Adatvédelmi incidens kezelési Szabályzat

Székhely: 7100 Szekszárd, Bezerédj u. 2.

KÉSZÜLT: 2020.

adatvédelmi tisztviselő igazgató

Preambulum

A személyes adatok védelme érdekében feladatok kerülnek megfogalmazásra, azért, hogy érvényesüljenek az adatok kezelésével, feldolgozásával kapcsolatos különböző jogszabályok előírásai. Adatvédelmi szempontból biztosítani kell az EU Parlament 2016. május 16-án hatályba lépett adatvédelmi rendelet adatbiztonsági követelményeinek megfelelve, a nagy tömegű személyes adatok, az adatkezelésre használt rendszer bizalmas jellegét, integritását, elérhetőségét és rugalmasságát, a fizikai vagy műszaki probléma esetén a visszaállíthatóságát, rendelkezésre állását és hozzáférhetőségét.

Az irányadó szabályokat a rendelet 33.,34.,55. cikkei és a preambulum 85.-88. pontjai tartalmazzák.

Jelen szabályozás a Szekszárdi Vagyonkezelő Kft. és tagvállalatai Adatvédelmi Szabályzatának biztonságpolitikai elveire épülve készült.

A szabályozás célja, hogy a holding minden tagvállalata részére egységes keretbe foglalja az adatvédelmi incidenssel kapcsolatos eljárási követelményeket, intézkedéseket, amelyeket az Adatkezelő valamennyi alkalmazottjának - a rávonatkozó mértékben - ismernie és a biztonsági követelmények érvényesítése érdekében alkalmaznia kell.
Biztosítani az adatvédelmi incidens, rendkívüli esemény, katasztrófa elhárításra, bekövetkezése esetén a szükséges intézkedésekre, valamint a rendkívüli időszakban a kötelezettségekre történő adatvédelmi felkészülést, illetve bekövetkezésük esetén az üzemszerű és adatvédelmi működőképességet.

1. A Szabályzat hatálya, érvényesítése:

1.1. A Szabályzat **területi hatálya**:

Kiterjed az Adatkezelő és tagvállalatai teljes működési területére, valamennyi alkalmazott informatikai eszközre és szoftverre.

1.2. A Szabályzat **személyi hatálya**:

Kiterjed az Adatkezelővel munkaviszonyban vagy munkavégzésre irányuló jogviszonyban álló valamennyi természetes és jogi személyre.

1.3. A Szabályzat **időbeli hatály**a:

A kiadás napjától visszavonásig érvényes.

1.4. A Szabályzat **érvényesítés**e és a megismerési kötelezettség:

A Szabályzat kidolgozása, elkészítése és szükség szerinti módosítása az adatvédelmi incidens-kezelési csoport feladata.
A Szabályzatban előírtak betartatásáért hatás- és jogosultsági körére vonatkozóan minden érintett alkalmazott felelős.

A Szabályzatban előírtak betartásának ellenőrzése az érintett szervezeti egység vezetőjének feladata.
A Szabályzat előírásait az Adatkezelőnél dolgozó minden személy a szakmai feladatköréhez szükséges mértékben köteles megismerni, a vonatkozó előírásokat betartani és betartatni.

1.5. A Szabályzat egyes előírásait, a munkavégzéséhez szükséges mértékben, minden, az Adatkezelővel munkaviszonyban, illetve egyéb szerződéses jogviszonyban álló foglalkoztatottal ismertetni kell.

1.6. A Szabályzat előírásait megszegőkkel, illetve a jelentési kötelezettséget elmulasztókkal szemben, a hatályos törvényeknek, rendeleteknek és belső szabályzatnak megfelelő, jogszerű felelősségre vonást kell alkalmazni.

2. Adatvédelmi incidenst kezelő csoport

A csoport döntést hozó vezetője a Szekszárdi Vagyonkezelő Kft. igazgatója,
tagjai:

adatvédelmi tisztviselő
rendszergazda
Szekszárdi Vagyonkezelő Kft. jogi képviselője,
részleg vezetője (HR, IT, Ügyfélszolgálat),

3. Az incidens kezelésével összefüggő feladatok:

- ✓ incidens azonosítása,
- ✓ incidens minősítését bizonyító adatok, dokumentumok vizsgálata,
- ✓ incidens által bekövetkezett kockázat, kár, veszélyhelyzet meghatározása,
- ✓ elhárítás érdekében teendő intézkedések meghatározása,
- ✓ incidens bejelentésére vonatkozó döntés meghozatala,
- ✓ incidens okainak feltárása,
- ✓ érintettek tájékoztatása,
- ✓ teljes vizsgálat megindítása igény szerint,
- ✓ kapcsolattartás a NAIH-val.

4. Adatvédelmi incidens azonosítása, minősítése, típusa:

A biztonságnak olyan sérülése, amely által a tárolt, továbbított vagy más módon kezelt adatok véletlen vagy jogellenes módon megsemmisül, elvész, megváltozik, jogosulatlanul közlésre kerül, vagy jogosulatlan hozzáférést eredményez.

- ➢ Személyes adatok feletti rendelkezés elvesztése,
- ➢ jogok korlátozása,
- ➢ hátrányos megkülönböztetés,
- ➢ személyazonosság-lopás vagy azzal való visszaélés,
- ➢ pénzügyi veszteség,
- ➢ az álnevesítés engedély nélküli feloldása,
- ➢ jóhírnév sérelme,

- titoktartási kötelezettség megszegése által bizalmas jelleg sérülése,
- gazdasági vagy szociális hátrány.

Az azonosítást követően a minősítés érdekében tisztázni kell az alábbiakat:

4.1. Milyen kockázatot jelent az érintett természetes személy(ek) jogaira és szabadságaira tekintettel.

4.2. Kiváltó okok, körülmények, amelyek az incidens bekövetkezéséhez vezettek. Az incidens bekövetkezésének körülményei.

4.3. A személyes adatok érzékenységének meghatározása,

4.4. Az incidensben érintett személyes adatok száma.

4.5.Az érintett adatok fajtái, ill. az érintetti kör speciális tulajdonságai.

5. Adatvédelmi incidens jelentése:

5.1. Az adatvédelmi incidenst az érintett tagvállalat vagy részleg, ill. az adatfeldolgozó a tudomására jutást követően indokolatlan késedelem nélkül azonnal jelenti az adatvédelmi incidenst kezelő csoport valamely állandó tagjának;

5.2. Ismertetnie kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

5.3. Közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

5.4. Ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

5.5. Ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is;

5.6. A csoport döntése alapján bejelenti az adatvédelmi incidenst (legfeljebb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott), a GDPR 55. cikk alapján illetékes felügyeleti hatóságnak, NAIH-nak.

Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

Ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, akkor nem kell bejelentenie a hatóságnak, de az incidenst nyilvántartásba kell venni.

Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

6. Az érintett tájékoztatása az adatvédelmi incidensről:

- Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.
- Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell az intézkedéseket is.
- Az érintettet nem kell tájékoztatni, ha az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
- az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az (1) bekezdésben említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.
- Ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását.

7. Az adatvédelmi incidensek nyilvántartása:

Az adatvédelmi nyilvántartás a NAIH által ajánlott és kitöltött bejelentő lapok (Melléklet) alapján, azok iktatásával és elektronikus másolatának tárolásával valósul meg, mely a teljes felsorolás nélkül az alábbiakat tartalmazza:

- az incidens jellege, az adatvédelmi incidenshez kapcsolódó tények, annak hatásai,
- érintettek kategóriái és száma,
- adatok kategóriái és száma,
- valószínűsíthető következmények,
- az incidens következményei elhárítására, következmények enyhítésére tett és tervezett intézkedések,

Az adatvédelmi incidensek nyilvántartását az adatvédelmi tisztviselő/felelős vezeti elektronikus dokumentumban, excel táblázatban.
A nyilvántartás része az incidenssel kapcsolatos vizsgálódás dokumentumának elektronikus másolata.
Az incidens vizsgálatát és kezelését - a NAIH honlapjáról letölthető - papíralapú incidens-bejelentő lap (Melléklet) kitöltésével kell dokumentálni.