



A modern vállalkozásokat érintő biztonsági kihívások és megoldásuk

Az adatbiztonság és az előírásoknak való megfelelés problémája



A kiberbiztonság jelenti a modern vállalatok túlélését és sikerét veszélyeztető legnagyobb kihívást. A nagy horderejű adatvédelmi incidensek mindennaposá váltak az elmúlt években.

A hírekben rendszeresen hallhatunk olyan kiskereskedőkkel, biztosítótársaságokkal, bankokkal és technológiai vállalatokkal kapcsolatos történeteket, amelyeknek betörték az informatikai rendszerébe. A becslések szerint 2014-ben több mint egy milliárd személyes adat biztonsága sérült, és ez a szám agresszíven halad a rossz irányba.

Ezzel egyidejűleg az előírások betartására irányuló nyomás is nagyobb, mint valaha. Miközben az adatok biztonságára vonatkozó szabályozások messze nem újkeletűek, a 2018 májusában hatályba lépő általános adatvédelmi rendelet (GDPR) a vállalatokat méretüktől függetlenül felelőssé teszi a személyes adatok biztonságára vonatkozó új biztonsági szintek betartásáért – potenciálisan magas bírságokat kilátásba helyez azok számára, akik nem gondoskodnak a rendszereik és adataik megfelelő védelméről.



A helyzet

Jelentős nyomás alatt kell az adatait és információit biztonságban tartania.

Az üzleti tevékenységtől függetlenül, olyan adatok birtokában van, amelyekre a bűnözők boldogan rátennék a kezüket. Jelentős mennyiségű személyes és pénzügyi adatot őriz az alkalmazottairól. Az ügyfelei olyan kapcsolattartási adataival rendelkezik, amelyeket visszaélésekhez vagy csalásokhoz használhatnak fel. Ha nagyvállalati ügyfelekkel dolgozik együtt, akkor akaratlanul is gyenge láncszem lehet a biztonsági rendszerükben.

És mindeközben nem csupán a hekkerek miatt kell aggódnia. Mint minden más, az EU polgárainak személyes adatait kezelő vállalathoz hasonlóan, az Ön számára is közeledik a 2018. májusi határidő, hogy az adatkezelési folyamatait rendbe tegye a GDPR-ellenőrzéshez. A jelentős pénzügyi büntetések, a hírnév és az üzletmenet sérülésének elkerülése érdekében az információkezelési folyamatainak meg kell felelniük a GDPR által meghatározott szigorú, „megfelelő biztonságot garantáló” szabványoknak.

Hogyan tudhatja adatait biztonságban, hogy azok könnyen elérhetők legyenek a szabályozásoknak megfelelően, de mégse kerülhessenek internetes tolvajok kezébe? Hogyan tarthatja az ügyfeleit biztonságban, és őrizheti meg az Önbe vetett bizalmukat? Hogyan tud hatékonyan eleget tenni a GDPR követelményeinek, de közben ne zavarja meg a vállalatában a munkavégzést?

A fenyegetések



A modern vállalatok fejlődésében kulcsszerepet játszik az adatbiztonság – részben azért, hogy eleget tegyenek a szigorú előírásoknak, részben pedig, hogy védjék az érzékeny információikat az elvesztésükből, az ellopásukból vagy a támadásokból fakadó károkkal szemben.

A GDPR előírásainak való meg nem felelés jelentős költségeket vonhat maga után

A vállalkozásokat akár 20 millió €-ra vagy az éves globális forgalmuk 4%-ára is megbírságozhatják, ha megszegik a GDPR előírásait.¹

A hírnevet csorbító kár valós veszély

Az előírásoknak való meg nem felelés vagy egy adatvédelmi incidens költségei jóval meghaladják a pénzügyi veszteséget a hírnevet ért sérülés és az üzletmenet folytonosságának veszélyeztetése miatt.

A strukturálatlan adatok veszélyt jelentenek a biztonságra és az előírások betartására

Az üzleti információk 85%-a „strukturálatlan” – talán az alkalmazottak személyes eszközein vagy fizikai példányokban a fiókok mélyén tárolják – melynek, köszönhetően lehetetlen követni, az információ áramlását a vállalkozásban². A strukturálatlan információ nem pusztán a potenciális adatvesztés, a lopás vagy a támadás veszélyét növeli, hanem meg is nehezíti az adatkezelési folyamatok nyilvántartásba vételét és jelentését az előírásoknak való megfelelés ellenőrzéséhez.

Nem a méret a lényeg

Nem csak a nagyvállalatok vannak kitéve adatvédelmi incidenseknek. Valójában, a kis- és középvállalkozások (KKV-k) 60%-a számolt be adatvédelmi incidensről az elmúlt év során³. A KKV-k is a GDPR hatáskörébe tartoznak, hiszen a rendelet helyszíntől függetlenül minden olyan vállalkozásra vonatkozik, amely EU-s állampolgárok adatait kezeli.

1. EU GDPR portál, „Frequently Asked Questions about the incoming GDPR” (Gyakran ismételt kérdések a küszöbön álló GDPR-ről) a www.eugdpr.org/gdpr-faqs.html webhelyen. 2. „A Guide to Improving Document Efficiency” (Útmutató a dokumentumok hatékonyságának javításához), Ricoh tanulmány, 2013. október 3. A Quocirca 2017. évi nagyvállalati MPS tanulmánya Adatkészlet: 240, több mint 500 alkalmazottat foglalkoztató szervezet az Egyesült Királyságból, Franciaországból, Németországból és az Egyesült Államokból, különféle iparágakból.



A megoldások

Tegye rendbe (digitális) adatait

A papír alapú adatok veszélyeztetik a vállalatát, ami több, mint egy biztonsági aggály. Ezek megnehezíthetik az előírások betartását, egy fontos ügyfél adatainak elvesztése épp olyan nagy károkat okoz, mintha valaki ellopná őket. Ha pontosan ismerik az adatok helyét, könnyebben gondoskodhatnak a biztonságukról és az elérhetőségükről, amikor valakinek szüksége van rájuk. **Ismerje meg, hogy hogyan tudja hatékonyan digitalizálni, rendszerezni és védeni a dokumentumait a Ricoh Print Security Optimisation szolgáltatásaival.**

Emelje a tétet az adatbiztonságban

Miután meghatározta a vállalata által tárolt és feldolgozott személyes adatok „ki, mi, hogyan” elvét, a következő kulcsfontosságú lépés a GDPR előírásainak betartásához, ha megerősíti ezeknek az adatoknak a biztonságosságát. A lehető legmagasabb szintű tanúsítványokkal rendelkező **Ricoh multifunkciós termékekben olyan beépített biztonsági funkciók találhatóak, amelyek segítenek megvédeni a vállalkozásában áramló adatokat.**

Szabaduljon meg a felesleges adatoktól

A GDPR előírásoknak való megfelelés egyik fő eleme, hogy a vállalata csak addig őrizze az információkat, ameddig azokra szüksége van. Amikor meg kell szabadulnia a felesleges, vagy azokat az adatoktól, amelyekhez már nem szabad tovább hozzáférniük, gondoskodnia kell ezek hatékony és biztonságos eltávolításáról, beleértve az eszközökön maradt adatokat is. **A Ricoh hitelesített és auditálható Adattisztítási szolgáltatása biztonságosan távolítja el a használati vagy szerződéses élettartamuk végét elért adatokat a készülékéről.**

A GDPR előírásaiban rejlő lehetőségek

Bármennyire is ijesztőnek és kényelmetlennek tűnhet a GDPR, valójában nagyszerű lehetőség a vállalatok számára, hogy megvizsgálják a meglévő adatkezelési folyamataikat, valamint beazonosítsák és korrigálják a biztonsági hiányosságait. A személyes adatok felülvizsgálata, rögzítése, áttekintése, nem csak a GDPR előírásainak való megfelelés felé tesz lépéseket, de jelentősen megerősítse az információbiztonságot és a védelmet a kibertámadásokkal szemben. **Forduljon hozzánk, hogy segíthessünk Önnek a megfelelő információbiztonság elérésében és az adatvédelmi előírásoknak való megfelelésben.**

Forduljon
szakértőhöz

Látogasson meg minket a www.ricoh.hu webhelyen, vagy forduljon a helyi Ricoh márkaképviselethez, és ismerje meg, hogy hogyan segíthetjük a legjobb gyakorlatokra támaszkodó adatbiztonság és a szabályozói előírásoknak való megfelelés felé vezető úton.



Ricoh Hungary Kft.
2040 Budaörs
Puskás Tivadar út 14.



+36 23 806 800



www.ricoh.hu

RICOH
imagine. change.

Az ebben a brosrában közölt információk és ábrák meghatározott üzleti körülményekre vonatkoznak. Az egyedi körülmények eltérő eredményeket vonhatnak maguk után. Az összes vállalati, márká-, termék- és szolgáltatásnév a meghatározott tulajdonosok tulajdona és bejegyzett védjegye. Copyright © 2017 Ricoh Europe PLC. Minden jog fenntartva. Ez a brosrú, a tartalma és/vagy az elrendezése nem módosítható és/vagy nem kiigazítható, részben vagy egészben nem másolható, és/vagy más munkákba nem építhető be a Ricoh Europe PLC előzetes írásos engedélye nélkül.