Kalipron Kft.
1107 Budapest, Basa utca 26.
Fax: 06/1 470-80-51 E-mail: kalipron@enternet.hu

Adatvédelmi incidens kezelés szabályzat

Az adatkezelő KALIPRON Kft., továbbiakban Adatkezelő, Magyarország Alaptörvényében foglaltakkal és az információs önrendelkezési jogról és az információszabadságról szóló 2011. CXII. törvény (a továbbiakban: Info tv.), valamint az Európai Parlament és a Tanács (EU) 2016/679 (2016. április 27.) számú általános adatvédelmi rendelete (a továbbiakban: „*GDPR*") rendelkezéseivel összhangban, a személyes adatok védelmének biztosítása érdekében az alábbiak szerint alkotja meg adatvédelmi incidensekre vonatkozó szabályzatát.

1. Adatvédelmi incidens definíciója:
Adatvédelmi incidens a biztonság bármely 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 (a továbbiakban: „Adatvédelmi jogsértést" eredményezi).

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat az érintetteknek, többek között:

- a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását;
- a hátrányos megkülönböztetést;
- a személyazonosság-lopást vagy a személyazonossággal való visszaélést;
- a pénzügyi veszteséget;
- az álnevesítés engedély nélküli feloldását;
- a jó hírnév sérelmét;
- a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését;
- a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

2. Adatvédelmi incidens, illetve bármely lényeges észrevétel bejelentése
Társaságunk Incidens kezelő rendszert vezetett be Informatikai Biztonsági Rendszerében rögzítettek szerint, az esetlegesen bekövetkező adatvédelmi incidensek kimutatása, kezelése, jelentése érdekében. Ez a fenyegetettséget és a behatolást is észleli, a naplóállományok bejegyzése az abban rögzítetteknek megfelelően az Informatikai vezető feladata.
Az informatikai rendszerben történt incidenst az Informatikai vezető jelenti az ügyvezetőnek, és ketten döntenek a kivizsgálásról, a kezeléséről, a kockázatának felméréséről, és amennyiben szükséges, határidőn belüli bejelentéséről.

Társaságunk adatokat átadhat feldolgozásra, szerződéses jogviszonyban más Adatkezelőknek, pl. könyvelésre, banki utalásra, munkaügyi ügyintézésre. Szerződésében mindig kiköti az adatkezelés biztonságát, GDPR előírások és szabályzatának való megfelelőségét. Az Adatfeldolgozó a lehetséges adatvédelmi incidenst, vagy annak csak a gyanúját is, az arról való tudomásszerzését követően 72 órán belül elektronikus módon köteles bejelenti az Adatkezelőnek.

Adatvédelmi incidenst észlelhet Társaságunk, mint Adatkezelő bármely dolgozója, alvállalkozója, felhasználó, ügyfél, bárki. A fentiekben említettek, bármely Adatfeldolgozó munkatársa, vezetője, külső fél az általunk kezelt, továbbá Adatfeldolgozóink által kezelt

adatokkal kapcsolatos bármilyen adatvédelmi jogsértés bejelentésére az Adatkezelő az alábbi email-címen működteti, melyet saját web-oldalán tesz közzé:

info@kalipron.hu

Adatkezelőként biztosítjuk, hogy a megadott elérhetőséget folyamatos ellenőrzés alatt tartjuk. Adatkezelő munkatársa a lehetséges adatvédelmi incidensről, az arról való tudomásszerzését követően azonnal elektronikus módon köteles tájékoztatni az ügyvezetőt, illetve munkaügyi adatok esetében a Munkaügyi vezetőt is, informatikai incidens esetén az informatikai vezetőt is.

3. Adatkezelő által vállalt kötelezettségek, adatvédelmi bejelentés kezelése

3.1. Bejelentés, észrevétel nyilvántartási rendszere

Társaságunk, az ügyvezetője felelőssége mellett az adatvédelmi megbízott segítségével az adatvédelmi incidens bekövetkeztekor a GDPR rendelkezéseinek megfelelően nyilvántartást vezet az adatvédelmi incidensekről.
Ezen nyilvántartás tartalmazza az egyes adatvédelmi incidensekhez kapcsolódó tényeket, azok hatásait és az orvoslásra tett intézkedéseket, a NAIH felé megküldendő információkat.
Az incidens vizsgálatát és kezelését - a NAIH honlapjáról letölthető - papíralapú incidens-bejelentő lap (Melléklet) kitöltésével, vagy azzal egyező adattartalmú bizonylattal kell dokumentálni. Az adatvédelmi incidens részleteinek rögzítéséhez javasolt nyilvántartási rendszert az alábbiakban egy konkrét példával mutatjuk meg.
sorszám, pl 01/2018.
Dátum: pl. 2018.01.28.
Az incidens leírása: pl. titkárság rossz helyre küldött emailt
Tudomásszerzés az incidensről: pl fogadó fél jelezte, maga a titkárság jelezte
Adatvesztés leírása: részletesen, konkrétan, egyértelműen. Pl. Legalább egy harmadik fél tudomást szerzett a szerződésben szereplő személyes adatokról.
Incidens természetes jellegének megnevezése, pl. a példánál: Téves mail küldés. Egy követeléskezelőnek szerettük volna átküldeni néhány adósunk adatait, de a mailcímük eleje megegyezett egy másik partnerével és emiatt tévedésből rossz helyre küldtük ki az adatokat.
Incidenssel érintettek száma, adatai, az adatok bizalmi kategóriája: pl. x db, magas
Az incidens következményeinek hatása: nem felmérhető, nem tudni, lényegtelen
Meghozott intézkedések (korrekció) pl, az érintettek értesítése
Javító intézkedések: Az alkalmazottaink figyelmét ismételten felhívtuk a levelezőrendszer megfelelő használatára, a hibalehetőségekre.
Hatósági értesítés: igen, NAIH értesítés dátuma: xxx
Ügy lezárása és dátuma: pl. 2018.02.01.
Adatvédelmi megbízott elérhetőségei: megadásra kerülnek ide.

3.2. Adatvédelmi incidens kivizsgálása és minősítése

Az ügyvezető a hozzá beérkezett adatvédelmi jogsértés bejelentést vagy belső rendszerében észlelt jogsértés gyanúját 72 órán belül megvizsgálja az előző pontban is rögzítettek szerint, és dönt arról, hogy a lehetséges jogsértés kockázatot jelent-e az érintett jogaira és szabadságaira nézve.
Az ügyvezető által a vizsgálatra kijelölt személyek:
Az Adatkezelő ügyvédje, Dr. Váradi Katalin
Informatikai vezetője, Süller József
Munkaügyi vezetője: Jeremiásné Kertész Éva
Adatvédelmi megbízott: Farkas Dorottya
És bárki, akit az ügyvezető bevonni kíván.

Az ügyvezető a vizsgálatba bevont személyekkel együtt minősíti az incidenst a körülmények ismeretében, de döntenek bármelyikük javaslata alapján arról is, hogy eseti szakértői megbízást adnak az incidens körülményeinek kivizsgálására.
Informatikai incidens esetén az informatikai biztonsági vezető, az incidens súlyának ismeretében tesz javaslatot az ügyvezető felé a következményekről, az incidens kezeléséről a hibák javításáról. Ezzel egyidőben az informatikai biztonságban résztvevők és szükség szerint az informatikai vagy szakmai rendszergazdák bevonásával a riasztásokban szereplő sérülékenység elhárítására haladéktalanul intézkednek.
A biztonsági esemény kivizsgálásának eredménye ismeretében az ügyvezető dönt a további esetleges fegyelmi, jogi eljárásról.

3.4. Az incidens kezelésével összefüggő feladatok:

- Incidens azonosítása, a személyes adatok száma, fajtája, speciális tulajdonságai, érintett személyek száma, köre),
- Incidens minősítését bizonyító dokumentumok és adatok, közlések vizsgálata
- Incidens által bekövetkezett kár, kockázat, vészhelyzet és sérelem meghatározása (milyen kockázatot jelent az érintett személy(ek) jogaira és szabadságára tekintettel)
- Incidens okainak feltárása (kiváltó okok és körülmények, körülmények összejátszása, együttes hatása, amelyek az incidens bekövetkeztéhez vezethettek).
- Elhárítás érdekében teendő, megtett intézkedések meghatározása
- Incidens minősítése: téves, valós, alacsony vagy nagy kockázatú stb.
- Incidens bejelentésére vonatkozó döntés meghozatala
- Teljes vizsgálat megindítására intézkedés igény szerint
- Érintettek tájékoztatása
- Kapcsolattartás a NAIH-val.

4.Téves bejelentés kezelése
Abban az esetben, ha a vizsgálat alapján bebizonyosodik, hogy nem történt adatvédelmi jogsértés, vagy Társaságunk, mint Adatkezelő az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, akkor az illetékes felügyeleti hatóság felé történő bejelentés mellőzhető.
Erről az Adatkezelő tájékoztatja az esetleges bejelentőt és lezárja az ügyet.
Pl. Ide tartoznak azok az esetek, amikor megfelelő intézkedések – mint például titkosítás alkalmazása – a személyes adatokhoz való hozzáférés jogosulatlan személyek számára nem biztosított, így a személyes adatok nem értelmezhetőek a titkosításhoz használt kulcs nélkül. Ugyanakkor megfelelő titkosítás mellett is fennállhat a bejelentési kötelezettség olyan esetekben, ha az adatvédelmi incidenssel érintett személyes adatokról nem áll rendelkezésre megfelelő biztonsági mentés/backup.

5. Bizonyított adatvédelmi incidens

5.1. Hatósági bejelentés
Amennyiben a vizsgálat alapján bebizonyosodik, hogy adatvédelmi jogsértés történt, azt a tudomásszerzést követő 72 órán belül az ügyvezető az adatvédelmi megbízott bevonásával bejelenti az illetékes felügyeleti hatóság felé, kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.
Ha fentieknek megfelelően az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, akkor nem kell bejelentenie a hatóságnak, de az incidenst akkor is nyilvántartásba kell venni.

Az adatvédelmi incidensről szóló bejelentést a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) mindenkori kapcsolati pontjára (http://naih.hu/uegyfelszolgalat,--kapcsolat.html) kell eljuttatni.
A bejelentés összeállításának és beadásának felelőse az ügyvezető, annak konkrét megbízásából az adatvédelmi megbízott, informatikai adatvédelmi incidens esetén fentiek tájékoztatása, bevonása mellett, az informatikai biztonsági vezető.
Az adatvédelmi incidensről szóló, az illetékes felügyeleti hatóság felé tett bejelentésben legalább:

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
b) közölni kell a további tájékoztatást nyújtó egyéb kapcsolattartó, vagy az adatvédelmi megbízott nevét és elérhetőségeit;
c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d) ismertetni kell a Társaságunk által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.
e) Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.
f) az adott adatvédelmi incidens sajátosságaira tekintettel Társaságunk fenntartja magának a jogot arra, hogy a bejelentésben további, az ügy szempontjából lényeges információkat tüntessen fel.

Társaságunk jogszabályi kötelezettségének megfelelően nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

Előfordulhat, hogy ezen bejelentés 72 órán belül nem tehető meg, a bejelentést így is meg kell tenni, de a megtett bejelentésben Társaságunk megjelöli a késedelem igazolására szolgáló indokokat is, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben közli.

Az adatvédelmi incidens előírásoknak megfelelő bejelentéséért a mindenkori ügyvezető felel, több cégvezető esetén a cégvezetők egyetemlegesen, külön-külön bejelentési kötelezettséggel és jogosultsággal felelnek.

5.2. Nagy kockázattal járó jogsértettség közlése az érintettel

Amennyiben a vizsgálat alapján bebizonyosodik, hogy valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, úgy Társaságunk képviseletében az ügyvezető (vagy delegáltja, de az ügyvezető felelősségére) indokolatlan késedelem nélkül, elvárható időben, amennyiben lehetséges, legkésőbb a tudomásszerzést követő 72 órán belül az ügyvezető köteles tájékoztatni az érintette(ke)t is az adatvédelmi incidensről.
Az érintett részére adott tájékoztatásban világosan és közérthetően kell ismertetni

- az adatvédelmi jogsértés jellegét,
- közölni vele a felügyeleti hatóság felé kötelezően tett bejelentés adattartalmát,
- és felvilágosítást kell adni mindazon lépésről, melyekkel az érintett megvédheti magát a jogsértés következményeitől.

Az érintett részére adott tájékoztatást minden esetben külön üzenet formájában (e-mailen, ennek hiányában postai levél útján) továbbítjuk.

Nem szükséges az érintett adatvédelmi jogsértésről való tájékoztatása, ha Társaságunk, mint adatkezelő, akár Adatfeldolgozója bevonásával is úgy intézkedik, hogy a következő feltételek bármelyike is teljesül:

- megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazta;
- az adatvédelmi jogsértést követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján (pl. honlapon közlemény közzétételével) érdemes tájékoztatni, amely biztosítja az érintettek n hatékony tájékoztatását.

6. Záró rendelkezések

Jelen Szabályzatban nem szabályozott kérdésekben a mindenkor hatályos Adatkezelési Szabályzat rendelkezései az irányadók azzal, hogy a jelen Szabályzat és az Adatkezelési Szabályzat közötti bármely eltérés esetén az Adatkezelési Szabályzatban előírtak, illetve a hatályos előírásokba foglaltak az irányadók.

Jelen szabályzat 2018. május 25 napjától hatályos visszavonásig vagy módosításáig.

Jelen Adatvédelmi Incidens Kezelési Szabályzat a Társaságunk általi közzététellel, azaz honlapunkon való elhelyezésétől is hatályosul és határozatlan időtartamra szól (visszavonásakor vagy későbbi módosított Szabályzat közzétételével veszti el hatályát).

Jelen Szabályzattal kapcsolatosan felmerülő bármely kérdés vagy észrevétel esetén az alábbi elérhetőségeken állunk bárki érintett rendelkezésére:
Levelezési cím: 1107 Budapest, Basa utca 26.
e-mail: info@kalipron.hu
web: www.kalipron.hu

…….
Ügyvezető