

Adatbiztonsági és adatvédelmi incidens szabályzat

1 Szabályzat célja

Jelen Szabályzat célja a Személyes Adatok biztonságára vonatkozó szabályok, valamint a Személyes Adatok biztonságának sérülése esetén követendő eljárás rögzítése.

2 Szabályzat hatálya

Jelen Szabályzat valamennyi az Alapítvány alkalmazottja vagy megbízottja által folytatott tevékenység esetén irányadó a Személyes Adatok biztonságára, illetve a Személyes Adatok biztonságának sérülésére vonatkozóan.

3 Személyes Adatok biztonsága

Az Alapítvány a Személyes Adatok fizikai biztonsága érdekében a következő intézkedéseket teszi:

- az Alapítvány telephelye, ahol az Adatkezelési tevékenység végzésére sor kerül olyan épületben van, amit zárt kerítés és zárt kapu véd, illetve kapucsengő megnyomását követően lehet a telephelyre bejutni;
- az Alapítvány telephelyének ajtaja állandóan zárva van, oda csak az ajtónyitógomb megnyomását követően és az ajtó belülről történő kinyitását követően lehet bejutni, az ajtóhoz kizárólag az Alapítvány munkatársai rendelkeznek kulccsal;
- az Alapítvány telephelyének ablakait rács védi;
- az Alapítvány riasztóberendezéssel rendelkezik, amit valamennyi olyan esetben bekapcsol, ha egyetlen személy sem tartózkodik a telephelyen;
- az Alapítvány a Személyes Adatok papíralapú kezelésének biztonsága érdekében a külön szabályzatokban, illetve az Adatkezelési tevékenységek nyilvántartásában meghatározottak szerint egyes Személyes Adatokat tartalmazó dokumentumokat páncélszekrényben, más Személyes Adatokat tartalmazó dokumentumokat zárt szekrényben, illetve zárt irodában tárol, továbbá szervezeti intézkedés útján biztosítja, hogy az egyes Személyes Adatokat tartalmazó dokumentumokhoz csak az arra jogosult munkatársak férjenek hozzá.

Az Alapítvány az elektronikusan kezelt Személyes Adatok biztonsága érdekében a következő logikai biztonsági intézkedéseket teszi:

- az Alapítvány a felhasználói profilokat hozott létre, amiket az egyes informatikai rendszerekhez hozzárendelt;
- az Alapítvány informatikai rendszerében az egyes felhasználókhöz felhasználói jogosultságokat rendelt hozzá;
- az Alapítvány tulajdonában álló számítógépek és laptopok operációs rendszerét jelszó védi;
- az egyes, személyes adatokat tartalmazó programokba felhasználónév és jelszó megadását követően lehet belépni;
- a számítógépek és laptopok meghatározott idő elteltével automatikusan lezáródnak,
- az Alapítvány informatikai rendszerét vírusvédelmi szoftver és hardveres tűzfal védi, továbbá
- a laptopokban lévő adathordozók titkosított formában tárolják az adatokat.

Az Alapítvány a Személyes Adatok biztonsága érdekében a következő adminisztratív biztonsági intézkedést teszi: az Alapítvány a Személyes Adatok Különleges Kategóriájába Tartozó Adatok biztonsága érdekében gyermekek kezelésének menetére és a kezelés dokumentálására vonatkozó

szabályzatot hozott létre, amelyet valamennyi kezelést végző munkatárssal megismertetett, valamint amely szabályzat alkalmazása tekintetében valamennyi munkatárs részére oktatást tartott.

4 Adatvédelmi Incidens

Amennyiben a Személyes Adatok biztonsága olyan sérülést szenved, 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, akkor Adatvédelmi Incidens következik be.

Adatvédelmi incidens következik be például a következő esetekben:

- Személyes Adatokat tartalmazó dokumentum véletlen megsemmisítése vagy elektronikus dokumentum véletlen törlése esetén;
- Személyes Adatokat tartalmazó dokumentum ellopása esetén;
- pendrive elvesztése esetén, ha azon Személyes Adatokat tartalmazó dokumentum volt;
- Személyes Adatokat tartalmazó e-mailnek nem a címzett részére történő megküldése esetén;
- mobiltelefon elvesztése esetén.

5 Tudomásszerzés Adatvédelmi Incidensről

Amennyiben az Alapítvány valamely munkatársának tudomására jut, hogy feltételezhetően adatvédelmi incidens következett be olyan Személyes Adatok tekintetében, amelyeket az Alapítvány kezel, akkor haladéktalanul tájékoztatja erről az Alapítvány adatvédelmi tisztviselőjét az adatvedelem@deveny.hu e-mail címre küldött e-mail útján, valamint az Alapítvány kuratóriumának elnökét személyesen vagy telefonon.

Az Alapítvány munkatársa a Személyes Adatokat érintő adatvédelmi incidens körülményeit nem vizsgálja, viszont a körülmények vizsgálatához szükséges valamennyi, rendelkezésére álló adatot átad az adatvédelmi tisztviselő, illetve a kuratóriumi elnök részére.

Az a tény, hogy az Alapítvány munkatársa a feltételezett Adatvédelmi Incidens bekövetkezését az adatvédelmi tisztviselő tudomására hozza nem alapozza meg az Alapítvány tudomásszerzését az Adatvédelmi Incidensről, mivel fennáll a lehetősége annak, hogy nem következett be Adatvédelmi Incidens vagy nem olyan Személyes Adatok tekintetében következett be Adatvédelmi Incidens, amely adatok tekintetében az Alapítvány Adatkezelőként jár el.

Az Alapítvány akkor bír tudomással arról, hogy Adatvédelmi Incidens következett be, ha a kivizsgálás alapján nagy valószínűséggel megállapítható, hogy Adatvédelmi Incidens következett be. Amennyiben a kivizsgálás alapján megállapítható, hogy az Alapítvány által kezelt Személyes Adatok tekintetében következett be Adatvédelmi Incidens, akkor az Alapítvány tudomásszerzésének időpontja az az időpont, amikor az Alapítvány munkatársa az Adatvédelmi Incidensről tudomást szerzett.

6 Adatvédelmi Incidensekkel kapcsolatos tények és körülmények feltárása

Az adatvédelmi tisztviselő a tudomására jutott, feltételezhető Adatvédelmi Incidensre vonatkozó tényeket – lehetőségeihez mérten – felderíti, így felveszi a kapcsolatot azzal a személlyel, aki az Adatvédelmi Incidensről a tudomására hozta, továbbá azonosítja az Adatvédelmi Incidenssel érintett Személyes Adatokat, valamint az Adatkezelési tevékenységeket az Alapítvány munkatársai közreműködésével.

Az adatvédelmi tisztviselő az Alapítvány kuratóriumának elnökét tájékoztatja az Adatvédelmi Incidens feltárásáról.

Amennyiben az adatvédelmi tisztviselő a rendelkezésére álló információk alapján nem tudja eldönteni, hogy az Adatvédelmi Incidens ténylegesen bekövetkezett-e, akkor az értesítéssel egyidejűleg személyes egyeztetésre időpontot egyeztet az Adatvédelmi Incidenssel érintett Személyes Adatokat kezelő munkatársakkal és Adatfeldolgozókkal és a személyes egyeztetést megszervezi a tájékoztatást követő 2 (két) munkanapon belül annak érdekében, hogy az Alapítvány a Nemzeti Adatvédelmi és Információszabadság Hatóság részére esetlegesen megteendő bejelentést határidőben meg tudja tenni.

7 Adatvédelmi incidens kivizsgálása

Az adatvédelmi tisztviselő vagy szükség esetén a fenti pont szerint értesített személyek a személyes egyeztetésen folytatják a vizsgálatát annak, hogy a Rendelet szerinti Adatvédelmi Incidens ténylegesen bekövetkezett-e. A kivizsgálást az adatvédelmi tisztviselő vezeti és dokumentálja.

Az Alapítvány a kivizsgálás során a következő lépéseket teszi meg:

- Adatvédelmi Incidenssel érintett dokumentumok, rendszerek, nyilvántartások azonosítása;
- Adatvédelmi Incidenssel érintett Személyes Adatok azonosítása;
- Adatvédelmi Incidenssel érintett adatokhoz hozzáférő személyek és Adatfeldolgozók azonosítása;
- információkérés az Adatvédelmi Incidenssel érintett Személyes Adatokat kezelő Adatfeldolgozóktól és személyektől az incidens körülményeinek pontosítása ügyében;
- az Adatvédelmi Incidens hatásainak azonosítása;
- az Adatvédelmi Incidens orvoslásához szükséges lépések azonosítása.

Amennyiben a kivizsgálásba bevont személyek megállapítása szerint az Adatvédelmi Incidens kivizsgálásához további személyek bevonása szükséges, illetve a kivizsgálás előreláthatólag rövid időn belül nem zárható le, akkor az adatvédelmi tisztviselő intézkedési tervet készít az Adatvédelmi Incidens kivizsgálására, amelyben az egyes feladatok elvégzéséért felelős személyeket, valamint a feladatok ellátásának határidejét feltünteti.

8 Adatvédelmi incidens dokumentálása

Az Alapítvány a kivizsgálás tekintetében elkészített dokumentációban a következőket tünteti fel:

- Adatvédelmi Incidensről történt tudomásszerzés körülményei;
- Adatvédelmi Incidens kivizsgálása során tett lépések;
- Adatvédelmi Incidens kivizsgálásának lezárását megalapozó tények, bizonyítékok;
- Adatvédelmi Incidens hatásai;
- Adatvédelmi Incidens kivizsgálása alapján tett megállapítás;
- Adatvédelmi Incidens orvoslására tett intézkedések;
- Adatvédelmi Incidens tekintetében szükséges jövőbeli intézkedések.

Amennyiben a kivizsgálásba bevont személyek arra a megállapításra jutnak, hogy Adatvédelmi Incidens nem következett be, akkor további vizsgálatot nem folytatnak, az adatvédelmi tisztviselő az incidens tekintetében készült dokumentációt lezárja.

Amennyiben a kivizsgálásba bevont személyek arra a megállapításra jutnak, hogy Adatvédelmi Incidens következett be, akkor az adatvédelmi tisztviselő az incidens tekintetében készült dokumentációt lezárja és az Adatvédelmi Incidens tekintetében szükséges további lépéseket megteszi.

9 Adatvédelmi incidens nyilvántartása

Az adatvédelmi tisztviselő vezeti az Alapítvány külön dokumentumba foglalt Adatvédelmi Incidens nyilvántartását. A nyilvántartásba felveszi azokat az adatvédelmi incidenseket, amelyek olyan Személyes Adatokat érintenek, amelyek tekintetében az Alapítvány adatkezelőként jár el.

10 Adatvédelmi incidens bejelentése

Az Alapítvány részéről a bejelentést az adatvédelmi tisztviselő teszi meg a Nemzeti Adatvédelmi és Információszabadság Hatóság bejelentésre rendszeresített <https://naih.hu/adatvedelmi-incidensbejelent--rendszer.html> domain alatt elérhető honlapján vagy papíralapon a Nemzeti Adatvédelmi és Információszabadság Hatóság honlapjáról letölthető nyomtatvány bejelentéskor hatályos verzióján indokolatlan késedelem nélkül, legkésőbb a tudomásszerzéstől számított 72 órával.

Ha az Alapítvány az Adatvédelmi Incidens, annak tudomására jutásától számított 72 órán belül nem jelenti be, akkor a későbbi bejelentéssel egyidejűleg igazolja a késedelem indokait.

11 Érintettek tájékoztatása az Adatvédelmi Incidensről

Az érintetteket az adatvédelmi tisztviselő tájékoztatja, szükség esetén, a Személyes Adataikat érintő Adatvédelmi Incidens bekövetkezéséről. Az Alapítvány az érintetteket elektronikus úton vagy postai úton értesíti a nyilvántartásaiban szereplő elérhetőségeken.

Az Alapítvány az Adatvédelmi Incidensre vonatkozó tájékoztatásban világosan és közérthetően nyújt tájékoztatást az alábbiakról:

- Adatvédelmi Incidens jellege;
- a tájékoztatást nyújtó egyéb kapcsolattartó neve és elérhetőségei;
- az Adatvédelmi Incidensből eredő, valószínűsíthető következmények;
- az Alapítvány által az Adatvédelmi Incidens orvoslására tett vagy tervezett intézkedések, beleértve adott esetben az Adatvédelmi Incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Hatályos: 2019. március 29. napjától

Fogalomtár

Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az Adatkezelő nevében Személyes Adatokat kezel;

Adatkezelés: a Személyes Adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

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;

Alapítvány: a Dévény Anna Alapítvány (székhely: 1051 Budapest, Október 6. u. 24; adószám: 1962679-2-41);

Egészségügyi Adat: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó Személyes Adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

Érintett: bármely információ alapján azonosított vagy azonosítható természetes személy;

Rendelet: az Európai Parlament és a Tanács (EU) 2016/679. rendelete a természetes személyeknek a Személyes Adatok kezelése tekintetében történő védelméről és az ilyen adtaok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről;

Szabályzat: a Dévény Anna Alapítvány adatbiztonsági és adatvédelmi incidens szabályzata;

Személyes Adat: azonosított vagy azonosítható természetes személyre vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

Személyes Adatok Különleges Kategóriájába Tartozó Adat: a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló Személyes Adat, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adat, az egészségügyi adat és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó Személyes Adatok.