Vállalati Irányelv

az

RWA Magyarország Kft.

adatbiztonságra vonatkozó szervezeti intézkedéseihez

TARTALOMJEGYZÉK

1. Bevezetés és alapelvek

Az európai általános adatvédelmi rendelet (GDPR) bevezetése alapvetően megváltoztatja a vállalatok számára a személyes adatok feldolgozását. Ez kiterjeszti a személyes adatok védelmét, és e célból különleges kötelezettségeket ró a vállalatokra. A személyes adatok magukban foglalják az összes, az azonosított vagy azonosítható természetes személyekre vonatkozó adatot, akár elektronikus, akár papír alapúak. Ez magában foglalja az olyan információkat, mint a név, a cím, de a személyi szám, IP-cím vagy a járművezető GPS adata is ide tartozik. Egy személy azonosítható, ha a felelős személy vagy egy másik személy közvetlenül vagy közvetve meghatározhatja, különösen egy azonosítóhoz, például névnek azonosítószámhoz, helyadatokhoz, online azonosítóhoz, vagy egy, vagy több olyan különleges jellemzőhöz való hozzárendelése révén, amelyek a személyazonosságának kifejezését szolgálják.
Bár az ügyfelek, a beszállítók és a szolgáltatók gyakran jogi személyek, és nem tartoznak az EU GDPR védelme alá, ezekkel a vállalatokkal való kapcsolattartás magában foglalja a tulajdonosok, a vállalatvezetők vagy a munkavállalók személyes adatainak feldolgozását, ezért az EU GDPR védelmét élvezik.

A GDPR a következő elveket határozza meg, amelyeket a személyes adatok feldolgozása során figyelembe kell venni:

Törvényesség
A személyes adatok feldolgozásához jogalapot kell biztosítani.
A feldolgozás feltétele különösen akkor adott, a) ha az érintett hozzájárult a meghatározott célokra történő feldolgozásához; b) a feldolgozás szükséges a szerződés teljesítéséhez vagy a szerződéskötést megelőző cselekvés végrehajtásához, és az érintett személy kérésére történik; vagy c) az adatfeldolgozás a jogi kötelezettségek teljesítéséhez szükséges (például a szövetségi adótörvény szerinti jogi nyilvántartási kötelezettségek).

Átláthatóság és elkülönítés
A feldolgozással kapcsolatban az érintett személyeket tájékoztatni kell különösen arról, hogy kik és milyen célból dolgozzák fel személyes adataikat. Világossá kell tenni számukra, hogy az érintett személyes adatokat fel fogják dolgozni, vagy fel kell dolgozni.
A személyes adatok feldolgozása csak meghatározott, világos és törvényes célokra történhet. A célváltoztatások általában csak az érintett személy hozzájárulásával megengedhetők, vagy ha azt a nemzeti jog megengedi.

Pontosság és adatminimalizálás
A személyes adatoknak tényszerűeknek, és naprakészeknek kell lenniük. A feldolgozásnak a céljához „szükségesnek" kell lennie. Ez vonatkozik az összegyűjtött adatok mértékére, a feldolgozásuk jellegére és a tárolás időtartamára is. Az adatminimalizálás elve szerint pl. a feldolgozást a szükséges szintre kell korlátozni. Ezért mindig szükséges megfontolni, hogy az üzleti célokra ténylegesen mely adatok szükségesek. A személyes adatokat törölni kell, amint megszűnik az adatfeldolgozás jogalapja vagy célja.

Integritás és titoktartás
A személyes adatoknak az elvesztéssel, lopással és jogosulatlan vagy jogellenes feldolgozással szembeni védelmét különösen megfelelő technikai és szervezési intézkedésekkel kell biztosítani. Mindegyik feldolgozás esetén tiszteletben kell tartani a titoktartás és az integritás elvét.

A személyes adatok különleges kategóriái
A személyes adatok speciális kategóriáinak feldolgozásakor óvatosan kell eljárni. Ide tartoznak a faji és etnikai származás, a politikai vélemények, a vallási vagy ideológiai hiedelmek, vagy a szakszervezeti tagság, a genetikai vagy biometrikus adatok feldolgozása természetes személy azonosítására, egészségügyi adatok, valamint egy személy szexuális életére vagy szexuális irányultságára vonatkozó adatok. A büntető ítéletek és bűncselekmények elbírálása szintén külön szabályozott. Az ilyen jellegű adatokat csak kivételes esetekben dolgozzuk fel, és nem lehet titkosítatlan e-mailen, vagy nem megfelelően biztosított mellékleten keresztül továbbítani.

Ez a politika arra irányul, hogy szervezeti intézkedések meghozatala révén biztosítsa ezen elvek betartását.

2. Hatály és tárgy

A vállalati politikát mindegyik munkavállalónak, bérelt alkalmazottnak és szabadúszónak (együttesen „munkavállalóknak") [1] be kell tartania.
Az informatikai berendezések és a feldolgozott adatok, különösen a személyes adatok biztonságának és védelmének biztosítása érdekében cégünk valamennyi munkavállalójának felelősségteljesen és gondosan kell kezelniük az informatikai berendezéseket.

A jogi és szerződéses kötelezettségek miatt, az Ön szakmai tevékenysége során Önre bízott vagy nyilvánosságra hozott adatokat titokban kell tartani.

3. Számítógépek és adatok biztonságos kezelése

3.1. „Clear Desk Policy"

A Clear Desk Policy azt jelenti, hogy minden bizalmas adatot meg kell védeni a jogosulatlan hozzáféréstől, különösen a munkahely elhagyásakor.

- Győződjön meg arról, hogy a bizalmas információkat tartalmazó számítógéppel kinyomtatott szövegek vagy dokumentumok ne legyenek elérhetők jogosulatlan személyek számára, pl. a nyomtató mellett vagy a másolóban.
- Semmilyen körülmények között ne tárolja a jelszavakat a munkaállomáson (pl. az asztal alatt, Post-it-en a képernyőn).

[1] Mindegyik személyes megnevezés esetében a választott forma mindkét nemre vonatkozik.

- A munkaállomás elhagyásakor a számítógépet le kell zárni. Ha hosszabb időre vagy a munka végeztével hagyja el a munkaállomást, a számítógépet megfelelően ki kell kapcsolni. Ezenkívül a munkaállomás elhagyásakor minden megnyitott dokumentumot el kell menteni, hogy elkerülje az adatvesztést (pl. rendszerösszeomlás, áramkimaradás stb. miatt).

A működési adatokat, mint például a Word vagy az Excel fájlokat mindig a hálózati meghajtó megfelelő mappájába kell menteni.
Ezenkívül a működési adatokat úgy kell tárolni, hogy egy munkavállaló kiesése/hiányzása esetén a képviselője vagy a felettese hozzáférhessen ezekhez az adatokhoz.
(például egy elérhető osztály meghajtón).

Minden munkavállaló köteles rendszeres időközönként törölni azokat a fájlokat és e-maileket, amelyekre már nincs szüksége, hogy az adatok áttekinthetők maradjanak. A betartandó törlési időkre vonatkozó további információk a mellékletben találhatók.

Ha egy munkavállaló ideiglenesen (pl. szülői szabadság) vagy véglegesen elhagyja a vállalatot, törölni kell minden felesleges adatot és e-mailt, és a megmaradó adatokat a felettesével egyeztetve át kell adnia egy kollégának.
A felettesének biztosítania kell az adatok megfelelő átadását.

3.2. Papíralapú dokumentumok vagy digitális adathordozók ártalmatlanítása, pl. USB-kulcsok, merevlemezek, memóriakártyák, CD / DVD-k (archív anyagokhoz is)

Azokat a számítógépeket és digitális médiát, amelyek hibásak vagy már nem szükségesek, át kell adni a felhasználó rendszergazdájának. A titkos vagy személyes tartalmú papír alapú dokumentumokat biztonságos módon kell ártalmatlanítani, pl. megfelelő aprítással.

A tárgyalótermek elhagyásakor minden érzékeny információt (pl. a flipchart táblákon) el kell távolítani, vagy magukkal kell vinni.

3.3. Digitális kommunikáció

A személyes vagy egyéb bizalmas adatainak a védelme érdekében, amelyeket az Ön szakmai tevékenysége során bíztak Önre vagy hoztak nyilvánosságra, fokozott figyelmet kell fordítani a digitális kommunikáció használatára.

A szakmai személyes adatok privát e-mail címről való elküldése nem megengedett.
A hírközlési szolgáltatásokat (WhatsApp, Viber, Hangouts stb.) az adatvédelmi és biztonsági szempontok miatt csak különös gonddal szabad igénybe venni. Bizalmas működési információ semmilyen körülmények között nem közölhető ilyen szolgáltatással. Ezenkívül tilos ügyfelekkel megállapodást kötni ilyen szolgáltatásról és/vagy csoportokat/fórumokat létrehozni működéssel összefüggésben. Ez érvényes függetlenül attól, hogy a munkaadó által biztosított eszközöket vagy a magán eszközöket használja.

Az internet nem felejt! Soha ne feledje, hogy az interneten közzétett információk nyilvánosak, és gyakran nehéz törölni őket.

3.4. Bring Your Own Device (BYOD)

Tilos a magán informatikai eszközök működési célokra történő használata.

4. Az érintettek jogai

Ha egy érintett kéri a személyes adatairól való tájékoztatást és/vagy személyes adatainak törlését, akkor haladéktalanul továbbítsa a kérelmet az adatvédelmi tisztviselőnek, és tájékoztassa a felettesét.

Az adatok helyesbítésére vonatkozó kérelmek esetén ellenőrizze a kérelmező személyazonosságát. Minden változást be kell jegyezni.

5. A működési informatikai eszközök használata

5.1. Általános kezelés

A rendelkezésre bocsátott informatikai berendezés kezelését a megfelelő gondossággal kell végezni. Ez megakadályozza az adatok károsodását és az azokkal való visszaélést. A rendelkezésre bocsátott berendezés kizárólag hivatalos célokra használható (kivéve az alkalmankénti felhasználást az 5.4. pont szerint).
A berendezés harmadik fél általi jogosulatlan használatát megfelelő módon meg kell akadályozni.

5.2. Adatmentés és adattárolás

Az adattárolás esetében különbséget kell tenni a központi hálózati meghajtók és az Ön számára biztosított informatikai eszközön található helyi adattároló között.
Alapvetően az adatokat mindig központi hálózati meghajtón kell tárolni, mivel ebben az esetben az adatok automatikusan biztonsági mentésre kerülnek.
Ha az adatokat helyileg kell tárolni (pl. külszolgálatban mobil eszközökön), azokat rendszeres időközönként át kell tenni a vállalat központi hálózatára.

5.2.1. Magánjellegű adatok tárolása a vállalat informatikai berendezésein

A magánjellegű adatok korlátozott mértékű tárolása az e-mail és az internet alkalmanként történő magánjellegű használata során (az 5.4. pont szerint) vállalat informatikai berendezésein megengedett, feltéve, hogy a tárolás egy különálló, „MAGÁN" jelzéssel ellátott mappában történik. A vállalat nem vállal felelősséget a tárolt magánjellegű adatok elvesztéséért. Hatósági vizsgálatok esetén nem zárható ki, hogy ezeket az adatokat is megtekinti a hatóság.

5.3. Hozzáférési védelem

A RI-Solution Data GmbH által nyújtott informatikai berendezések hozzáférés védelemmel (felhasználónév és jelszó) vannak ellátva. Ne állítsa be az informatikai eszközt úgy, hogy az PIN kód vagy jelszó megadása nélkül használható legyen. Ne hagyja nyitva az eszközöket, és ne hagyja felügyelet nélkül mások előtt.

5.3.1. Hozzáférési jogosultságok

Minden munkavállaló megkapja a szükséges jogosultságokat a tevékenységi köréhez. Ha további jogosultságok szükségesek, azokat írásban kell kérni a felelős felettestől.

5.4. Alkalmi magánjellegű használat

5.4.1. E-mail és internet

Amennyire a vállalat érdekei nem szólnak az ellen, a magánjellegű használat néha megengedett.
A munkavállalóknak ezt a lehetőséget felelősségteljesen kell alkalmazniuk, miközben védeniük kell a vállalat érdekeit, és nem szabad zavarniuk a szolgáltatást.
Tiltottak a jogilag kétes, erőszakos vagy pornográf tartalmak, szerzői jogsértések, lánclevelek vagy láncleveleklhez hasonló tevékenységek, pl. párt-politikai levelezések vagy nem vállalati jellegű levelezéseket a munkavállalók csoportjainak.

5.4.2. Telefonálás

A telefon (mobil és vezetékes) magánjellegű használata korlátozott mértékben engedélyezett a meglévő átalányösszegig, amíg azt vissza nem vonják.

5.4.3. Közösségi média

Alapvetően a magánhasználatnak - azaz a magánszemélyként való megjelenésnek a közösségi hálózatokban - szigorúan el kell különülnie a szakmai használattól. Különösen tilos magánjellegű célokra felhasználói fiókot létesíteni a közösségi hálózaton, céges adatok feltüntetésével. Ebbe nem tartozik bele a vállalatnak munkaadóként való megjelölése.

A szakmai használat hatálya a felsővezető konkrét feladatától függ. Mindenesetre a kiadványoknak minden esetben meg kell felelniük a vonatkozó jogszabályoknak, különösen a szerzői jognak. Hasonlóképpen be kell tartani a megnevezett/ábrázolt személyek személyiségi jogait. Ezért mindig szerezze be az érintett személyek beleegyezését (például kollégák, felettesek), mielőtt bármilyen tartalmat, például fényképeket, videókat vagy szövegeket közzétenne. Ha másokat idéz, mindig adja meg a forrásra való hivatkozást vagy linket.

5.5. Hálózati kapcsolatok használata

A külső hálózatokon (pl. nyilvános WLAN) keresztül történő VPN-kapcsolatok esetében fokozott óvatosságot kell biztosítani a biztonság szempontjából, és a VPN-kapcsolatot azonnal aktiválni kell.
A felhasználó számára tilos a biztonsági intézkedések megváltoztatása a vállalat vagy harmadik felek számítógépein, vagy hálózatain, vagy a biztonság szempontjából releváns adatok rögzítése és átadása.

5.6. Cserélhető adathordozók használata

A cserélhető adathordozók különleges biztonsági kockázatot jelentenek, és ezért a lehető legnagyobb gondossággal és figyelemmel kell kezelni őket. Kizárólag olyan cserélhető adathordozókat szabad használni, amelyeket a vállalat szakmai használatra bocsátott ki, vagy amelyeket a munkavállaló az RI-Solution Data GmbH-val konzultálva újonnan vásárolt. Semmilyen körülmények között sem használhat saját cserélhető adathordozót.

Cserélhető adathordozó használata esetén a következő utasításokat kell betartani:

- A magánjellegű adatok vagy nem vállalati programok feltöltése a vállalat informatikai berendezéseire cserélhető adattároló eszközök segítségével nem megengedett; még vállalati cserélhető adathordozókkal sem!
- A cserélhető adathordozókat, például az USB flash meghajtókat soha ne hagyja szabadon, felügyelet nélkül!
- A cserélhető adathordozókra is vonatkozik: Minden elvesztést azonnal jelenteni kell a 7. pontnak megfelelően!

5.7. A mobil informatikai eszközök biztonságos kezelése

A mobil informatikai eszközök szállítása alapvető biztonsági kockázat. Ezért ezeket szállítás közben nem szabad felügyelet nélkül hagyni.
Nem megengedhető, hogy a mobil informatikai eszközt felügyelet nélkül hagyja az autóban vagy a tömegközlekedésben. Megfelelő figyelmet kell fordítani különösen a nem vállalati helyiségekben (konferenciatermekben, szállodákban és hasonló helyeken).

- Ne használja a saját felhő tároló szolgáltatását (például Dropbox, i-Cloud, Google Drive) a vállalati adatokhoz!
- Győződjön meg arról, hogy az olyan kapcsolatok, amelyek nem szükségesek, például a WLAN le vannak tiltva. Ez alól kivételt képez a Bluetooth funkció.
- Ha csak olyan alkalmazásokat használ, amelyek szakmai célokra hasznosak, mindenképpen megbízhatók és biztonságosak legyenek! Csak a szükséges hozzáférési jogokat szabad engedélyezni.

A vállalat által kibocsátott eszközöket csak a RI-Solution Data GmbH-n keresztül lehet kivonni a működésből. A mobiltelefonokat vissza kell szolgáltatni az adminisztráció és az objektumkezelés területének.
A mobil informatikai eszközökre is érvényes: Minden elvesztést azonnal jelenteni kell a 7. pontnak megfelelően!

5.8. Szoftver

Csak a jogszerűen engedélyezett és az RI-Solution Data GmbH által jóváhagyott szoftverek telepíthetők és használhatók. Ezek közé tartoznak a képernyővédők, a demó programok és a számítógépes játékok.

5.9. Az e-mailek kezelése

Az e-mailek és azok mellékletei károsodást okozó szkripteket tartalmazhatnak, ezért a szükséges óvatossággal kell azokat ellenőrizni. Ügyeljen a feladó megbízhatóságára. Ne nyisson meg e-mailt vagy mellékletet, ha a feladó vagy a téma gyanúsnak tűnik, és lépjen kapcsolatba a felettesével vagy az adatvédelmi tisztviselővel anélkül, hogy továbbítaná a gyanús e-mailt.
Bizalmas/érzékeny tartalom esetén győződjön meg arról, hogy soha nem küldi ezeket általános e-mail címekre (amely nem egy adott személy nevére szól - például office@...at). Kivételes esetekben forduljon a feletteséhez.

6. Központi CRM adatbázis

Az ügyfelek vagy leendő ügyfelek személyes adatait marketing célokra csak a vállalat központi CRM-adatbázisában kell szerkesztve elmenteni és mindegyik marketing tevékenység esetén (pl. levelezés, SMS, tömeglevél) kizárólag onnan kell lehívni.

7. Viselkedés az informatikai biztonság sérülése esetén/Az informatikai eszközök elvesztése

Vírusveszély, adat kémkedés, adatvesztés vagy informatikai eszközök elvesztése vagy a vállalat informatikai biztonságát befolyásoló egyéb körülmények esetén haladéktalanul tájékoztatni kell a felettest és az adatvédelmi tisztviselőt.

8. Záró rendelkezések

Mivel a vállalkozás fennállása nagymértékben függ az informatikai berendezések működésétől, a fent említett szabály(ok) közül egy vagy több megsértése súlyos károkat okozhat és a munkajogi következményekhez vezethet.

Bármely, az adatvédelemmel vagy ezzel az irányelvvel kapcsolatos kétség vagy bizonytalanság esetén forduljon a feletteséhez.

Ez az irányelv 2018. május 25-én lép hatályba.

Tóth-Ivancsik Andrea ügyvezető	Bene László ügyvezető