SZÍNHÁZ- ÉS FILMMŰVÉSZETI EGYETEM

REKTORI-KANCELLÁRI KÖZÖS UTASÍTÁS

IKT.SZ.: SZFE/2371/2021

Színház- és Filmművészeti Egyetem
31/2021. (09.16.) számú rektori-kancellári közös utasítása
a Színház- és Filmművészeti Egyetem Incidenskezelési Szabályzatáról

Hatályos: 2021. szeptember 17. napjától

Tartalomjegyzék

1 A SZABALYZAT CELJA, HATALYA, ALAPELVEK

1.1 Bevezető rendelkezések

1. A Színház- és Filmművészeti Egyetem (a továbbiakban: Egyetem) jelen szabályzatban (a továbbiakban: Szabályzat) határozza meg a biztonságos működés alapelveit, továbbá a tevékenysége során felmerülő rendkívüli események, incidensek bejelentésének, kivizsgálásának és kezelésének rendjét.
2. A rendkívüli események kezelése kapcsán alapvető fontosságú a megelőzés. A megelőzés érdekében az Egyetemnek
   - rendelkeznie kell a biztonságos működéshez szükséges szabályzatokkal;
   - eleget kell tennie a biztonságos informatikai környezet működtetéséhez szükséges technológiai feltételeknek; továbbá
   - meg kell hoznia azokat a technikai és szervezési intézkedéseket, amelyek hozzájárulnak az Egyetem biztonságos működéséhez (például: zárt és tűzbiztos irattár, iratmegsemmisítő, szigorúan szabályozott hozzáférési jogosultságok, titkosított adattárolás, biztonsági másolat, naplózás stb.);
   - a munkatársait rendszeres adatvédelmi, információbiztonsági és biztonsági képzésben kell részesítenie, továbbá magas szinten kell tartania a biztonsági tudatosságot; valamint
   - a biztonsági intézkedéseket és azok hatásosságát folyamatosan vizsgálnia kell, s szükség szerint a változó körülményekhez kell igazítania.
3. A Szabályzat hatálya alá tartozó személyek kötelesek a tevékenységük során az adott tevékenységre vonatkozó szabályzatokban vagy szerződésekben foglalt rendelkezések mellett a jelen Szabályzat előírásai szerint eljárni. A Szabályzat előírásait minden munkafolyamat és az Egyetem területén végzett tevékenység során, annak teljes tartama alatt figyelembe kell venni.

1.2 A Szabályzat célja

4. A Szabályzat célja, hogy meghatározza az Egyetem tevékenysége során felmerülő rendkívüli esemény bejelentésének, kivizsgálásának és kezelésének szabályait.

1.3 A Szabályzat személyi hatálya

5. A Szabályzat személyi hatálya kiterjed az Egyetemmel foglalkoztatási jogviszonyban állókra (a továbbiakban: munkavállalók) és az Egyetemmel hallgatói jogviszonyban állókra (a továbbiakban: hallgatók).
6. A Szabályzat egyes előírásainak hatálya a rájuk vonatkozó mértékben mindazon természetes személyekre (a továbbiakban: külső személyek) is kiterjed, akik az Egyetemmel szerződéses kapcsolatba kerülnek vagy az Egyetem területén tartózkodnak, illetve az Egyetem honlapját használják. A külső személyekre vonatkozó szabályokat a szerződés létrejötte előtt, továbbá az Egyetem területére belépéskor, valamint a honlap használata során ismertetni kell.

1.4 A Szabályzat tárgyi hatálya

7. A Szabályzat tárgyi hatálya mindazon rendkívüli eseményekre kiterjed, amelyek az Egyetem tevékenysége keretében vagy a területén, továbbá a honlapjának üzemeltetése során merülnek fel.
8. A Szabályzat elsősorban a rendkívüli események bejelentésével, előzetes vizsgálatával és elhatárolásával kapcsolatos eljárási rendet tartalmazza, a részletes kivizsgálást a rendkívüli esemény **2.3 pont** szerinti megfelelő kategóriájával kapcsolatos más szabályzatok előírásai szerint kell elvégezni.

1.5 Alapfogalmak

9. Jelen Szabályzat alkalmazása során az alábbi fogalmakat kell alkalmazni:

a) *adat*: valaki vagy valami megismeréséhez, jellemzéséhez hozzásegítő, nyilvántartott tény, részlet, értelmezhető, de még nem értelemzett ismeret

b) *információ*: a kapott adat felruházása az adott helyzetben általunk tulajdonított jelentéssel, értelmezett ismeret

c) *adatvédelem*: a személyes adatok (magánszféra) jogi védelme, alkotmányos alapjog

d) *biztonság*: valakinek vagy valaminek veszélytől, kártól, jogtalan beavatkozástól, bántódástól való védett állapota, helyzete. A biztonság az Egyetem azon állapota, amelyben a folyamatos, zavartalan és teljes körű felsőoktatási és a kapcsolódó üzemeltetési, üzleti tevékenység folytatható, fenntartható, illetve a rendeltetésszerű működést veszélyeztető szándékos vagy gondatlan, jogellenes magatartások, valamint az ezekkel szemben állított védelmi erőforrások és intézkedések kiegyenlítik egymást

e) *adatbiztonság*: a személyes adatok jogosulatlan kezelése, így különösen jogosulatlan megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások, valamint eljárási szabályok összessége; az adatkezelés azon állapota, amelyben a személyes adatok sérülésének, illetéktelen felhasználásának, megsemmisülésének kockázati tényezőit – és ezáltal a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a minimálisra csökkentik

f) *információbiztonság*: bizalmasság, sértetlenség, rendelkezésre állás elvének érvényesülése (részterületei: személyi, fizikai, adminisztratív, elektronikus biztonság)

g) *alapkövetelmények:* rendelkezésre állás (elérhetőség a jogosultaknak), sértetlenség (sérthetetlenség, valódiság), az adatok jellegétől függő bizalmas kezelés, hitelesség, a teljes információs rendszer működőképessége

h) *informatikai biztonság*: ha az információs rendszer védelme az alapkövetelmények szempontjából zárt (minden fontos fenyegetést figyelembe vesz), teljes körű (a rendszer összes elemére kiterjed), folyamatos (az időben változó körülmények ellenére is megszakítás nélküli) és kockázatarányos (a feltehető kárérték és a kár valószínűségének szorzata nem haladja meg az előre rögzített küszöbértéket)

i) *rendkívüli esemény vagy incidens:* bármilyen tevékenység vagy gyanús jelenség, amely kívül esik a szokásos gyakorlaton és paramétereken, váratlan, nem kívánt, általában kellemetlen esemény vagy jelenség, az Egyetem tevékenységének ellátását lassító, akadályozó vagy megbénító gondatlan vagy jogellenes magatartások és a természeti csapások eseményeinek összessége

j) *általános biztonsági incidens:* olyan esemény vagy jelenség, amely vagy a természet erőinek hatására következik be (villámcsapás, vihar, belvíz, árvíz, szélsőséges időjárás stb.), vagy egyéb módon (pl. tűz, csőtörés, áramszünet, betörés, bombariadó stb.) környezeti vagy vagyoni kárt, illetve a működésben zavart okoz

k) *adatvédelmi incidens:* a(z adat)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, s ez az érintett jogaira és szabadságaira valószínűsíthetően kockázattal jár

l) *információbiztonsági incidens:* nem kívánt vagy nem várt egyedi, vagy sorozatos információbiztonsági esemény, amely nagy valószínűséggel veszélyezteti az üzleti tevékenységet és fenyegeti az informatikai rendszert

m) *kockázat:* fenyegetettségek bekövetkezési valószínűsége és a bekövetkezéskor keletkező károk függvénye

2 A RENDKÍVÜLI ESEMÉNYEK KEZELÉSE

2.1 A rendkívüli esemény észlelése és bejelentése

10. A rendkívüli esemény észlelése az az időpont, amikor a munkavállaló, a hallgató vagy a külső személy valamely szokásos tevékenységét technikai vagy más akadály, jelenség miatt nem tudja elvégezni.

11. Az Egyetem tevékenysége vagy a honlapja használata során észlelt rendkívüli eseményt az észlelés után haladéktalanul, a melléklet szerinti nyomtatvány kitöltésével, és a(z) incidens@szfe.hu e-mail címre megküldéssel, be kell jelenteni. Azt a rendkívüli eseményt, amelyről már az észlelés pillanatában megállapítható, hogy általános biztonsági incidens (pl. tűz, árvíz, betörés) az Egyetem belső működési rendje szerint kell kezelni, az elhárítást az észszerűen elvárható módon meg kell kezdeni. Amennyiben az általános biztonsági incidens következményeinek elhárítása során vagy azt követően felmerül, hogy a környezeti kár érinti a személyes adatok kezelését, értesíteni kell az adatvédelmi tisztviselőt. Amennyiben az általános biztonsági incidens olyan környezeti kárt okozott, amely az informatikai biztonsági intézkedések sérelmét jelenti, értesíteni kell az információbiztonsági felelőst.

12. Ha a rendkívüli eseményről az észlelés pillanatában megállapítható, hogy információs rendszereket érint, az Informatikai Biztonsági Szabályzat szerinti és észszerűen elvárható haladéktalan informatikai intézkedéseket meg kell tenni.

2.2 Incidensvizsgáló bizottság

13. A rendkívüli eseményről / incidensről szóló bejelentést az adatvédelmi tisztviselő és az információbiztonsági felelős fogadja.

14. A rendkívüli esemény előzetes kivizsgálásához incidensvizsgáló bizottságot kell létrehozni, melynek állandó tagjai az adatvédelmi tisztviselő és az információbiztonsági felelős, azonban a létszám további szakértőkkel bővíthető.

15. A rendkívüli esemény kategóriájának megállapításáig az incidensvizsgáló bizottság munkáját az információbiztonsági felelős koordinálja.

16. Az incidensvizsgáló bizottság összetétele a rendkívüli esemény jellegétől függően változhat. Az incidensvizsgáló bizottság összetétele a rendkívüli esemény előzetes, illetve a részletes kivizsgálása során felmerült tények ismeretében is változhat.

17. Az információbiztonsági felelős értesíti mindazon szakterületeket, amelyek a rendkívüli esemény előzetes kivizsgálásában érintettek lehetnek. A szakterületek megfelelő felkészültséggel és tapasztalattal rendelkező munkatársat delegálnak a bizottságba.

18. Az incidensvizsgáló bizottság koordinálásával kapcsolatos feladatokat a rendkívüli esemény kategóriába sorolását követően az a felelős személy látja el, akinek hatáskörét a rendkívüli esemény érinti. Az incidensvizsgáló bizottságot adatvédelmi incidens esetén az adatvédelmi tisztviselő koordinálja és képviseli az Egyetem szervezeti egységei felé. Az incidensvizsgáló bizottságot informatikai biztonsági incidens esetén az információbiztonsági felelős koordinálja és képviseli az Egyetem szervezeti egységei felé. Az incidensvizsgáló bizottságot általános biztonsági incidens esetén a kancellár által kijelölt munkatárs koordinálja és képviseli az Egyetem szervezeti egységei felé.

19. Amennyiben a rendkívüli esemény több szakterületet is érint, az Egyetem kancellárja dönt az incidensvizsgáló bizottságot koordináló személyről.

20. Az incidensvizsgáló bizottság tagjainak – szükség esetén – munkaidőn kívül is rendelkezésre kell állniuk.

21. Az incidensvizsgáló bizottság megalakulásáról az incidensvizsgáló bizottság koordinálását végző személy az előzetes kivizsgálás megkezdésével egyidejűleg értesíti a rektort és a kancellárt.

22. Az adatvédelmi tisztviselő és az információbiztonsági felelős munkaköri leírásában szerepeltetni kell az incidensvizsgáló bizottságban történő részvételüket, illetve a rendkívüli események előzetes és részletes kivizsgálással kapcsolatos teendőiket.

2.3 A rendkívüli esemény előzetes kivizsgálása, a rendkívüli események elhatárolása

23. Az incidensvizsgáló bizottság az előzetes kivizsgálás keretében megvizsgálja a rendkívüli eseményről szóló bejelentés adatait, s besorolja a rendkívüli eseményt.

24. A rendkívüli eseményről szóló adatok előzetes megvizsgálása során az alábbi szempontokat kell figyelembe venni:

    a) a rendkívüli esemény személyes adatot érint-e,
    b) a rendkívüli esemény az informatikai biztonsági előírások sérelmére utal-e,
    c) a rendkívüli esemény környezeti kárt, illetve a működés zavarát okozta-e?

25. A rendkívüli esemény – az előzőekben felsorolt szempontok alapján – lehet adatvédelmi incidens, informatikai biztonsági incidens és általános biztonsági incidens (vagy kettő, esetleg mindhárom egyidejűleg).

26. Az adatvédelmi incidens az adatvédelmi tisztviselő, az informatikai biztonsági incidens az információbiztonsági felelős, az általános biztonsági incidens az általános biztonsági feladatokat ellátó munkatárs (a továbbiakban: biztonsági felelős) hatáskörébe tartozik. Amennyiben egy incidens adatvédelmi és információbiztonsági incidens is, az incidens az adatvédelmi tisztviselő felelősségi körébe tartozik elsődlegesen.

27. A rendkívüli esemény érinthet egyszerre több szakterületet is. Az előző pont alapján kijelölt személynek gondoskodnia kell a szakterületek zökkenőmentes együttműködéséről, valamint az érintett szakterületek alapvető előírásainak érvényesítéséről a rendkívüli esemény előzetes vizsgálata során.

28. A rendkívüli események elhatárolásához az Adatvédelmi Szabályzat, az Informatikai Biztonsági Szabályzat, továbbá az általános biztonsági előírásokat figyelembe kell venni.

29. A rendkívüli események kategóriába sorolásával kapcsolatos problémák esetén a kancellár dönt.

30. A rendkívüli események előzetes kivizsgálását lehető leghamarabb, legfeljebb 2 naptári napon belül el kell végezni.

31. Az előzetes vizsgálat eredményeként el kell dönteni, s írásba kell foglalni, hogy a rendkívüli esemény melyik **2.2. pontban** írott kategóriába tartozik. Az előzetes vizsgálat eredményének rögzítésével egyidejűleg – szükség szerint – intézkedni kell a további, részletes vizsgálat megindításáról. Amennyiben az előzetes vizsgálatot követően nem indul további, részletes vizsgálat, annak tényét és okát az előzetes vizsgálat eredményét rögzítő dokumentumban fel kell tüntetni.

32. Amennyiben a rendkívüli esemény adatvédelmi incidens, a tudomásra jutás időpontja az az időpont, amikor az incidensvizsgáló bizottság írásba foglalta, hogy adatvédelmi incidens történt. Az adatvédelmi incidens részletes vizsgálatát az Adatvédelmi Szabályzatba írott eljárási rend szerint kell folytatni. Az adatvédelmi incidens részletes vizsgálata során szem előtt kell tartani az adatvédelmi felügyeleti hatóságnak történő bejelentés határidejét.

33. Amennyiben a rendkívüli esemény informatikai biztonsági incidens,

a) figyelembe kell venni a különböző informatikai biztonsági szabályozásokban a sérülékenységek elhárítására vonatkozó rendelkezéseket;

b) amennyiben az Egyetem rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt azzal az eszközzel azonnal el kell kezdeni;

c) ha az Egyetem nem rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt manuális módon kell azonnal elkezdeni;

d) amennyiben a sérülékenység elhárítása belső erőforrásból nem kivitelezhető, akkor külső szakértőket kell bevonni az elhárítás folyamatába.

34. Az informatikai biztonsági incidens részletes vizsgálatát az Informatikai Biztonsági Szabályzat szerint kell folytatni.

35. Amennyiben a rendkívüli esemény általános biztonsági incidens, a további, részletes vizsgálatot az Egyetem belső működési rendje szerint kell lefolytatni.

2.4 A rendkívüli eseménnyel kapcsolatos dokumentációs kötelezettség

36. Az incidensvizsgáló bizottság üléseiről emlékeztetőt, döntéseiről indoklást is tartalmazó jegyzőkönyvet, vizsgálatairól pedig intézkedési javaslatokat is tartalmazó jelentést kell készíteni.

37. Az incidensvizsgáló bizottság munkáját tartalmazó dokumentumok kezelésére az Egyetem mindenkori iratkezelési szabályai az irányadók.

38. Amennyiben az incidens vizsgálata során az Egyetem tevékenységével kapcsolatban olyan megállapításra kerül sor, amelynek nyilvánosságra hozatala vagy közismertsége a befolyásmentes működést veszélyezteti, az incidensvizsgáló bizottság korlátozhatja a munkájáról szóló dokumentumokba betekintők körét (ide nem értve a rektort és a kancellárt).

39. Az Egyetem az Adatvédelmi Szabályzat (AVSZ) szerinti nyilvántartást vezet a bekövetkezett adatvédelmi incidensekkel kapcsolatos tényekről és intézkedésekről.

40. Az Egyetem az Informatikai Biztonsági Szabályzatnak (IBSZ) megfelelő nyilvántartást vezet a bekövetkezett informatikai biztonsági incidensekkel kapcsolatos tényekről és intézkedésekről.

41. Az Egyetem a belső működési rendje szerinti nyilvántartásokat vezeti a bekövetkezett általános biztonsági incidensekkel kapcsolatos tényekről és intézkedésekről.

42. Az adatvédelmi incidensek vizsgálata során keletkezett, papíralapú és elektronikus, iktatott dokumentumokat az adatvédelmi tisztviselő az adatvédelmi incidens vizsgálatának lezárásától számított 10 évig őrzi meg, illetéktelenek számára hozzá nem férhető, zárt helyen.

43. Az informatikai biztonsági incidensek vizsgálata során keletkezett, papíralapú és elektronikus, iktatott dokumentumokat az információbiztonsági felelős az informatikai biztonsági incidens vizsgálatának lezárásától számított 10 évig őrzi meg, illetéktelenek számára hozzá nem férhető, zárt helyen.

44. Az általános biztonsági incidensek vizsgálata során keletkezett, papíralapú és elektronikus, iktatott dokumentumokat a kancellár által kijelölt szervezeti egység az általános biztonsági incidens vizsgálatának lezárásától számított 10 évig őrzi meg, illetéktelenek számára hozzá nem férhető, zárt helyen.

3 ZARO RENDELKEZESEK

45. Jelen Szabályzat annak aláírását követő napon lép hatályba.
46. Jelen Szabályzat hatálybalépésével minden hasonló tárgyú szabályzat hatályát veszti.
47. Jelen Szabályzatot a Kancellári Kabinet gondozza.
48. A Jelen Szabályzat megtalálható és elérhető a www.szfe.hu oldalon.

Budapest, 2021. szeptember 16.

Novák Emil
mb. általános rektorhelyettes

PH

dr. Szarka Gábor
kancellár

4 A SZABALYZATHOZ TARTOZO DOKUMENTUMOK JEGYZEKE

4.1 Incidensbejelentő űrlap

4.2 Incidens kivizsgálási jegyzőkönyv

SZÍNHÁZ- ÉS FILMMŰVÉSZETI EGYETEM

SZFE 1865

ŰRLAP A BIZTONSÁGI ESEMÉNYEK JELENTÉSÉHEZ

A biztonsági esemény megnevezése (érintett rendszer, érintett személyes adatok köre – és becsült száma amennyiben releváns):

A tapasztalás helye és idő pontja:

Az érintett személyek megnevezése:

Az esemény pontos leírása:

--- Ezt a részt csak papír alapú bejelentések során kell kitölteni ---

Az észlelő neve:

Dátum:_____év___hó___nap ....

Észlelő aláírása IBF vagy DPO aláírása

SZÍNHÁZ- ÉS FILMMŰVÉSZETI EGYETEM

SZFE 1865

MELLÉKLET A 2.SZÁMÚ
REKTORI-KANCELLÁRI KÖZÖS UTASÍTÁSHOZ

SZÍNHÁZ- ÉS FILMMŰVÉSZETI EGYETEM

JEGYZŐKÖNYV RENDKÍVÜLI ESEMÉNY (INCIDENS) KIVIZSGÁLÁSÁHOZ

I. RÉSZ: ELŐZETES KIVIZSGÁLÁS

Készült: év hó nap óra perc[1]

Helyszín[2]:

Jelen vannak[3]:

A rendkívüli esemény bejelentésének ideje:

év hónap nap óra perc

A rendkívüli esemény (bejelentés tartalmának) rövid leírása[4]:

A rendkívüli esemény személyes adatot érint-e?[5] ☐ igen ☐ nem

A rendkívüli eseménnyel érintett személyes adatok köre[6]:

☐ természetes személyazonosító adatok

☐ elérhetőségi adatok

☐ egészségi állapottal, szociális helyzettel kapcsolatos adatok

☐ pénzügyi adatok (pl. számlaszám, bankkártya szám stb.)

☐ egyéb[7]:

---

[1] Ha az előzetes kivizsgálás alapján adatvédelmi incidens történt, akkor ennek megállapításától (az előzetes kivizsgálás lezárásától) kell számítani az adatvédelmi hatósághoz történő bejelentés GDPR szerinti határidejét. Az előzetes kivizsgálást legfeljebb 48 órán belül célszerű lefolytatni. Azokat a kérdéseket, amelyek ezen idő alatt nem tisztázhatók, részletes kivizsgálás során lehet megválaszolni, kezelni.

[2] Itt azt a helyszínt kell feltüntetni, ahol a jegyzőkönyvet írják, melynek során célszerű az Egyetem és a szervezeti egység nevét és címét teljesen kiírni, valamint az irodahelyiség elhelyezkedését (emelet, ajtó) is megadni.

[3] Nevek, beosztások felsorolása; ha van az incidensvizsgáló bizottságnak elnöke, akkor ennek feltüntetése, valamint a jegyzőkönyvvezető megjelölése.

[4] A leírásban azt kell röviden megfogalmazni, amit a bejelentés tartalmaz; pl. ma 10 óra 23 perc óta nem elérhető a levelezőrendszer, vagy ma 9 óra 18 perckor nyitva volt az irattár ajtaja, a helyiség őrizetlen volt 2 órán keresztül, vagy Y hónap N napján 20 óra 17 perckor, XZ feladótól érkezett e-mail szerint zárolták a tanulmányi adatok adatbázisát, és csak K forint/euro/dollár fizetése ellenében teszik ismét elérhetővé stb.

[5] Tekintettel arra, hogy ez a rész az előzetes kivizsgálás adatait tartalmazza, az itt megadott „nem" válasz esetén is célszerű lehet folytatni a vizsgálatot, mert a részletes kivizsgálás során kiderülhet, hogy mégis sérült a személyes adatok biztonsága.

[6] Több is megjelölhető, illetve ha a bejelentés alapján a rendkívüli esemény nem érinti a személyes adatokat, akkor át kell húzni. (Megjegyzés: a részletes kivizsgálás során ezeket az adatköröket fel kell majd tüntetni, de nem itt, hanem a részletes kivizsgálásról szóló jegyzőkönyvben.)

[7] Az „egyéb" szó után célszerű pontosan megjelölni, hogy milyen típusú személyes adatok sérültek (pl. fényképek).

A rendkívüli eseménnyel érintett személyes adatok hozzávetőleges száma[8]: db

A rendkívüli eseménnyel érintett személyek köre[9]:

- ☐ hallgató
- ☐ törvényes képviselő
- ☐ munkavállaló
- ☐ szerződött partner
- ☐ egyéb[10]:

A rendkívüli eseménnyel érintett személyek hozzávetőleges száma[11]: fő

A rendkívüli esemény a személyes adat[12]:

- ☐ jogellenes vagy véletlen megváltoztatását
- ☐ jogellenes vagy véletlen elvesztését
- ☐ jogosulatlan közlését
- ☐ jogellenes vagy véletlen megsemmisítését eredményezte vagy
- ☐ jogosulatlan hozzáférést eredményezett.

A rendkívüli esemény következményei[13]:

II. RÉSZ: A RENDKÍVÜLI ESEMÉNY (INCIDENS) KATEGÓRIÁBA SOROLÁSA[14]

A rendkívüli esemény adatvédelmi incidens? ☐ igen ☐ nem

A rendkívüli esemény informatikai biztonsági incidens? ☐ igen ☐ nem

A rendkívüli esemény általános biztonsági incidens? ☐ igen ☐ nem

III. RÉSZ: RÉSZLETES KIVIZSGÁLÁS SZÜKSÉGESSÉGE:

A rendkívüli esemény részletes vizsgálata szükséges? ☐ igen ☐ nem

A rendkívüli esemény részletes vizsgálatának vagy elmaradásának oka[15]:

---

[8] Amennyiben a személyes adatok száma pontosan nem határozható meg, hozzávetőleges számot kell megállapítani. A részletes kivizsgálás során ez a szám módosulhat.

[9] Több is megjelölhető.

[10] Az „egyéb" szó után célszerű pontosan megjelölni, hogy milyen érintettekről van szó (pl. vendég).

[11] Amennyiben az érintettek száma pontosan nem határozható meg, hozzávetőleges számot kell megállapítani. A részletes kivizsgálás során ez a szám módosulhat.

[12] Több is megjelölhető. Azt, hogy jogellenes vagy véletlen cselekmény történt, be kell karikázni vagy a nem kívánt kifejezést ki kell húzni.

[13] Itt mind az adatkezelőnél, mind az érintettnél jelentkező következményeket javasolt összefoglalni.

[14] Ha a rendkívüli esemény egyidejűleg több kategóriába is besorolható, akkor minden olyan kategóriánál „igen"-t kell jelölni, amely kategóriába esik az incidens.

[15] E rovatban célszerű megjelölni azokat a körülményeket, amelyek a részletes kivizsgálást vagy annak mellőzését indokolják.

A rendkívüli eseményt bejelentő meghallgatása szükséges? ☐ igen ☐ nem

A rendkívüli eseményt bejelentő neve és elérhetősége[16]:

IV. RÉSZ: AZ ADATVÉDELMI FELÜGYELETI HATÓSÁGHOZ TÖRTÉNŐ BEJELENTÉSHEZ SZÜKSÉGES INFORMÁCIÓK[17]:

Az adatvédelmi incidenst az adatvédelmi felügyeleti hatóságnak be kell jelenteni?

☐ igen ☐ nem

Az adatvédelmi felügyeleti hatósághoz történő bejelentés határideje[18]:

év hónap nap óra perc

Az Egyetem alkalmazott-e olyan technikai és szervezési védelmi intézkedés(eke)t, amelyek eredményeként az adatvédelmi incidensben érintett személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára az adatok értelmezhetetlenek? ☐ igen ☐ nem

Az Egyetem által alkalmazott technikai és szervezési védelmi intézkedések felsorolása[19]:

Az adatvédelmi incidens valószínűsíthetően kockázattal jár az érintettek jogaira és szabadságaira nézve? ☐ igen[20] ☐ nem

Az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve? ☐ igen[21] ☐ nem

Az adatvédelmi incidens ☐ súlyos[22] ☐ enyhe[23]

Az adatvédelmi incidensből eredő, valószínűsíthető következmények:

---

[16] Csak abban az esetben kell kitölteni, ha a részletes kivizsgálása során a meghallgatása szükséges.

[17] Ezt a részt akkor is ki kell tölteni, ha részletes kivizsgálás is lesz, mert ha a részletes kivizsgálás hosszabb ideig tart, akkor az adatvédelmi felügyeleti hatóságnak történő bejelentéssel nem lehet várni annak a befejezéséig. Ebben a jegyzőkönyvben szerepelnek azok az információk, amelyeket az adatvédelmi felügyeleti hatóságnak be kell jelenteni. Ha lesz részletes kivizsgálás, és az információk változnak, a részletes kivizsgálás befejezése után az adatvédelmi hatóságnak történő bejelentés kiegészíthető, módosítható. (lásd még: Adatvédelmi Szabályzat)

[18] A kategóriába sorolást (ezen jegyzőkönyv lezárását) követő legfeljebb 72 óra.

[19] Csak akkor kell kitölteni, ha az előtte levő kérdésre „igen" volt a válasz. Példák: az elvesztett pendrive-on titkosítottan/álnevesítve tárolták a személyes adatokat; a jogosulatlan hozzáférés sikertelen volt, mert a kétkulcsos azonosítást nem tudta a támadó feltörni

[20] „Igen" válasz esetén az adatvédelmi incidenst be kell jelenteni a Nemzeti Adatvédelmi és Információszabadság Hatóságnak.

[21] „Igen" válasz esetén az adatvédelmi incidensről az érintetteket is tájékoztatni kell.

[22] Súlyos adatvédelmi incidens: olyan incidens (pl. adatvesztés, adatsérülés), mely valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve (pl.: a jogosulatlan hozzáféréssel érintett adatok esete; az olyan adatsérülés, adatvesztés, amelynél az adatok naplózott állományból nem állíthatók helyre).

[23] Enyhe adatvédelmi incidens: minden incidens, amely nem súlyos (pl. átmeneti szolgáltatásleállás, -kiesés az Egyetem munkavállalói által használt belső rendszerekben, amely nem jár adatsérüléssel vagy adatvesztéssel)

Az adatvédelmi incidens adatvédelmi felügyeleti hatóságnak történő bejelentés időpontja[24]:

év hónap nap óra perc[25]

Az adatvédelmi incidensről az érintetteket értesíteni kell?

☐ igen ☐ nem

Az adatvédelmi incidensről az érintettek értesítésének időpontja[26]:

év hónap nap

Az érintettek értesítésének módja[27]:

V. RÉSZ: A RENDKÍVÜLI ESEMÉNY KEZELÉSÉVEL KAPCSOLATOS INTÉZKEDÉSEK[28]:

A rendkívüli esemény elhárítására, kezelésére tett intézkedések és azok időpontja[29]:

A rendkívüli esemény ismétlődésének megelőzésére tett intézkedések és azok határideje[30]:

A rendkívüli esemény kezelésére, illetve az ismétlődés megelőzésére tett intézkedések ellenőrzése szükséges? ☐ igen ☐ nem

A rendkívüli esemény kezelésére, illetve az ismétlődés megelőzésére tett intézkedések ellenőrzésének tervezett időpontja:

év hónap nap

Egyéb, a rendkívüli esemény szempontjából fontos, de az előző rovatokba nem besorolható információ:

Előzetes kivizsgálás lezárva: év hónap nap óra perc[31]

---

[24] Fontos, hogy itt ne a 72 órás határidő, hanem a bejelentés tényleges megtörténtének időpontja szerepeljen.
[25] Az óra/perc az adatvédelmi felügyeleti hatóságnak történő elektronikus bejelentés esetén töltendő ki.
[26] Az értesítés kiküldése vagy közzététele tényleges megtörténtének időpontja szerepeljen itt.
[27] Az értesítés módja lehet egyedi levél, e-mail, honlapon vagy nyomtatott sajtóban közzététel stb.
[28] Ezt a részt akkor is ki kell tölteni, ha lesz részletes kivizsgálás.
[29] Ebben a részben a bejelentéssel egyidejűleg megtett, haladéktalan intézkedéseket kell feltüntetni (pl. áramtalanítás, felelős személy értesítése, irattár ajtajának bezárása és őrzése stb.)
[30] Ha az előzetes kivizsgálás során ilyen intézkedés nem történik, áthúzható vagy a részletes kivizsgálásra lehet hivatkozni.

aláírások[32]

Záradék:[33]

Készült: … példányban/… lap
Kapják:
1. sz. példány:
2. sz. példány:
Kezelési utasítások:

---

[31] Ettől az időponttól számít az adatvédelmi felügyeleti hatóságnak történő incidensbejelentés határideje. Javasolt a kezdő időponttól számított legfeljebb 48 óra után befejezni az előzetes kivizsgálást, és ha még maradtak nyitott kérdések, akkor azokat részletes kivizsgálás során tisztázni.

[32] A teljes incidensvizsgáló bizottság is aláírhatja, de ha van a bizottságnak vezetője, akkor az ő és a jegyzőkönyvvezető aláírása is elegendő lehet.

[33] A záradékban leírható, hogy hány példányban és hány lapon készült a jegyzőkönyv, az egyes példányokat kik kapják, továbbá felsorolhatók a jegyzőkönyvhöz csatolt dokumentumok, illetve e helyen lehet rögzíteni azt a tényt, hogy a vizsgálatban szereplő megállapítások miatt a dokumentum egésze vagy annak egy része zártan kezelendő. Ha ilyen kezelési rendelkezés megfogalmazására sor kerül, azt el kell látni dátummal és az intézményvezető aláírásával. A zárt kezelés oka csak olyan információ lehet, amelynek szélesebb körű vagy nyilvános ismerete az Egyetem befolyásmentes működését megzavarhatja (pl. pontos adatbiztonsági beállítások, biztonsági mentések tárolási helye, titkosítási módszerek leírása stb.).