam a vállalkozásomnál kezelt valamennyi személyes adatot? Ismerem a folyamatokat, amelyekben személyes adatokat kezelek?

7. Tudom, hogy melyik folyamatban vagyok adatkezelő és melyikben adatfeldolgozó?

8. Rendelkezem adatvédelmi nyilvántartással (a bonyolultabb adatkezeléseknél adattérképpel) amely tartalmazza valamennyi kötelező tartalmi elemet (jogalap, cél, törlési határidő stb.)?

9. A jogos érdeken alapuló adatkezeléseknél elvégeztem az érdekmérlegelési tesztet?

10. Azonosítottam a magas kockázatú adatkezeléseket?

11. Elvégeztem a magas kockázatú adatkezelésekre az adatvédelmi hatásvizsgálatot?

12. Rendelkezem belső adatvédelmi szabályzattal, amely a munkavállalóim tevékenységét, illetve azok ellenőrzésének feltételeit is szabályozza?

13. Az ügyfeleim felé rendelkezem frissített adatvédelmi tájékoztatóval?

14. Az EU-n kívülre továbbítok személyes adatot? Amennyiben igen, azt milyen adatvédelmi mechanizmus alatt (megfelelőségi határozat, Kötelező Vállalati Szabályok, szerződéses kikötések stb.), milyen jogalappal teszem?

15. Készítettem tervet az adatvédelmi incidensek észlelésére/értékelésére/kezelésére/ a hatóság és az érintettek értesítésére?

16. Átnéztem a beszállítói/adatfeldolgozói szerződéseket? Azok megfelelnek a GDPR-nak?

17. Rendelkezem információbiztonságra vonatkozó stratégiával és mechanizmusokkal? Rendelkezem valamilyen bevett tanúsítvánnyal, mint például az ISO 27001 (információbiztonsági irányítási rendszer)?

18. Az információbiztonsági irányítási rendszerem megfelelő színvonalú (vírusvédelem, tűzfal, mobil eszközök védelme, VPN, megfelelő szintű titkosítás, magáncélú használat szabályozása, jelszóvédelem stb.)?

19. A fizikai biztonságra megfelelő mechanizmusokkal rendelkezem?

20. Használok felhő alapon szolgáltatásokat? Azok megfelelnek a GDPR-nak?

21. A személyes adatokhoz való hozzáférés a vállalkozásomnál megfelel az adatminimalizálás elvének? Mindenki csak olyan személyes adathoz fér hozzá, amire a munkájához feltétlenül szüksége van?

22. A honlapom megfelel a GDPR-nak? Átnéztem a direkt marketing, hírlevél küldési gyakorlatomat?

23. Az érintettek jogainak gyakorlására fel vagyok készülve (helyesbítéshez való jog, törléshez való jog, adathordózhatósághoz való jog, tiltakozáshoz való jog stb.)? Van rá megfelelő eljárásom?

24. Az ügyfél adatbázisom, CRM rendszerem megfelel a GDPR-nak?

25. Végzek profilozást (ügyfeleim szokásainak vizsgálata, hűségkártya stb.)? Ez a gyakorlatom megfelel a GDPR-nak?

26. A munkaviszonnyal kapcsolatos tevékenységeimet átnéztem, azok megfelelnek a GDPR-nak (toborzás, felvételi eljárás, képzés, bérszámfejtés, beléptető rendszer, munkaidő nyilvántartás, biztonsági kamerarendszer, munkavállalók megfigyelése stb.)?

27. Az általam gyártott, forgalmazott termékek, nyújtott vagy igénybe vett szolgáltatások (szoftverek is) megfelelnek a *beépített adatvédelem* és az *alapértelmezett adatvédelem* („privacy by design” és „privacy by default”) elveinek?

28. Elvégeztem a személyes adatot kezelő munkavállalóimnak az adatvédelmi tudatosságnövelő/képzési felkészítését?

29. Az adatvédelmi irányítási rendszerem rendszeres ellenőrzésére alakítottam ki mechanizmusokat?

30. Minden fenti tevékenységemet megfelelően ledokumentáltam az „elszámoltathatóság” elvének megfelelően?

dr. Czifra Péter, ügyvéd

dr. Frivaldszky Gáspár, ügyvéd, információbiztonsági vezető auditor

Smohay Ferenc, az ABT Adatbiztonsági Tanácsadó Kft. ügyvezető igazgatója