EÖTVÖS JÓZSEF FŐISKOLA

6500 Baja, Szegedi út 2.
Tel: +36 79 524 624
info@ejf.hu
www.ejf.hu

EÖTVÖS JÓZSEF FŐISKOLA BAJA

Adatvédelmi tisztviselő elérhetőségei

6500 Baja, Szegedi út 2.
adatvedelem@ejf.hu

SZC/1-13/2021

Eötvös József Főiskola

adatvédelmi incidenskezelési szabályzata[1]

Baja, 2021. április 20.

[1] Megállapította a Szenátus 17/2018.(05.23.) számú határozata, 2018.05.25. napi hatállyal. Utoljára módosította a Szenátus 24/2021.(04.20.) számú határozatával, 2021.04.21. napi hatállyal.

2.5. *„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;

2.6. *„harmadik személy":* az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, 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 felhatalmazást kaptak;

3. Az adatvédelmi incidens fogalma

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. [*GDPR 4. cikk 12.*]

4. Az incidens típusok besorolása következményük szerint

4.1. **Bizalmassági incidens:** személyes adatok véletlen vagy felhatalmazás nélküli közlése, vagy az ezekhez való hozzáférés; illetéktelen személyek számára válik hozzáférhetővé az adat.

Ennek oka lehet külső szándékos informatikai támadás, lehet szoftver vagy hardver meghibásodásból adódó nem kívánt hozzáférési lehetőség megnyílása, illetve jogosulatlan adattovábbítás véletlenül vagy szándékosan.

Papír dokumentumok esetében hasonlóan, bármi módon illetéktelen által történő megismerése a dokumentumban foglalt személyes adatoknak. Ez adódhat véletlen továbbításból, tévesen címzett küldeményből, elzárás elmulasztásából, szervezetlen tárolási körülményekből.

Fentieken kívül bármilyen esemény, magatartás, mely a személyes adatok illetéktelenek általi megismerését eredményezi, bizalmassági incidensnek minősül.

4.2. **Sértetlenséggel kapcsolatos incidens:** A személyes adatok véletlen vagy jogtalan megváltoztatása; az adatállomány ugyan megmaradt, de az eredeti tartalmához képest nem kívánt változás áll elő benne, amely az érintettre nézve kockázattal jár.

A tárolt adatbázis nem veszik el, hozzáférhető, de valamilyen technikai hardveres vagy szoftveres hiba vagy emberi mulasztás, esetleg szándékos emberi magatartás következtében nem kívánt változás áll be az adatokban, melyek így már nem a valóságot tükrözik.

Papír dokumentumok esetében az adathordozók olyan sérülése, külső behatás miatti elváltozása eredményezhet ilyen incidenst, melynek következtében az adatok kiolvasása más, vagy bizonytalan eredménnyel jár.

4.3. **Hozzáférhetőséggel kapcsolatos incidens:** A személyes adatok véletlen vagy jogtalan megsemmisítése vagy ezek „elvesztése".

Hozzáférhetőségi incidens az is, amikor a tárolt adatok nem semmisülnek meg, viszont valamilyen technikai vagy külső okból az Adatkezelő és/vagy az Adatfeldolgozó nem fér hozzá az adatbázishoz, nem tudja lekérni azokat, a kívánt és rendeltetésszerű adatkezelési műveleteket nem tudja végrehajtani.

Ide tartozik továbbá az elektronikus és a papír adathordozók, adatok bármi módon történő nem kívánt elveszítése, megsemmisülése, illetve törlése is.

5. Lehetséges incidensek a gyakorlatban (nem kimerítő jellegű felsorolások)

5.1. Bizalmassági incidens:

Informatikai: adatszivárgás, illetéktelen személy hozzáférése, az adatok nem kívánt nyilvánosságra kerülése; amit eredményezhet szoftverhiba, hardverhiba, szándékos emberi magatartás, tévedés vagy mulasztás; mobil informatikai eszközök elveszítése, jelszó kiszivárgása.

Veszélyeztetett egységek: Adatkezelő szervezeti egységeinél működő hardverrendszerek, mobil informatikai eszközök, valamint az ügyvitelhez használt szoftverek.

Dokumentumkezelés: irattárba adás elmulasztása, eltérő rendeltetésű iratok véletlen összefogásából adódó téves közlés, iratok felügyelet nélkül hagyása – különösen közös használatú helyiségekben –, iratok elveszítése.

Veszélyeztetett adathordozók: számviteli bizonylatok, szerződéses dokumentumok, személyügy iratanyag.

5.2. Sértetlenséggel kapcsolatos incidens:

Informatikai: Adatállományok megváltozása, egyes személyes adatok felcserélődése, konkrét érintett természetes személy személyes adatainak keveredése más érintett adataival, egyes személyes adatok megváltozása, módosulása következtében az érintett nem, vagy nem megfelelően azonosítható; amit eredményezhet szoftverhiba, hardverhiba, szándékos emberi magatartás, tévedés vagy mulasztás.

Veszélyeztetett egységek: Adatkezelő szervezeti egységeinél működő hardverrendszerek, mobil informatikai eszközök, valamint az ügyvitelhez használt szoftverek.

Dokumentumkezelés: iratok folyadék, napsugárzás miatti rongálódása, helytelen tárolás miatti károsodása.

Veszélyeztetett adathordozók: számviteli bizonylatok, szerződéses dokumentumok, személyügy iratanyag.

5.3. Hozzáférhetőséggel kapcsolatos incidens:

Informatikai: Adatvesztés, adatokhoz való hozzáférési képesség teljes vagy részleges elveszítése, adatok véletlen vagy szándékos törlése, adatállományok olyan sérülése, mely a hozzáférést és/vagy a megfelelő olvashatóságot gátolja; amit eredményezhet szoftverhiba, hardverhiba, szándékos emberi magatartás, tévedés vagy mulasztás, adathordozók, mobil informatikai eszközök elveszítése.

Veszélyeztetett egységek: Adatkezelő szervezeti egységeinél működő hardverrendszerek, mobil informatikai eszközök, valamint az ügyvitelhez használt szoftverek.

Dokumentumkezelés: iratok elveszítése, véletlen elzárása, téves továbbítása melynek eredményeként a visszakézbesítésig nem férhet hozzá Adatkezelő, iratok megsemmisülése.

Veszélyeztetett adathordozók: számviteli bizonylatok, szerződéses dokumentumok, személyügy iratanyag.

6. Kockázatértékelés

Az incidensek, illetve az incidens gyanúját keltő események vizsgálatakor, kezelésekor folyamatosan kockázatértékelést kell végezni minden, a vizsgálatban, kezelésben résztvevő személynek.

6.1. A kockázatértékelés szempontjai:

a) az incidens jellege az érintett adathordozók típusára tekintettel (papír dokumentumok, elektronikus tárolók, hordozható elektronikus eszközök, online adattovábbításra közvetlenül alkalmas eszközök, online „térben" megvalósuló incidens),

b) az incidenssel érintettek száma és kategóriái,

c) az incidenssel érintett adatok kategóriái és száma (pl. csak név, vagy közvetlen kapcsolatfelvételre alkalmas elérhetőségi adatok is érintettek, esetleg profil építésre alkalmas adatösszesség),

d) különleges adatok érintettsége (pl. egészségi állapotra vonatkozó adatok),

e) az érintettek vagyoni helyzetére utaló adatok érintettsége (pl. méltányossági kérelmek, számviteli bizonylatokon tárolt adatok),

f) az incidens lehetséges következményei milyen súlyosan érinti az érintettek jogait,

g) az incidenssel érintett adatok alapján mennyire könnyű az érintettet egyedileg azonosítani.

6.2. Lehetséges következmények az érintettekre nézve:

a) jó hírnév sérelme,

b) pénzügyi veszteség,

c) a személyes adataik feletti rendelkezés elvesztése vagy a jogaik korlátozása.

6.3. „Érzékeny adatok" - ezen személyes adatokat érintő incidensek vélhetően kockázatot jelentenek a természetes személyek jogaira, szabadságaira:

a) egészségügyi adatok,

b) az érintett pénzügyi helyzetére vonatkozó adatok.

II. INCIDENSKEZELÉS ÉS FELELŐSÖK

1. Észlelés és jelzés

1.1. Adatvédelmi incidens (a továbbiakban: incidens), vagy incidens gyanúját keltő esemény bekövetkezése esetén az ezt észlelő személy haladéktalanul köteles jelezni az eseményt a Kancellárnak a következő kommunikációs csatornákon:
- e-mailben,
- sürgős intézkedést igénylő esetben telefonon.

1.2. A jelzésben ismertetni kell legalább:

a) az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit (pl. hallgató, foglalkoztatott, partner képviselője, stb.) és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit (pl. név, lakcím, e-mail cím, jövedelemre vonatkozó adatok, stb.) és hozzávetőleges számát,

b) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket (pl. adatok nyilvánosságra kerülése, végleges elveszítése, érintett illetéktelen általi elérése, stb.).

Felelős: Észlelő személy (bármely foglalkoztatott).

1.3. Kancellár értesíti az Adatvédelmi Tisztviselőt a fentiekről, és bevonja az incidens kezelésébe.

2. Incidenskezelési folyamat elindítása

2.1. Kancellár az Adatvédelmi Tisztviselővel együtt:

a) Az I/6. pont szerinti kockázatértékelést folyamatosan végzi tevékenysége során.

b) Értékeli a hozzá érkezett jelzést, szükség esetén további információkat kér az észlelőtől.

c) Elsődleges feladata az azonnali intézkedések szükségességének felmérése, indokolt esetben intézkedés megtétele, kezdeményezése (soron kívüli biztonsági mentés készítése, bizonyos szoftver használatának tiltása, lekapcsolódás az internetről, stb.).

d) Megállapítja, hogy személyes adatot érintett-e az esemény, amennyiben igen, azonosítja a következményt, vagy a fennálló kockázatot (sérülés, elvesztés, hozzáférhetetlenség, illetéktelen hozzáférése, nyilvánosságra kerülés). Megállapítja továbbá, hogy mely szervezeti egységet érinti az esemény, és milyen adathordozókat érint (informatikai eszközök, hordozható eszközök, papír dokumentumok).

Felelős: Kancellár és Adatvédelmi Tisztviselő.

2.2. Adatvédelmi Tisztviselő:

a) Javaslatot tesz a Kancellár felé az incidenskezelő-csoport összehívására, annak összetételét és az összehívás időpontját megjelölve.

b) Amennyiben az érintettek érdekeinek védelme megkívánja, az Adatvédelmi Tisztviselő soron kívül kezdeményezhet intézkedéseket a következmények elhárítása érdekében, a Kancellár értesítésével.

Felelős: Adatvédelmi Tisztviselő, Kancellár.

3. Incidenskezelő csoport és feladatai

3.1. A csoport összetétele:

a) Kancellár,

b) az érintett szakterület vezetője vagy az általa delegált személy,

c) informatikai vonatkozású esemény esetén az informatikai szakember,

d) Adatvédelmi Tisztviselő,

e) speciális szakértelmet igénylő esemény esetén a megfelelő szakértelemmel bíró foglalkoztatott vagy külső szakértő.

3.2. Az incidenskezelő csoport az I/6. pont szerinti kockázatértékelést folyamatosan végzi tevékenysége során.

3.3. A csoport feladatai:

a) az incidenssel érintett személyek kategóriáinak és számának meghatározása;

b) az incidensben érintett személyes adatok kategóriáinak (pl. személyazonosító adatok, elérhetőségek, pénzügyi adatok, egészségügyi adatok) és számának meghatározása;

c) az incidensben érintett adatokkal kapcsolatban annak feltárása, hogy mennyire könnyű azok alapján az érintettet egyedileg azonosítani;

d) incidens okozta kockázatok besorolása (részletes feladatleírás a II/4. pontban);

e) következmények, lehetséges következmények azonosítása, intézkedés az elhárításukra, enyhítésükre, további következmények megelőzésére;

f) bejelentési kötelezettség mérlegelése, az ezzel kapcsolatos kötelezettségek megállapítása, majd eszerint – az incidens észlelésétől számított 72 órán belül – bejelentés az adatvédelmi hatóság felé, illetve az érintett értesítése (részletes feladatleírás a II/5. és II/6. pontokban);

g) incidens bevezetése az adatvédelmi incidensek nyilvántartásába (1. számú melléklet szerinti tartalommal);

h) az incidensért felelős személy kilétének megállapítása, ha ez megállapítható, illetve felelőssége jellegének feltárása (szándékosság, gondatlanság);

i) írásos összefoglaló készítése az incidensről és kezeléséről,

j) javaslat a további incidensek elkerülésére, benne az esetlegesen szükséges változtatások, új szabályok megjelölésével.

3.4. Az incidens kivizsgálása során figyelemmel kell lenni az esetlegesen korábban bekövetkezett adatvédelmi incidensek vizsgálati tapasztalataira.

Felelős: incidenskezelő csoport aktuális összetétel szerinti tagjai a Kancellár vezetésével, Adatvédelmi Tisztviselő.

4. Kockázatok besorolása és a lehetséges következmények azonosítása

4.1. A kockázatok besorolása az I/6. pont szerinti kockázatértékelés szempontjai alapján, valamint az incidens konkrét körülményeinek (pl. adatbiztonság csökkent szintje, szándékos magatartásra utaló adatok) figyelembevételével történik.

4.2. A kockázat-besorolás fokozatai:

a) alacsony kockázatú (vagy kockázattal nem járó) incidens: ha az érintett adatok nem teszik lehetővé az érintett azonosítását (pl. több személyre, személyek csoportjára utaló, az érintett egyedi azonosítására nem alkalmas adat kiszivárgása);

b) közepes kockázatú incidens: ha az érintett adatok könnyen lehetővé teszik az érintett azonosítását, de az eset körülményei (pl. vétlen incidens), vagy az adatok jellege miatt, észszerűen nem kell az érintettre nézve hátrányos következményekkel számolni (pl. név vagy szakmai tapasztalat, vagy olyan adatok érintettek az incidens által, amelyek rosszindulatú felhasználása nem életszerű);

c) magas kockázatú incidens: ha olyan adatok érintettek az incidensben, amelyek rosszindulatú felhasználásával észszerűen számolni lehet, (pl. egészségügyi adatok) vagy ha az érintett adat(ok) jellege miatt valószínűsíthető, hogy az incidens hátrányos következményekkel járhat az érintettre nézve.

Felelős: incidenskezelő csoport aktuális összetétel szerinti tagjai a Kancellár vezetésével, Adatvédelmi Tisztviselő.

5. Bejelentés

5.1. Az adatvédelmi incidenst az Adatkezelő a tudomásszerzést követően 72 órán belül köteles bejelenteni a felügyeleti hatóságnak, ha az valószínűsíthetően kockázattal jár az érintett magánszférájára nézve.

5.2. **A tudomásszerzés időpontja:** az az időpont, amikor az Adatkezelő az eseményt adatvédelmi incidensként azonosítja; tehát amikor az adatkezelő észszerű mértékű bizonyossággal rendelkezik arról, hogy olyan biztonsági esemény történt, amely személyes adatokkal kapcsolatos jogellenes műveletekhez vezethet, vagy vezetett.

Mindemellett az esemény kivizsgálását azonnal el kell kezdeni és 72 órán belül dönteni kell a bejelentésről.

Ha eddig az időpontig nem lehetett kellő bizonyosságot szerezni az incidensről, akkor a Kancellár és az Adatvédelmi Tisztviselő bevonásával állást kell foglalni az incidens vélelmezésének kérdésében. Vélelmezett incidens esetén meg kell kezdeni az incidens bejelentését és kezelését.

5.3. A bejelentést a https://naih.hu/adatvedelmi-incidensbejelento-rendszer linken elérhető online bejelentő rendszer használatával kell megtenni, az alábbi felügyeleti hatóságnak:

Nemzeti Adatvédelmi és Információszabadság Hatóság
Cím: 1055 Budapest, Falk Miksa utca 9-11.
Postacím: 1363 Budapest, Pf. 9.
Telefon: +36 1 391 1400
Fax: +36 1 391 1410
E-mail: ugyfelszolgalat@naih.hu
Webhely: http://www.naih.hu/

5.4. A bejelentésben ismertetni kell legalább:

a) 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 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,

e) valamint a felügyeleti hatóság által a bejelentéshez mindenkor megkívánt információkat.