Cégnév (a továbbiakban Adatkezelő): Art-Light Bt
Képviseli: Kovács András, ügyvezető
Székhely:
Cégjegyzékszám:

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

2024. február 13.

Tartalomjegyzék

ELŐZMÉNYEK

Adatkezelő szolgáltatása iránt érdeklődők személyes adatait, megbízói, vásárlói, beszállítói kapcsolati adatait, valamint számlázási adatokat kezel, amiket megoszt adatfeldolgozóival, illetve különböző technológiák használatával megoszt azok szolgáltatóival (egyéb címzettekkel).

Jelen Szabályzat az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (a továbbiakban: GDPR) és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: Infotv.) foglalt rendelkezések alapján az adatvédelem és az adatbiztonság rendjét az alábbiak szerint szabályozza.

Az Adatkezelő valamennyi adatkezelési tevékenysége során biztosítja a GDPR rendelkezéseinek betartását.

E Szabályzat rendelkezéseit meg kell ismertetni az Adatkezelő valamennyi foglalkoztatottjával és az egyéb munkavégzésre irányuló szerződésekben elő kell írni, hogy a Szabályzat betartása és érvényesítése minden foglalkoztatottra nézve kötelező.

.....

Kovács András

ügyvezető

Adatkezelő képviselője

I. FEJEZET
ÁLTALÁNOS RENDELKEZÉSEK

1. A Szabályzat célja

A Szabályzat célja, hogy **meghatározza** a természetes személyek személyes adatainak, Adatkezelő által történő kezelésének l**egfontosabb adatvédelmi szabályait,** különös figyelemmel az adatkezeléssel, adatfeldolgozással, adattovábbítással kapcsolatos adatvédelmi követelményekre.
A Szabályzat célja, valamint meghatározni a szükséges adatvédelmi és adatbiztonsági szabályokat a személyes és különleges adatok **véletlen vagy jogellenes megsemmisítése, elvesztése megváltoztatása, vagy jogosulatlan felhasználásuk megakadályozása érdekében**.

2. A Szabályzat hatálya

A Szabályzat személyi hatálya kiterjed az Adatkezelőre és vele munkavégzésre irányuló egyéb jogviszonyban állókra.
A Szabályzat tárgyi hatálya kiterjed az Adatkezelő által kezelt valamennyi személyes adatra, a velük végzett adatkezelési- és feldolgozási műveletek teljes körére, keletkezésük, felhasználásuk, feldolgozásuk helyétől, valamint megjelenési formájuktól (elektronikus és/vagy papír alapon) függetlenül.
A Szabályzat időbeli hatálya annak kihirdetésétől visszavonásáig érvényes.

3. Felelősség

A szabályzat betartásáért minden munkatárs felelős.
Mindenki köteles gondoskodni arról, hogy jogosulatlan személyek ne tekinthessenek be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.
Az Adatkezelő, munkatársai és az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek munkatársai és megbízottjai (alvállalkozói) kötelesek:

- az adatkezelés során megismert személyes adatokat titokként megőrizni, jogviszonyukat követően is;
- a tudomásukra jutott adatkezeléssel kapcsolatos jogsértésekről haladéktalanul tájékoztatni a felettesüket és az Adatkezelő képviselőjét;

II. FEJEZET
AZ ADATKEZELÉSRE VONATKOZÓ SZABÁLYOK

4. Az adatkezelés célja, jogalapja

Az Adatkezelő:

a) a rendeltetésszerű működéséhez;
b) a munkáltatói jogok gyakorlásához, illetve a foglalkoztatottak jogainak gyakorlásához és kötelezettségeik teljesítéséhez;
c) a tevékenységével összefüggően szolgáltatás nyújtása érdekében nélkülözhetetlenül szükséges személyes adatokat kezeli.

Az Adatkezelő személyes adatot mindig valamely jogalap fennállása esetén kezelhet, melyek az alábbiak lehetnek: hozzájárulás/ olyan szerződés teljesítése, amelyben az Érintett az egyik fél/ jogi kötelezettség/ létfontosságú érdek/ közérdek/ jogos érdek (érdekmérlegelési teszttel alátámasztva).
A hozzájárulás szabályai: önkéntes; konkrét; megfelelő, előzetes tájékoztatáson alapul; az érintett akaratának kifejezett kinyilvánítása; utólag igazolható; bármikor, könnyen, negatív következmények nélkül visszavonható; 16. év korhatár alatt törvényes képviselő által tehető. Az Adatkezelő a visszavonás tényét az adatkezelés során rögzíti és az adatot a továbbiakban nem kezeli.

Különleges adat kezelése - Adatkezelő által - csak az Érintett kifejezett hozzájárulásával, mint jogalappal történhet.

Jogos érdek jogalap esetén az érdekmérlegelési tesztet az Érintett kérelmére rendelkezésre kell bocsátani.

Jogos érdek mérlegelése - jogi személyek vagy egyéb szervezetek kapcsolattartói személyes adatainak adatkezeléséhez: Adatkezelő tevékenysége során kezeli azoknak az érintetteknek a személyes adatait, akiket a társaságunkkal üzleti kapcsolatot létesítő jogi személyek, illetve jogi személyiséggel nem rendelkező társaságok (egyéb szervezetek) kapcsolattartójukként jelölnek ki. Az adatkezelési tevékenység magában foglalja az érintettek elérhetőségi adatainak, így többnyire nevének, titulusának, telefonszámának és e-mail címének kezelését is. Adatkezelő jogos érdekében áll a szolgáltatása iránt érdeklődő, vagy azt igénybe vevő gazdasági társaságokkal történő hatékony és gyors kapcsolattartás, a partner illetékes munkatársaival, megbízottjaival való közvetlen egyeztetés és kommunikáció, melyhez elengedhetetlen a kapcsolattartó személyek adatainak kezelése. Kapcsolattartói adatok kezelésének hiányában adatkezelőnek a szerződött partner általános elérhetőségein kellene kapcsolatot tartania a partnerrel, ami megnehezítené a kapcsolattartást és az üzletmenet folytonosságát. A kapcsolattartóként kijelölt természetes személyek észszerűen számíthatnak arra, hogy a szerződés fennállása alatt a kapcsolat felvételéhez, illetve folyamatos fenntartásához szükséges személyes adataikat munkáltatójuk, illetve megbízójuk az Adatkezelő, mint üzleti partner részére átadja, ugyanis ez az érintett által végzett feladatok ellátásához szorosan kapcsolódó körülmény. Nem áll fenn az adatkezelő jogos érdekén kívül más jogalap, ami a személyes adatok kezelését lehetővé tenné, beleértve a hozzájárulás jogalap lehetőségét is, aminek teljesítése a felek között fennálló szerződéses kapcsolat fennállását teljesen ellehetetlenítené (pl. minden egyes kapcsolattartótól előzetesen be kellene szerezni a hozzájárulást), valamint a hozzájárulás valamennyi fogalmi eleme nem tudna érvényesülni. A személyes adatok adatkezelő jogos érdekén alapuló kezelése szükségesnek és arányosnak tekinthető az adatkezelés valamennyi aspektusát figyelembe véve. A kapcsolattartó adatainak kezelése nem jár kifejezett előnnyel az érintettre nézve, de az adatkezelés olyan körülmény, amely az érintett és a partner között fennálló jogviszonyhoz szorosan kapcsolódik, abból értelemszerűen következik. Adatkezelő biztosítja a GDPR 6. cikk (1) bekezdésének f) pontja szerinti jogalap alkalmazásához szükséges biztosítékok és garanciák érvényesülését. Az adatkezelés során nem sérülnek vagy korlátozódnak az érintettek jogai, jogos érdekeit, alapvető szabadságai olyan mértékben és módon, hogy az adatkezelést korlátozni vagy módosítani kellene a lehetséges hatások csökkentése érdekében.

5. Az adatkezelés elvei

Személyes adat kizárólag egyértelműen meghatározott **jogszerű célból** kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének **tisztességesnek és törvényesnek** kell lennie, valamint az adatkezelést az érintett számára **átlátható** módon kell végezni.

Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához **elengedhetetlen**, a cél elérésére alkalmas. A személyes adat **csak a cél megvalósulásához szükséges mértékben és ideig kezelhető**, figyelemmel a jogszabályokban meghatározott megőrzési kötelezettségre.

A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

Az adatkezelés során biztosítani kell az **adatok pontosságát, teljességét** és – ha az adatkezelés céljára tekintettel szükséges – **naprakészségét**, valamint azt, hogy **az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani**.

Az Adatkezelő az adatkezelés során arra alkalmas technikai és szervezési intézkedések alkalmazásával biztosítja a személyes adatok megfelelő biztonságát.

6. Az érintett előzetes tájékoztatásának követelménye

Adatkezelőnek az érintett személyt az adatkezelésről és a jogairól tájékoztatni kell, adatkezelési műveletek megkezdését **megelőzően vagy legkésőbb az adatok megszerzésének időpontjában**.

Ha Adatkezelő a személyes adatokat az érintettől gyűjti be, a tájékoztatást az adatfelvételkor, **utólag igazolható módon** kell megadni, például az ezt tartalmazó dokumentumot az érintettel aláíratni. Elektronikus adatkezelés esetén a könnyen hozzáférhető adatkezelési tájékoztató meglétét rögzíteni, hozzájárulás jogalap esetén annak megadását naplózni kell.

Ha az Adatkezelő a személyes adatokon a megszerzésük céljától **eltérő célból** további adatkezelést kíván végezni, a **további adatkezelést megelőzően tájékoztatnia kell** az érintettet erről az eltérő célról és minden releváns kiegészítő információról.

Ha személyes adatokat **nem az érintettől** szerezték meg, az Adatkezelő az adatok megszerzését követő ésszerű határidőn belül (**maximum 1 hónap**) bocsátja a tájékoztatást az érintett rendelkezésére.

Az érintett tájékoztatását a személyes adatok kezeléséről **tömören, átláthatóan, érthetően és könnyen hozzáférhető és olvasható formában, világosan és közérthetően** megfogalmazva kell megtenni.

7. Az adatkezelésben Érintettet megillető jogosultságok és az Érintett jogai érvényesülésének biztosítása

Érintett a **hozzájárulását bármikor, negatív következmények nélkül visszavonhatja,** kérheti a személyes adathoz való **hozzáférést**, illetve azok **helyesbítését**, **törlését, kezelésének korlátozását, hordozását, tiltakozhat** a személyes adatok kezelése ellen, **panaszt tehet** és **jogorvoslatot kérhet** a Hatóságnál vagy Bíróságnál, valamint jogorvoslatot kérhet Hatósággal, Adatkezelővel vagy Adatfeldolgozóval szemben.

8. Az érintetti kérelmek kezelése

Az Adatkezelő az Érintett kérelmét, a kérelem benyújtásától számított legrövidebb idő alatt, de legfeljebb **egy hónapon belül elbírálja** és az Érintettnek közérthető formában, írásban választ ad.
Adatkezelő az Érintett kérelmét csak és kizárólag abban az esetben teljesíti, ha **meggyőződött az Érintett személyazonosságáról**.
A kérelem teljesítését úgy kell biztosítani, hogy ez alatt az **Érintett más személy adatait ne ismerhesse meg.**
A **kérés teljesíthetősége függ az adatkezelés jogalapjától**, például jogi kötelezettség (pl. Számviteli tv.) esetén a kérelmet el kell utasítani.
Az adatkezelő minimális adatkezelési aktivitása miatt külön nyilvántartásokat nem vezet.
Az Adatkezelő az érintetti kérelmek tényét az adatkezelés során elektronikus rendszereiben, külön mappában rögzíti, és az adatot a továbbiakban a kérelemnek megfelelően kezeli vagy nem kezeli.

9. Az adatkezelési tevékenységek azonosítása és nyilvántartása

Az Adatkezelőnél végzett minden, személyes adatokkal kapcsolatos adatkezelést adatkezelési céllal kell meghatározni és nyilvántartani.
Az adatkezelő minimális adatkezelési aktivitása miatt külön nyilvántartásokat nem vezet.
Az adatkezelések nyilvántartását egyben az Adatkezelési tájékoztató tartalmazza.
Adatfeldolgozói tevékenység nincs.

10. Eljárás adatfeldolgozó igénybevétele esetén

Ha az Adatkezelő adatfeldolgozásnak minősülő szolgáltatást – pl. könyvelés, IT szolgáltatás, vagyonvédelem, rendezvényszervezés, futárszolgálat stb. – vesz igénybe, akkor a szerződés megkötésekor, jogviszony létrejöttekor a külső szolgáltatótól **meg kell követelnie a GDPR-ban előírt garanciák teljesítését (használandó dokumentum: Adatfeldolgozói szerződésbe_Személyes adatok kezelésére vonatkozó kikötések).**

11. A személyes adatok tárolási időtartamát követő feladatok

Adatkezelő a GDPR 5. cikk (1) bekezdés e) pontja szerinti, „a személyes adatok korlátozott tárolhatósága” alapelvnek történő megfelelés biztosítása érdekében jelen Szabályzatban az alábbiakat határozza meg:
Adatkezelő **a személyes adatokat az adatkezelési, adatfeldolgozói tevékenységek nyilvántartásában foglalt, adatkategóriák törlésére előirányozott határidőkben törli, vagy igény esetén visszaadja.** Adatkezelő a határidők nyilvántartását **dokumentumkezelő nyilvántartással (használandó dokumentum: „Dokumentumkezelő nyilvántartás”)** vagy **dokumentumkezelő szoftver igénybevétel biztosítja.** A **közeljövőben aktuális határidők felülvizsgálatára havonta, a hónap utolsó munkanapján kerül sor**, az azt követő hónapban - az adatkezelési cél megszűnését követően - pedig **az adatok visszaállíthatatlanul törlésre, a dokumentumok megsemmisítésre vagy visszaadásra kerülnek**.
A cél megvalósulását követően lehet szó biztonsági mentésben történő további megőrzésről, a **biztonsági mentések előre meghatározott megőrzési idejének megfelelően** (egy biztonsági mentés jellemzően fél-1 évnél tovább nem őrizhető meg).

Az adatmegőrzési kötelezettséget az adatok eredeti példányán kell érvényesíteni. Például a papír alapon kibocsátott számlák esetében hiába tárolja el máshol (pl. szkennelve) az

Adatkezelő a teljes számlaképet, jogszabály szerint nem ezt kell megőriznie, hanem a papír alapú eredeti példányt. Mindazonáltal, ha vannak mentett példányok, legkésőbb a kötelező törlési időpontban azokat is törölni kell.

III. FEJEZET
AZ ADATTOVÁBBÍTÁS SZABÁLYAI

12. Az adattovábbítás rendje

Az adattovábbítást megelőzően Adatkezelő és/vagy Adatfeldolgozó **megvizsgálja a továbbítandó személyes adatok pontosságát, teljességét és naprakészségét**.
Amennyiben a továbbítandó adatok pontatlanok, hiányosak vagy már nem naprakészek, azok kizárólag abban az esetben továbbíthatók, ha

a) az az adattovábbítás céljának megvalósulásához elengedhetetlenül szükséges, és
b) az adattovábbítással egyidejűleg tájékoztatja a címzettet az adatok pontosságával, teljességével és naprakészségével összefüggésben rendelkezésére álló információkról.

Személyes adat továbbítása csak abban az esetben lehetséges, ha az adattovábbítás **jogalapja egyértelmű, célja és az adattovábbítás címzettje pontosan meghatározott.**

13. Adattovábbítás külső megkeresés alapján

Az Adatkezelő szervezetén kívüli szervtől vagy magánszemélytől érkező, személyes adatokat érintő adatközlésre irányuló megkeresés **csak törvényben meghatározott esetekben, vagy** abban az esetben teljesíthető, ha az érintett ehhez írásban **hozzájárulását adta**.
Adatkezelő az adattovábbításról adattovábbítási nyilvántartást köteles vezetni az **„Adatvédelmi nyilvántartások" dokumentum „Adattovábbítási nyilvántartás" oldalán.**

14. Adattovábbítás külföldre

Adattovábbítás azzal is megvalósul, ha multinacionális tevékenységű technológiai vállalatok által kínált szolgáltatásokat vesz igénybe az Adatkezelő, például Social Media felületeket, szoftver csomagokat, tárhelyszolgáltatókat.
Az **EGT-államba** irányuló adattovábbítást úgy kell tekinteni, **mintha Magyarország területén** belüli adattovábbításra kerülne sor.
Személyes adat **EGT-n kívüli, harmadik országba vagy nemzetközi szervezet** részére történő, jogszerű továbbításához a következő feltételek valamelyikének megléte szükséges:
I. Adattovábbítás **megfelelőségi határozat** alapján (megfelelő országok listája: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)
II. Adattovábbítás **megfelelő garanciák** alapján, ezek lehetnek:

- Általános adatvédelmi kikötések és egyéb szerződéses rendelkezések
- BCR (Kötelező erejű vállalati szabályok)
- Magatartási kódex és tanúsítás
- Közhatalmi és közfeladatot ellátó szervek által alkalmazható eszközök

III. **Különös helyzetekben** biztosított eltérések 49. cikk (kivételes jogalapok):

- Az érintett megfelelő, a kockázatokra is kiterjedő tájékoztatást követően kifejezetten hozzájárult a tervezett továbbításhoz
- Az érintett és az adatkezelő közötti szerződés teljesítéséhez szükséges
- Az adatkezelő és valamely más személy közötti, az érintett érdekét szolgáló szerződés

megkötéséhez vagy teljesítéséhez szükséges
- Fontos közérdekből szükséges
- Jogi igények előterjesztése, érvényesítése és védelme miatt szükséges
- Az érintett vagy más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen megadni hozzájárulását
- A továbbított adatok a nyilvánosság tájékoztatását szolgáló nyilvántartásból származnak

IV. FEJEZET
AZ ADATBIZTONSÁG

Adatkezelő, illetőleg tevékenységi körében Adatkezelő által megbízott Adatfeldolgozó köteles gondoskodni az adatok biztonságáról. Ahhoz, hogy az adatkezelő **igazolni tudja** a rendeletnek való megfelelést, olyan belső szabályokat kell alkalmaznia, valamint olyan technikai és szervezési intézkedéseket kell végrehajtania, amelyek teljesítik a GDPR, különösen a beépített és az alapértelmezett adatvédelem elveit.
Adatkezelő az adatbiztonsági folyamatait úgy alakítja ki, hogy azok a személyes adatokat **megvédjék a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.**
Adatkezelő törekszik - a GDPR-nak való megfelelés érdekében - **a személyes adatok kezelésének minimálisra csökkentésére, a személyes adatok mihamarabbi álnevesítésére**, a személyes adatok funkcióinak és **kezelésének átláthatóságára**, valamint arra, hogy az Érintett nyomon követhesse az adatkezelést, a Adatkezelő pedig biztonsági elemeket hozhasson létre és tovább fejleszthesse azokat.

15. Fizikai védelmi intézkedések

Védendő helyiségnek kell tekinteni minden helyiséget, ahol számítástechnikai eszközöket, papíralapú dokumentumokat tartanak, tárolnak.
A védendő helyiségeket el kell látni:
- a mechanikai védelemmel: a bejárati ajtókat biztonsági zárral, szükség esetén ráccsal,
- betöréses lopás- és rablás jelzésére alkalmas elektronikus vagyonvédelmi jelzőrendszerrel,
- tűzjelző berendezéssel és poroltóval, az épületet villámhárítóval.

A papíralapon kezelt személyes adatok biztonsága érdekében a Adatkezelő az alábbi intézkedéseket alkalmazza:
- az adatokat **csak az arra jogosultak ismerhetik meg**, azokhoz más nem férhet hozzá, más számára fel nem tárhatók;
- a dokumentumokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben helyezi el;
- a Adatkezelő adatkezelést végző munkatársa a nap folyamán csak úgy hagyhatja el az olyan helyiséget, ahol adatkezelés zajlik, hogy a rá bízott adathordozókat elzárja, vagy az irodát bezárja;
- a Adatkezelő adatkezelést végző munkatársa a munkavégzés befejeztével a papíralapú adathordozót elzárja;
- amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat alkalmazza a Adatkezelő.
- Személyazonosító igazolványok fénymásolása, fotózása, scannelése: a GDPR szükségesség és a célhoz kötöttség elvének való megfelelés érdekében Adatkezelő **nem készít fénymásolatot, vagy elektronikus másolatot semmilyen formában személyazonosító igazolványokról.**

16. Informatikai biztonsági intézkedések

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében a Adatkezelő **az alábbi intézkedéseket és garanciális elemeket** alkalmazza:

- az adatkezelés során használt **számítógépek a Adatkezelő tulajdonát képezik, vagy azok fölött tulajdonosi jogkörrel** megegyező joggal bír;
- Az adatkezelőnél **csak jogtiszta** – vásárolt, vagy üzleti használatra is ingyenes - **szoftverek** használhatók.
- a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható **jogosultsággal** - legalább **felhasználói névvel és jelszóval** – lehet csak hozzáférni, a jelszavak cseréjéről a Adatkezelő rendszeresen, illetve indokolt esetben gondoskodik;
- **kétlépcsős hitelesítést** kell alkalmazni felhőben tárolt adatok elérésére;
- az adatokkal történő minden számítógépes rekord nyomon követhetően **naplózásra** kerül;
- amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul **törlésre** kerül, az adat újra vissza nem nyerhető;
- a személyes adatokat kezelő hálózaton a **vírusvédelem**ről folyamatosan gondoskodik;
- a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával **megakadályozza illetéktelen személyek hálózati hozzáférését**.

Elektronikus levelezés, e-mail fiók, adattovábbítás védelme:

Csak olyan levelezőrendszer használható, amelynél biztosított a rendszer és azok elemei, különösen a szerverek **fizikai és logikai védelme**, a kéretlen és kártékony kódot tartalmazó elektronikus levelek kiszűrése és blokkolása.

Különleges és érzékeny személyes adatokat elektronikus levelezésben **titkosítottan kell** továbbítani: e-mail titkosítása vagy dokumentum titkosítása formában.

Az Érintettek értesítése elektronikus kapcsolattartás során:

Abban az esetben, ha az Adatkezelő bármely munkatársa az Érintett számára elektronikus levelet küld, az Érintett elektronikus levélcímét köteles a küldés során úgy megjelölni, hogy az az elektronikus levél egyetlen címzettje számára se legyen látható. Ezt az Adatkezelő munkatársai elsősorban **„titkos másolat”-tal** történő címzéssel kötelesek megtenni, de a Adatkezelő kidolgozhat olyan üzenetküldő rendszert (például hírlevélküldésre), amely alapvető beállításként, további emberi beavatkozás nélkül automatikusan így küldi meg az információt az Érintettek számára.

17. Adatvédelmi ellenőrzés

A Szabályzat rendelkezéseit az uniós vagy magyar, adatkezelést érintő **jogszabályok változásakor, új adatkezelések bevezetésekor, de legalább 3 évente egyszer felül kell vizsgálni.** Az adatvédelmi ellenőrzés az ütemtervben meghatározottakon túl **szúrópróbaszerűen,** vagy az adatvédelmi **incidens kivizsgálása során** tett megállapítás (pl. adatkezelésre vonatkozó előírás be nem tartása vezetett az incidens bekövetkezéséhez) következményeként is végezhető.

V. FEJEZET

AZ ADATVÉDELMI ELŐÍRÁSOK MEGSÉRTÉSE

18. Az adatvédelmi incidens

Adatvédelmi incidens: **a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.**

Az adatvédelmi incidenst az adatkezelő köteles indokolatlan késedelem nélkül, és ha lehetséges, **legkésőbb 72 órával azután**, hogy az adatvédelmi incidens a tudomására jutott, **bejelenteni** az illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

A leggyakrabban előforduló incidenstípusok és a kockázatcsökkentő intézkedések:

1. **Téves címzett** részére küldött postai vagy elektronikus levelek:
   - Postai küldemény esetén Adatkezelőnek válaszborítékkal együtt küldött újabb levélben kérnie kell a téves címzettet a nem neki szóló küldemény visszaküldésére.
   - E-mailben téves címzett részére küldött személyes adatokat tartalmazó dokumentum esetén fel kell kérni a téves címzettet az üzenet és csatolmányainak törlésére.
2. **Ellopott, elveszett** számítástechnikai eszközök, telefonok.

Az incidensről való tudomásszerzést követően Adatkezelőnek haladéktalanul azonosítania kell, hogy az eszköz használója milyen adatokhoz, szerverekhez fért hozzá. A további hozzáférés megakadályozása (letiltás, jelentés) szükséges

19. Az adatvédelmi incidens észlelése és továbbítása

Az Adatkezelő **minden munkatársa** köteles a biztonságot érintő összes esemény (incidens) bekövetkezése esetén **haladéktalanul értesítenie** felettesét és az az Adatkezelő képviselőjét (együtt: Felelősök).

20. Az adatvédelmi incidens kivizsgálása

Amennyiben az incidens még folyamatban van, ha lehetséges, a Felelősök intézkednek annak **megállításáról és kezeléséről** (következmények, okok, felelősök feltárása, dokumentáció, jövőbeni tervszerű megelőzés kidolgozása). Amennyiben szükséges, további adatokat kérnek az incidensre vonatkozóan.

Felelősök kivizsgálják, hogy az incidens **kockázattal jár-e** a természetes személyek jogaira és szabadságaira nézve.

A vizsgálatot legkésőbb a bejelentés beérkezésétől számított **48 órán belül be kell fejezni**.

21. Az adatvédelmi incidens értékelése

Az adatvédelmi incidens **kockázattal jár** a természetes személyek jogaira és szabadságaira nézve **például:**

- az adatkezelésből hátrányos megkülönböztetés,
- személyazonosság-lopás vagy személyazonossággal való visszaélés,
- pénzügyi veszteség,
- a jó hírnév sérelme,
- a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése,
- az álnevesítés engedély nélkül történő feloldása, vagy

- bármilyen egyéb jelentős gazdasági vagy szociális hátrány fakadhat; vagy ha
- az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy
- nem rendelkezhetnek saját személyes adataik felett; vagy ha
- olyan személyes adatok kezelése történik, amelyek faji vagy etnikai származásra, vagy politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utalnak, valamint ha
- a kezelt adatok genetikai adatok, egészségügyi adatok vagy a szexuális életre, büntetőjogi felelősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó biztonsági intézkedésekre vonatkoznak; vagy ha
- személyes jellemzők értékelésére, így különösen munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet, egészségi állapot, személyes preferenciák vagy érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére vagy előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából; vagy ha
- kiszolgáltatott személyek – különösen, ha gyermekek – személyes adatainak a kezelésére kerül sor; vagy ha
- az adatkezelés nagy mennyiségű személyes adat alapján zajlik, és nagyszámú érintettre terjed ki.

22. Az adatvédelmi incidens bejelentése a NAIH-nak

Amennyiben az incidens **vélhetőleg kockázattal jár** az Érinettek jogaira és szabadságaira, úgy legkésőbb **72 órával azután**, hogy az adatvédelmi incidens a Adatkezelő tudomására jutott, az adatvédelmi incidenst **bejelenti a NAIH-nak**. A bejelentést nem kell elhalasztani addig, amíg az incidenssel kapcsolatos kockázat és hatás teljes körű felmérése meg nem történik, mivel a teljes körű kockázatértékelés a bejelentéssel párhuzamosan is megtörténhet.
A NAIH-nak történő bejelentés itt tehető meg: https://www.naih.hu/tudnivalok-az-adatvedelmi-incidensek-kezeleserol

23. Az Érintettek tájékoztatása az adatvédelmi incidensről

Amennyiben az adatvédelmi incidens veszélyességének **súlyossága valószínűsíthetően magas** kockázattal jár az Érintett személyek jogaira nézve, a Adatkezelő a kockázati értékelés elvégzését követően azonnal **tájékoztatja az adatvédelmi incidensben Érintetteket**.
Az Érintetteket írásban elektronikus vagy postai úton kell tájékoztatni, amely kizárólag akkor mellőzhető, ha az Érintett elérhetősége ismeretlen.
Az Érintetteket úgy kell tájékoztatni minden esetben, hogy annak ténye, tartalma és a tájékoztatott Érintetti kör bizonyítható legyen.

24. Helyesbítő-megelőző intézkedések bevezetése

A vizsgálat eredménye alapján Adatkezelő helyesbítő és/vagy megelőző intézkedéseket vezet be a hasonló adatvédelmi incidensek megelőzése érdekében.

25. Az adatvédelmi incidens nyilvántartása

Az adatkezelő minimális adatkezelési aktivitása miatt külön nyilvántartásokat nem vezet.
Az Adatkezelő az incidens körülményeit és kezelését az **elektronikus rendszereiben, külön mappában menti el és tárolja.**

VI. FEJEZET

ÉRTELMEZŐ RENDELKEZÉSEK

A Szabályzat alkalmazásában:

Adatbiztonság: az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere.

Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől).

Adatfeldolgozó: az személy vagy szervezet, aki/amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi.

Adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése

Adatkezelő: az a személy vagy szervezet, aki/amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott Adatfeldolgozóval végrehajtatja

Adatmegsemmisítés: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése,

Adattovábbítás külföldre: személyes adatok továbbítása EGT-n (Európai Gazdasági Térség: az Európai Unió országai, valamint Izland, Norvégia és Liechtenstein) kívüli, harmadik országban adatkezelési tevékenységet folytató adatkezelőhöz;

Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele,

Adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges

Adatvédelem: a személyes adatok jogszerű kezelését, az Érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége;

Azonosítható természetes személy: az természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági,

Címzett: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz,

Érintett: bármely információ alapján azonosított vagy azonosítható természetes személy, akinek személyes adatait az Adatkezelő kezeli;

Érzékeny adat: állami azonosítók [társadalombiztosítási szám, vezetői engedély], pénzügyi információk [hitelkártya, bankszámla], konkrét földrajzi hely, nyitott szövegmezők, ahol nemkívánatos események fordulhatnak elő, autós baleset feljegyzések, viták és peres ügyek feljegyzései, munkabiztonsági feljegyzések stb.

Felügyeleti hatóság: egy tagállam által a GDPR 51. cikkének megfelelően létrehozott független közhatalmi szerv, ez Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH).

Harmadik ország: minden olyan állam, amely nem EGT-állam,

Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek,
Hozzájárulás: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez,
Különleges adat: a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre, az egészségi állapotra, valamint a kóros szenvedélyre vonatkozó és a bűnügyi személyes adat;
Nyilvántartási rendszer: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;
Profilalkotás: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.
Személyes adat: bármely meghatározott, azonosított vagy azonosítható természetes személlyel [Érintett] kapcsolatba hozható adat és az adatból levonható, az Érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az Érintettel helyreállítható. Az Érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek
Személyes adatok határokon átnyúló adatkezelése:
személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy Adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy
személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az Adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint Érintetteket (GDPR 4. cikk 23.);