BALATONI REGIONÁLIS TÖRTÉNETI KUTATÓINTÉZET,
KÖNYVTÁR ÉS KÁLMÁN IMRE EMLÉKHÁZ

ADATVÉDELMI INCIDENSKEZELÉSI SZABÁLYZAT

Hatályos: 2019. augusztus 1-től.

Tartalomjegyzék

Adatvédelmi incidens fogalma az EU vonatkozó, 2016/679 RENDELETE értelmében:

(1) „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.

(2) Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, 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, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

1. Adatvédelmi incidens kezelése, bejelentése

(1) Adatkezelő munkavállalója vagy szerződéses partnere (adatfeldolgozó) a tudomására jutott incidens kapcsán mérlegeli, hogy az incidens érinti-e az adatvédelmet.

(2) Amennyiben az incidens adatvédelmet érint, adatkezelő munkavállalója vagy szerződéses partnere (adatfeldolgozó) **az adatvédelmi incidens tényét haladéktalanul jelenti fenntartójának és adatvédelmi tisztviselőjének az adatvédelmi incidens bejelentő nyomtatványon (2. sz. melléklet).**

(3) Adatkezelő munkavállalói részére előírás, hogy az adatvédelmi incidens-bejelentés és -kezelés teljes folyamatát írásban dokumentálják a későbbi azonosíthatóság és bizonyíthatóság érdekében.

(4) A dokumentálás bizonyítékai (dokumentumok) az adatvédelmi tisztviselő jóváhagyását követően lerakásra kerülnek az intézmény vezetői titkárságán és megküldésre kerülnek a fenntartónak, valamint az adatvédelmi tisztviselőnek.

(5) Adatkezelő képviselője az adatvédelmi tisztviselővel együttműködésben megvizsgálja, hogy sérültek-e az érintettek személyes jogai, az adatok titkosítottak voltak-e, az adatok védettek voltak-e (anonimizálás, álnevesítés), magas kockázattal járnak-e a személyes jogok sérülékenysége terén. Amennyiben a fenti feltételek vizsgálata negatív

eredményt ad, úgy az adatvédelmi incidenst az adatkezelő az adatvédelmi tisztviselőn keresztül az illetékes felügyeleti hatóságnál jelenteni köteles.

(6) Következésképpen, amint az adatkezelő tudomására jut az adatvédelmi incidens, azt indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenteni köteles az illetékes felügyeleti hatóságnál, kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés 72 órán belül nem tehető meg, úgy meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

(7) Az említett 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 az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
c. ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d. 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.

(8) Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

(9) Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

2. Adatvédelmi incidenskezelési protokoll (folyamatleírás)

(1) NYILVÁNTARTÁS: Az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze a törvény követelményeinek való megfelelést. Mindezt a 2. sz. mellékletben kell megtenni és megküldeni a fenntartó és az adatvédelmi tisztviselő számára.

(2) ELLENŐRZÉS: Incidens bejelentésekor ellenőrizni kell, hogy megtörténtek-e a szükséges intézkedések, főképpen:

a. az incidens megállapítása
b. az incidens bejelentése az adatvédelmi tisztviselőn keresztül a Felügyeleti Hatóságnak
c. az érintett(ek) értesítése és tájékoztatása az adatvédelmi incidensnek a személyek jogaira és szabadságára irányuló kockázatáról, annak fokáról és segíteni kell a természetes személyt a sérelem hatásaink kivédését vagy mérséklését szolgáló javaslatokkal.

(3) KIVIZSGÁLÁS, ELEMZÉS ÉS ÉRTÉKELÉS: Az adatvédelmi incidens napvilágra kerülése után azonnal ki kell vizsgálni, majd elemezni kell az incidens kialakulásának körülményeit és fel kell mérni a belőle fakadó károkat, adatvédelmi sérelmeket és ezen sérelmek fokát. Ezt a műveletsort az intézmény vezetője és az intézmény adatvédelmi tisztviselője együtt végzik el.

(4) MÓDOSÍTÁS ÉS FEJLESZTÉS: Az elemzés és értékelés eredményeinek megfelelően ki kell alakítani a sérülékenység megszüntetését szolgáló intézkedési tervet és azt az intézkedésért felelős személy(ek) számára a lehető legrövidebb időn belül továbbítani szükséges.

Az adatvédelmi incidens-kezelési protokoll-folyamat ábráját jelen szabályzat *1. sz. melléklete* tartalmazza.

3. Érintettek tájékoztatása

(1) Az érintettet az adatkezelő indokolatlan késedelem nélkül tájékoztatja, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes

személyek jogaira és szabadságaira nézve, annak érdekében, hogy megtehesse a szükséges óvintézkedéseket. Az érintettek tájékoztatásáról az észszerűség keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a felügyeleti hatósággal, és betartva az általa vagy más érintett hatóságok például bűnüldöző hatóságok által adott útmutatást.

(2) A vonatkozó EU-rendelet értelmében az említett 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 az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
c. ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d. 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.

(3) A vonatkozó EU-Rendelet 34. cikk (3) bekezdés értelmében az érintettet nem kell az 1. bekezdésben említettek szerint tájékoztatni, ha a következő feltételek bármelyike teljesül:

a. 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;
b. 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 valósu
c. l meg;
d. a tájékoztatás aránytalan erőfeszítést tenne szükségessé vagy aránytalanul magas költséget igényelne. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

(4) 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, vagy megállapíthatja a (3) bekezdésben említett feltételek valamelyikének teljesülését.

A szabályzat 2019. augusztus 01. napján lépett hatályba.

Siófok, 2021. június 01.

Balatoni Regionális Történeti Kutatóintézet Könyvtár Siófok

.....

Igazgató