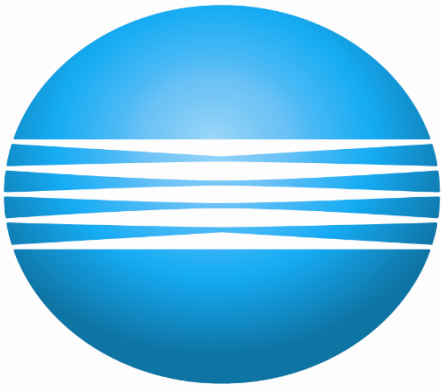

KONICA MINOLTA

A KONICA MINOLTA MAGYARORSZÁG KFT. BELSŐ ADATKEZELÉSI SZABÁLYZATA

Érvényes: 2018. május 25.-től

Bevezető

A Konica Minolta Magyarország Kft. („**Adatkezelő**”) számára kiemelkedően fontos a vállalaton belüli adatbiztonság. Üzleti folyamataink során nem kizárólag munkatársaink és a vállalat adatait kezeljük, hanem ügyfeleink, üzleti partnereink és minden olyan személyek adatait, akikkel kapcsolatba kerülünk. Az adatokkal való visszaélések lehetősége egyre növekszik, és az adatkezeléssel kapcsolatos jogszabályok szigorodnak, ezeket a kockázati tényezőket pedig hatékonyan kell kezelnünk, szem előtt tartva ugyanakkor azt is, hogy az adatokhoz való gyors és hatékony hozzáférés kulcsfontosságú az üzleti tevékenységünk során.

A jelen belső adatkezelési szabályzat („**Szabályzat**”) előírásait az Adatkezelő mindenkori adatkezelési tájékoztatóiban foglaltakkal összhangban kell alkalmazni a személyes adatok gyűjtése, kezelése és tárolása során. A jelen Szabályzatban és az adatkezelési tájékoztatókban foglaltak ismerete és maradéktalan betartása a vállalat munkájában résztvevő minden személy számára kötelező az adatvédelmi jogszabályoknak való megfelelés érdekében.

Ha bármilyen kérdése merül fel az adatvédelemmel kapcsolatban, adatvédelmi tisztviselőnk bármikor szívesen fogadja megkeresését. Elérhetősége az alábbi:

Dr. Frederike Rehker
Konica Minolta Business Solutions Europe GmbH
Europaallee 17
30855 Langenhagen, Németország
Telefon: +49 (0)511 7404-0
E-mail: dataprotection(at)konicaminolta.eu

1. Miért készült ez a Szabályzat?

1.1. Az Adatkezelő a Szabályzattal biztosítja, hogy a szervezetén belül:

- Az adatvédelmi jogszabályoknak megfeleljen és helyes gyakorlatot alkalmazzon;
- Az adatkezelés alapelveit érvényesítse;
- A munkavállalók, ügyfelek és üzleti partnerek jogait megfelelően védje;
- Az adatvédelmi incidenseket megelőzze és felmerülésük esetén kezelje őket.

1.2. Adatok, mint az üzleti tevékenységünk kulcsai

Az Adatkezelő által kezelt adatok az üzleti tevékenység végzéséhez elengedhetetlenek, ezért az adatkezelés a napi munkavégzés feltétlenül szükséges részét képezi. Az Adatkezelő különböző területeinek támogatása és működése érdekében adatok gyűjtése, kezelése és tárolása valósul meg. Ezek konkrét módja az adott terület céljaitól, működésétől és szervezetétől függ.

1.3. Adatvédelmi kockázatok

A versenyhelyzeti előny, a jövedelmezőség, a jogi megfelelőség valamint a vállalat jó hírnevének megőrzése érdekében biztosítanunk kell az adatok rendelkezésre állását, elérhetőségét, sértetlenségét és bizalmasságát. A fenti cél eléréséhez az adatvédelem érdekében biztosítanunk kell magunkat az adatvédelmi kockázatokkal szemben. A kezelt adatok komoly támadásoknak lehetnek célpontjai, amelyekkel szemben hatásos fizikai és informatikai eszközökkel kell védekeznünk. Fizikai

fenyegetés többek között a papír alapon tárolt adatok eltűnése, megsemmisülése, eltulajdonítása, természeti és egyéb katasztrófák bekövetkezése; informatikai fenyegetés többek között az üzleti kémkedés, számítástechnikai csalás, számítógépes vírusok és hackertámadások.

A kezelt adatok természetétől függően különböző mértékű kockázatokkal kell számolni, a vállalatra gyakorolt hatásokat mérlegelve. Néhány példával szemléltetjük az adatkezeléssel járó lehetséges kockázatokat:

- Titoktartási kockázat, pl. ha egy ügyfél bepereli a vállalatot, amiért az adatait jogosulatlanul harmadik féllel közöltük.
- Üzleti kockázat, pl. ha a kezelt adatok hiányossága, pontatlansága rossz üzleti döntések meghozatalát eredményezik.
- Felügyeleti bírság kockázata, pl. ha az adatkezelés jogszerűtlensége esetén a felügyelő hatóság bírsággal sújtja a vállalatot.
- Jó hírnév sérelme, pl. ha hackerek érzékeny adatokhoz férnek hozzá, és ezeket közzéteszik.

1.4. Adatkezelési alapelvek

Az adatvédelemmel kapcsolatos hazai és Európai Uniós jogszabályok alkalmazandók függetlenül attól, hogy az adatokat elektronikusan, papíralapon vagy más módon tárolják. A törvénynek való megfelelés érdekében a személyes adatokat megfelelő módon kell gyűjteni és kezelni, azokat biztonságosan kell tárolni, és tilos azokat jogellenesen megosztani.

Az adatvédelmi jogszabályok alapján az adatkezelés legfontosabb alapelvei a következők:

- az adatkezelés tisztességes és jogszerű;
- az adatokat kizárólag jogszerű célokból lehet hozzáférhetővé tenni;
- az adatok gyűjtése nem túlzó mértékű;
- az adatok pontosak és naprakészek;
- az adatok a szükségesnél hosszabb időn túl nem kezelhetők;
- az adatokat az érintettek jogainak megfelelően kezelik;
- az adatok megfelelő védelmét biztosítják;
- Az adatok az Európai Gazdasági Térségen (EGT) kívülre nem továbbíthatók, kivéve, ha az adott ország vagy terület megfelelő szintű védelmet biztosít

2. Kikre és milyen adatokra vonatkozik a Szabályzat?

2.1. A Szabályzat az alábbi személyekre vonatkozik:

Az Adatkezelő minden vezetőjére, munkavállalójára, beszállítójára és nevében vagy képviseletében eljáró más személyekre.

2.2. A Szabályzat az alábbi adatokra vonatkozik:

A Szabályzat az Adatkezelő által kezelt álló minden személyes adatra vonatkozik. Személyes adat az azonosított vagy azonosítható természetes személyre vonatkozó bármely információ. Azonosítható az a természetes személy, aki közvetlen vagy közvetett módon (különösen például név, szám, helymeghatározó adat, online azonosító) alapján azonosítható.

Ha valamilyen információ vagy dokumentum személyes adat jellege kérdéses, akkor ajánlott azt a kockázatok elkerülése érdekében személyes adatként kezelni mindaddig, amíg az információ jellege egyértelműen nem tisztázódik.

3. Milyen hatásköröket határoz meg a Szabályzat?

A 2.1. pont hatálya alá tartozó valamennyi személy felelősséggel tartozik és köteles biztosítani, hogy a személyes adatok gyűjtése, tárolása és kezelése a jogszabályoknak és a mindenkori adatkezelési tájékoztatóban foglaltaknak megfelelően történjen.

3.1. A vezetőség hatáskörei

- Az Adatkezelő vezetősége gondoskodik a megfelelő technológiai védelmi és szervezési intézkedéseket meghatározásáról és biztosítja ezek végrehajtását;
- Az adatvédelmi incidensek bekövetkezésekor konzultál az adatvédelmi tisztviselővel, vagy ha ilyen tisztség nincs, külső szakértőt von be és ezek útján az adatvédelmi incidenst haladéktalanul bejelenti a felügyeleti hatóságnak;
- Gondoskodik az Adatkezelő által végzett adatkezelési tevékenységek nyilvántartásának vezetéséről.

3.2. Az adatvédelmi tisztviselő hatáskörei

- Megbizonyosodik arról, hogy a technológiai védelmi és szervezési intézkedések végrehajtásra kerültek;
- Adatvédelmi incidens bekövetkezte esetén megteszi a jogszabályban előírt intézkedéseket és együttműködik a vezetőséggel;
- A vezetőséget tájékoztatja az adatvédelmi feladatokról, kockázatokról és problémákról;
- Ellenőrzi az adatkezelési jogszabályoknak való megfelelést (információgyűjtés, adatkezelési tevékenységek elemzése, ajánlások megfogalmazása);
- Adatvédelmi képzést és tanácsadást nyújt a Szabályzat hatálya alá tartozó személyeknek;
- A munkavállalók adatvédelmi kéréseit kezeli és kérdéseiket megválaszolja;
- Az érintettek adatkezelésre vonatkozó kérelmeit kezeli;
- Az adatok kezelésével megbízott harmadik felekkel kötött megállapodásokat ellenőrzi;
- Együttműködik a felügyeleti hatósággal és kapcsolattartó pontként szolgál a felügyeleti hatóság felé az adatkezeléssel összefüggő ügyekben, valamint adott esetben bármely kérdésben konzultációt folytat vele;
- Jóváhagyja a különböző marketingkommunikációk, nyereményjátékok, feliratkozási lehetőségek során alkalmazott adatvédelmi nyilatkozatokat és tájékoztatásokat;
- Kezeli az újságírók vagy más média szolgáltatók adatvédelmi megkereséseit;
- Szükség esetén más munkavállalókkal is együttműködik, hogy a marketingcélok megvalósítása során az adatvédelmi elvek betartását megfelelően biztosítsa.

3.3. Az IT vezető hatáskörei

- Felügyeli, hogy az adatok tárolására használt valamennyi rendszer, szolgáltatás és berendezés megfelelően biztonságos és rendeltetésszerűen működik;
- Rendszeres ellenőrzéseket végez a hardverek és szoftverek biztonságos működése érdekében;
- Értékeli az olyan harmadik felek szolgáltatásait, amelyeket az Adatkezelő az adatok tárolásával vagy kezelésével bízott meg

4. Adatbiztonsági előírások

4.1. Általános adatvédelmi rendelkezések

- Biztosítani kell, hogy kizárólag olyan személyek férjenek hozzá az adatokhoz, akiknek azokra a munkájuk során szükségük van; ennek érdekében az elektronikus adatokat tároló rendszereket

megfelelő jogosultságkezeléssel kell ellátni, a papír alapon tárolt adatokat pedig megfelelő fizikai védelemmel, tárolási- és irattározási módszerekkel kell védeni.

- Biztosítani kell, hogy az adatokat tartalmazó számítógépek és más elektronikus eszközök, illetve adathordozók, valamint papír alapú dokumentumok ne maradjanak felügyelet nélkül.
- Személyes adatok informális módon, akár szóban, akár írásban vagy elektronikusan (pl. privát emailcím vagy chat szolgáltatás útján) nem oszthatók meg abból a célból sem, ami miatt kezelik őket.
- Az Adatkezelő szükség szerint oktatást vagy felvilágosítást biztosít minden munkavállalójának az adatvédelmi kötelezettségeik teljesítéséhez.
- Az alkalmazottaknak haladéktalanul értesíteniük kell közvetlen felettesüket és/vagy az adatvédelmi tisztviselőt, ha bármilyen gyanúra okot adó körülményt észlelnek (pl. számítógépes vírust) vagy adatvédelmi incidens jut a tudomásukra (pl. adatokat tartalmazó USB elvész)
- Az adatokat a szükség szerinti legkevesebb helyen szabad tárolni.

4.2. Az adatok tárolása

4.2.1. Papíralapon tárolt adatok

- Gondoskodni kell arról, hogy a papíralapú iratok és a kinyomtatott dokumentumok ne legyenek olyan helyen, ahol jogosulatlanok láthatják azokat.
- Amikor nincs szükség az adatokra, akkor a papírokat vagy a fájlokat zárt fiókban vagy tároló szekrényben kell tárolni.
- Ha az adatokat tartalmazó dokumentumokra már egyáltalán nincs szükség, azokat iratmegsemmisítőben meg kell semmisíteni.
- A kinyomtatott anyagokat és beérkező faxokat haladéktalanul be kell gyűjteni, elkerülve azt, hogy illetéktelenek az adatokat megismerhessék.
- Ha valamilyen dokumentum megtekintése csak adatellenőrzéshez szükséges (pl. személyi igazolvány) vagy más adatkezelő részére lesznek továbbítva, kerülni kell a dokumentumokról való másolatkészítést.

4.2.2. Elektronikusan vagy adathordozón tárolt adatok

- Az adatok elektronikus tárolása esetén azokat védeni kell az illetéktelen hozzáféréstől és a véletlen törléstől.
- Az adatokat olyan biztonságos jelszavakkal kell védeni, amelyeket rendszeresen megváltoztatnak, és amelyeket az alkalmazottak egymással nem osztanak meg.
- Az adatokat csak a kijelölt meghajtókon és kiszolgálókon lehet tárolni, és azok kizárólag megfelelő felhőalapú szolgáltatásokra tölthetők fel.
- Ha az adatot hordozható adathordozón (például CD-n vagy DVD-n) tárolják, ezeket biztonságosan el kell zárni, amikor azokat nem használják.
- Az adatokat gyakran kell biztonsági menteni, és a biztonsági mentések integritását rendszeresen ellenőrizni kell.
- Minden adatot tartalmazó kiszolgálót és számítógépet jóváhagyott biztonsági szoftvernek és tűzfalnak kell védenie.
- Az adatokat nem szabad megosztani arra jogosulatlan személyekkel. Az adatokat rendszeresen felül kell vizsgálni és frissíteni, ha azt észlelik, hogy azok elavultak. Ha már nem szükségesek az adatok, törölni kell azokat.
- Az alkalmazottak kötelesek iránymutatást kérni a felettesüktől vagy az adatvédelmi tisztviselőtől az adatvédelemmel kapcsolatos bármely felmerülő kérdés esetén.

4.2.3. Adatok továbbítása, az elektronikus levelezésre vonatkozó előírások

Az adatokat nem szabad informális módon megosztani. Különösen nem szabad adatokat titkosítatlan e-mailben továbbítani, ugyanis a kommunikációnak ez a formája nem biztonságos.
Az adatokat e-mailben történő továbbítás előtt minden esetben titkosítani kell. Az IT vezető ad tájékoztatást arra vonatkozóan, hogy az adatok hogyan továbbíthatók biztonságosan engedélyezett külső kapcsolatok részére.
Személyes adatokat az Európai Gazdasági Térségen kívülre a felettes vagy adatvédelmi tisztviselő kifejezett engedélyével lehet továbbítani.

4.2.4. Az adatok pontossága

- A jogszabályok alapján az Adatkezelő minden ésszerű lépést megtesz annak biztosítása érdekében, hogy az általa kezelt adatok pontosak és naprakészek legyenek.
- Minden adatokkal dolgozó alkalmazottnak kötelessége ésszerű lépéseket tenni annak biztosítása érdekében, hogy az adatok a lehető legpontosabbak és naprakészek legyenek.
- Az alkalmazottaknak minden lehetőséget meg kell ragadniuk az adatok naprakésszé tételére. Például, hogy amikor az ügyfelekkel telefonálnak, egyúttal egyeztetik az adataikat is.
- A Társaság az érintettek számára megkönnyíti a tárolt adataik frissítését. Például a cég weboldalán lehetőség szerint biztosít erre lehetőséget.
- Az adatokat frissíteni kell, ha pontatlanságokat fedeznek fel. Például, ha egy ügyfél már nem érhető el a tárolt telefonszámán, akkor azt el kell távolítani az adatbázisból.

4.2.5. Tájékoztatáshoz való jog

Minden személy, akinek az Adatkezelő személyes adatát kezeli, jogosult tájékoztatást kapni többek között arról, hogy milyen adatokat kezelnek róla, hogy azokhoz hogyan jutottunk hozzá, hogyan történik az adatok naprakészen tartása és hogy a vállalat hogyan biztosítja az adatvédelmi kötelezettségeknek való megfelelést.

Ha egy személy kapcsolatba lép ilyen információk megszerzése érdekében, ezt az érintett hozzáférési kérésének nevezzük. Az adatkezelő a kért adatok átadását megelőzően a hozzáférési kérelmet benyújtó személy személyazonosságát minden esetben ellenőrzi. Az érintettek hozzáférési kéréseit az alkalmazottak kötelesek továbbítani a felettesüknek vagy az adatvédelmi tisztviselőnek.

Az Adatkezelő alkalmazottai szintén jogosultak tájékoztatást kapni a vállalattól a kezelt adataikról a vonatkozó adatkezelési tájékoztatóban foglaltak szerint.