LXIX/2020. ÉVFOLYAM 6. SZÁM

Akadémiai Értesítő

A Magyar Tudományos Akadémia Hivatalos Lapja

Kiadja:
A MAGYAR TUDOMÁNYOS AKADÉMIA
TITKÁRSÁGA

Budapest, 2020. június 26.

A Magyar Tudományos Akadémia Elnöksége 2020. május 26-i ülésén hozott határozatai

Az Elnökség határozatait elektronikus úton hozta meg.

35/2020 (V. 26.) számú elnökségi határozat

Az Elnökség megismerte és tudomásul vette az MTA elnökének a COVID-19 veszélyhelyzet kapcsán végzett akadémiai szakmai feladatokról szóló tájékoztatását.

36/2020 (V. 26.) számú elnökségi határozat

Az Elnökség megismerte és tudomásul vette a Magyar Tudományos Akadémia elnökének tájékoztatását a Magyar Tudományos Akadémia elhalasztott májusi 193. közgyűlésének online platformon való megrendezése tárgyában kiírt közvélemény-kutatás eredményéről.

37/2020 (V. 26.) számú elnökségi határozat

Az Elnökség támogatja, hogy a közgyűlési tárgysorozat az alábbi napirendi ponttal bővüljön: Az Akadémia döntéshozó testületeinek elektronikus szavazási módja.
Az Elnökség javasolja, hogy a Közgyűlés a szavazásban részt vevők több mint 2/3-ának elfogadó szavazatát írja elő ezen napirendi pont szerinti határozathoz.

38/2020 (V. 26.) számú elnökségi határozat

Az Elnökség támogatja, hogy írásbeli vitát és véleménynyilvánítást követően a Közgyűlés tagjai az Akadémia e-választási rendszerén keresztül hozzanak döntést 2020. június hónap során a megküldött, 193., rendes közgyűlésre tervezett tárgysorozat 4–14., 17. és 18. pontok, valamint a Magyar Tudományos Akadémia köztestület döntéshozó szerveinek elektronikus eszköz útján való tanácskozásának és döntéshozatalának szabályairól.

39/2020 (V. 26.) számú elnökségi határozat

Az Elnökség támogatja, hogy a halasztott 193., rendes közgyűlés 2020. június 30-ra legyen összehívva, mely online formában vitatja meg a tervezett tárgysorozat 1. (Elnöki beszámoló), 15. (Kiváló Kutatóhely cím adományázásának alapelvei) és 16. (Az MTA főhivatású *választott vezetőire vonatkozó összeférhetetlenség szabályozása) pontját, valamint támogatja a tisztújítás lefolytatását* június–július hónapok során – a jogi és járványhelyzet függvényében – személyes vagy online formában.

40/2020 (V. 26.) számú elnökségi határozat

Az Elnökség megismerte és tudomásul vette a Doktori Tanács elnökének a doktori eljárásokhoz kapcsolódóan a járványhelyzet idején tartandó elektronikus ülésezésről és védésről szóló tájékoztatóját.

41/2020 (V. 26.) számú elnökségi határozat

Az Elnökség megtárgyalta az MTA 2019. évi Kormánytájékoztatójának koncepciója és annotált tartalomjegyzéke című dokumentumot, és a 102/2020. (IV. 10.) Korm. rendelet 5. § (1) bekezdésben kapott felhatalmazás alapján dönt az előterjesztés 3. számú melléklete szerinti tartalom elfogadásáról azzal, hogy a dokumentum megtárgyalását a veszélyhelyzet megszűnését követően 90 napon belül összehívandó közgyűlés napirendjére kell tűzni.

42/2020. (V. 26.) számú elnökségi határozat

1. Az Elnökség egyetért azzal a javaslattal, hogy a tudományos bizottságok megújítására az MTA legfőbb vezetőinek és közgyűlési bizottságainak, valamint a tudományos osztályok elnökeinek megválasztását követően kerüljön sor, az előterjesztés mellékletében foglalt ütemezés szerint. Az Elnökség a jelenleg működő bizottságok mandátumát a megújításig meghosszabbítja.
2. Az Elnökség felkéri a tudományos osztályok elnökeit, hogy tájékoztassák a tudományterületükhöz tartozó köztestületi tagokat a tudományos bizottságok választott tagjai megválasztásának rendjéről.

43/2020. (V. 26.) számú elnökségi határozat

Az Elnökség megismerte az MTA Kiváló Kutatóhely címadományozási rendszert kidolgozó Elnöki Bizottság elnökének szóbeli tájékoztatását a bizottsági munkáról. Az Elnökség felkéri a Bizottság elnökét, hogy az Elnökség vitájában felvetettek figyelembevételével előkészített anyagot terjessze a Közgyűlés elé.

A Magyar Tudományos Akadémia elnökének 12/2020. (V. 28.) számú határozata

A Magyar Tudományos Akadémia és az MTA Titkársága adatvédelmi incidens kezelési szabályzata, valamint az informatikai hibák elhárításának rendje

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 15. § (1) a) bekezdésben meghatározottak, valamint az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 számú a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló általános adatvédelmi rendelet 33. és 34. cikkben megfogalmazottak teljesítésére, a Magyar Tudományos Akadémiáról szóló 1994. évi XL. törvény 14. §-ában, és a Magyar Tudományos Akadémia Elnökségének 32/2009. (VI. 23.) számú állásfoglalásában biztosított jogkörömben eljárva, a Magyar Tudományos Akadémia Alapszabályával összhangban, a Magyar Tudományos Akadémia és az MTA Titkársága **adatvédelmi incidens kezelésére, valamint az informatikai hibák elhárításának rendjére vonatkozó szabályzatát** jelen határozatban foglaltak szerint határozom meg.

I. Bevezető rendelkezések

1. §
A szabályzat célja

Jelen határozat célja a Magyar Tudományos Akadémia (a továbbiakban: Akadémia), a Magyar Tudományos Akadémia Titkársága (a továbbiakban: Titkárság) vonatkozásában a személyes adatok védelméhez fűződő jogok érvényesülésének biztosítása, a Szervezet által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása, valamint az adatvédelmet sértő cselekmények kezelési folyamatának rögzítése, a felelősségi körök meghatározása és a szükséges eljárási rend kialakítása.

2. §
Szabályzat hatálya

(1) Szervi hatály
Jelen szabályzat hatálya az Akadémiára és a Titkárság költségvetési szervre terjed ki.

(2) Személyi hatály
Jelen szabályzat hatálya a Titkársággal közszolgálati vagy munkajogviszonyban, illetve munkavégzésre irányuló egyéb jogviszonyban álló munkatársakra (a továbbiakban együtt: munkatársak) terjed ki.

(3) Tárgyi hatály
Jelen szabályzat hatálya kiterjed a Titkárság által kezelt adatokat tároló, vagy feldolgozó teljes számítástechnikai infrastruktúrára, valamint a papír alapon kezelt adatállományra:
a) a számítástechnikai berendezésre és eszközre (számítógépek, nyomtatók, hálózati eszközök stb.),
b) a szoftverekre (rendszerprogramok, alkalmazások, adatbázisok, stb.),
c) az adatokat és a programokat tartalmazó adattárolókra és adathordozókra (hálózati adattárolók, CD-k, DVD-k, Blu-Ray diskek stb.),
d) az informatikai folyamatokban használt összes dokumentációra,
e) információs rendszer fizikai környezetére (épületek, számítógéptermek, irodák, kábelezés stb.)
f) továbbá a papír alapon kezelt adatokkal kapcsolatos adatvédelmi incidensek eljárásrendjére.

3. §
Értelmező rendelkezések

a) Személyes adat: Azonosított vagy azonosítható természetes személyre („érintett”) 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.
b) Informatikai rendszer: Meghatározott feladatok elvégzésére szolgáló számítástechnikai eszközcsoport (hardver és szoftver), valamint a hozzá tartozó használati mód (leírások, szabályzatok, jogosultsági rendszer).
c) Adatvédelmet sértő esemény: A mindennapi munkavégzéshez használt informatikai rendszerek működésében, vagy a személyes adatokat érintő adatkezelési folyamatok végzése során a munkatársak tapasztalhatnak olyan eseményt, amely veszélyezteti, illetve veszélyeztetheti a személyes adatok bizalmasságának, sértetlenségének és rendelkezésre állásának fenntartását.
d) Informatikai hiba: Az informatikai rendszer működésében tapasztalható, a munkát akadályozó, a megszokottól eltérő működés, szolgáltatásmegszakadás, -lassulás, mely nem minősül adatvédelmi incidensnek.
e) Adatvédelmi incidens: Az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
f) Hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság.
g) Adatgazda: Annak a szervezeti egységnek a vezetője, ahová jogszabály vagy szervezeti és működési szabályzat (SZMSZ) az adat kezelését rendeli, illetve ahol az adat keletkezik.
h) Szakrendszerfelelős: meghatározott feladat ellátáshoz kapcsolódó szakrendszer működtetésének folyamatosságáért az SZMSZ vagy eseti vezetői döntés alapján felelős személy.

i) Szakrendszergazda: A szervezeti egységek felhasználó oldali alkalmazásüzemeltetésével (pl. jogosultság kezelés) és az adott szakrendszer logikai, funkcionális működésének meghatározásával megbízott munkatárs. Az alkalmazásgazda a rendszergazdával szorosan együttműködik.
j) Adatkezelő: az Akadémia és a Titkárság (jogi személy) amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajttatja.
k) Adatvédelmi tisztviselő (Data Protection Officer, továbbiakban: DPO): Az adatkezelő és az adatfeldolgozó által kijelölt természetes vagy jogi személy, akinek feladata a személyes adatok kezelésére vonatkozó jogi előírások, valamint az érintettek jogai érvényesülésének elősegítése, valamint adatvédelmi jogszabályban meghatározott kötelezettségeinek teljesítése.
l) OTRS rendszer: (Open Technology – Real Service), a Titkárság által üzemeltetett incidens-, hiba- és igénybejelentő rendszer. A program kezeli a felhasználók részéről beérkező incidenseket, kérdéseket, panaszokat, ajánlásokat, hibajelentéseket amelyekhez egyedi jegyet rendel. A jegyek kezelésének folyamata transzparens, naplózott formában követhető. Elérhetősége: https://otrs.titkarsag.mta.hu/

II. Adatvédelmet sértő esemény, valamint informatikai hiba észlelése során követendő eljárás menete

4. §
Fogalmi meghatározások

(1) Adatvédelmet sértő események lehetnek különösen, de nem kizárólagosan:
a) személyes adatokat tartalmazó nyomtatott vagy elektronikus iratok, dokumentumok elvesztése,
b) személyes adatokat tartalmazó nyomtatott vagy elektronikus iratok, dokumentumok nem jogosult személy általi fellelése,
c) szervezeti érintettségű személyes adatok illetéktelen nyilvánosságra kerülése, publikus forrásokban való nem jogosult személy általi fellelése (pl. facebook),
d) személyes adatokat tartalmazó e-mailek hibás címzetteknek történő továbbítása vagy tudomásszerzés ilyen továbbításról,
e) harmadik fél által a személyes adatokat tároló informatikai rendszerhez vagy adatkezelő szoftverhez történő jogosulatlan hozzáférés,
f) a személyes adatok jogosulatlan titkosítása, amelynek következtében a személyes adatokhoz – akár átmenetileg – nem lehet hozzáférni vagy az Adatkezelő adatkezelései során felhasználni,
g) ha az Adatkezelő munkavállalója jogosulatlanul hozzáfér személyes adatokhoz, vagy a jogosultsági szintjét meghaladóan fér hozzá a személyes adatokhoz, vagy a munkavállaló által jogosulatlanul végrehajtott adatkezelési művelet (például a személyes adatokat tartalmazó adatbázis kimentése külső adathordozóra),
h) személyes adatok vétlen vagy szándékos, felhatalmazás nélküli nyilvánosságra hozatala,
i) személyes adatokat tartalmazó dokumentum más számára történő hozzáférhetővé tétele,
j) személyes adatokat tartalmazó postai küldemény téves címzetthez történő elpostázása,
k) személyes adatokat vagy egyéb védendő bizalmas adatokat tartalmazó adathordozó, rendszer dokumentáció vagy informatikai eszköz, illetve programok elvesztése vagy ellopása, személyes adatokat tartalmazó adatkörök kiszivárgása.

(2) Informatikai események, melyek adatvédelmi incidenst eredményezhetnek különösen de nem kizárólagosan:
a) a személyes adatokat tároló informatikai eszköz, vagy az ilyen adatokat tartalmazó dokumentumok sérülése, megsemmisülése (ideértve a tűzesetet, vagy a vízkár által okozott sérülést, vagy megsemmisülést), amelynek következtében a személyes adatokhoz – akár átmenetileg – nem lehet hozzáférni, vagy az Adatkezelő adatkezelései során felhasználni,
b) a folyamatosság jelentős megszakadása, pl. tűz, árvíz, áramkimaradás, számítógépes vandalizmus következtében,
c) tényleges vagy megkísérelt számítógépes betörés, megtévesztés vagy visszaélés,
d) vírusfertőzések, különösen ha azok több rendszert érintenek,
e) a hardver- és szoftverkonfiguráció illetéktelen megváltoztatása,
f) a jogosulatlan hardver- és szoftvertelepítés és -használat,
g) a hardvereszköz jogosulatlan megbontása,
h) a Szervezet informatikai rendszerének jogosulatlan használata, a hozzáférési rendszer kijátszása,
i) a saját jogosultsággal való visszaélés,
j) más személy felhasználói azonosítójának használata,
k) a telepített szoftver biztonsági beállításainak engedély nélküli, önkényes megváltoztatása,
l) az adatok jogosulatlan törlése, módosítása,
m) károkozó számítógépes program létrehozása, telepítése, tárolása, terjesztése, futtatása,
n) adatátviteli csatorna engedély nélküli lehallgatása,
o) jogosulatlan erőforrás-használat, erőforrások túlterhelése,
p) a hálózati eszközök működésének engedély nélküli befolyásolása, módosítása,
q) az informatikai biztonsági kontrollok kijátszása, a hálózati határvédelmi rendszer megkerülése,
r) az informatikai biztonság veszélyeztetésére alkalmas felhívást, közlést hordozó üzenetek terjesztése,
s) személyes adatokat tartalmazó adatkörök megsemmisülése.

5. §
Adatvédelmi esemény bejelentésének szervezeten belüli lehetőségei, azok dokumentálása

(1) A 4.§ (1) és (2) bekezdésében jelzett eseményről tudomást szerző vagy észlelő munkatárs kötelessége ennek haladéktalan – észlelést követő 1 órán belüli – bejelentése a 5. § (4) bekezdésében rögzített lehetőségek valamelyikén.

(2) Tudomásszerzésnek minősül az, ha
a) az adatvédelmi incidens bekövetkezésére utaló körülményt az Adatkezelő munkavállalója fedezi fel,
b) az Adatkezelő e-mailen, postai levélben vagy más kommunikációs eszköz útján üzenetet, levelet kapott, amely adatvédelmi incidens bekövetkezésére utaló körülményt tartalmaz (abban az esetben is, ha az üzenet vagy a levél névtelen),
c) az Adatkezelőt telefonon keresztül adatvédelmi incidens bekövetkezésére utaló körülményről értesítik (abban az esetben is, ha a hívó fél ismeretlen vagy névtelen),
d) a sajtóban vagy más honlapokon megjelent, adatvédelmi incidens bekövetkezésére utaló körülményről értesül az Adatkezelő, vagy arról értesítik,
e) az Adatkezelő által megbízott adatfeldolgozó e-mailben vagy telefonon jelzi, hogy az Adatkezelő által kezelt személyes adatokkal összefüggésben adatvédelmi incidens következett be.

(3) A 4. § (1), illetve (2) bekezdésben jelzett esemény során, ha a probléma informatikai jellegű, a probléma elhárításáig a felhasználónak tilos a hibásnak feltételezett szoftvert, adatot a számítógépről eltávolítania mindaddig, amíg erre a Titkárság Informatikai Főosztályától (a továbbiakban: IFO) felhatalmazást nem kapott. A helyreállítást csak kellően képzett és gyakorlott munkatársak hajthatják végre. A probléma észlelésekor a felhasználó köteles a számítógépet azonnal kikapcsolni, ha szükséges, a rendszer áramtalanításával. A rendszer bekapcsolására csak az IFO-tól kapott felhatalmazást követően kerülhet sor.

(4) **Az adatvédelmi incidensek bejelentésének** nyilvántartása és kezelése az OTRS rendszerben történik. Bejelentő a bejelentését az alábbiakban részletezettek szerint több módon megteheti:
a) Webes (Intranet) felületen, ahol a Bejelentő maga rögzíti az észlelt problémát az OTRS rendszerben. *Jegyek / Új jegy* menüpont és a *„Címzett”* mezőben az „**Adatvédelmi incidens**” értéket kiválasztva.
b) E-mail-ben: a Bejelentő e-mailt ír az **incidens@titkarsag.mta.hu** e-mail címre, az erre a címre érkező e-mailek, automatikusan **Adatvédelmi incidensként** kerülnek rögzítésre az OTRS rendszerben.
c) Telefonon az IFO munkatársának a 061-411-6224 számon. Az IFO-munkatárs a telefonos bejelentés alapján közvetlenül rögzíti az eseményt az OTRS rendszerben. Amennyiben az IFO-munkatárs nem tudja fogadni a hívást, a hívás hangpostára vált, ahol rögzítésre kerül hangüzenet formájában a bejelentés. A hangüzenetek automatikusan bejelentést generálnak az OTRS rendszerben. Az eset adatvédelmi incidens jellegét az üzenetben egyértelműen jelezni kell!
d) A Bejelentő a közvetlen vezetője felé személyesen és írásban is megteheti a bejelentést, aki azt továbbítja az előzőekben felsorolt valamelyik csatornára.

(5) Az **informatikai hiba bejelentések** nyilvántartása és kezelése az OTRS rendszerben történik. Bejelentő a bejelentését az alábbiakban részletezettek szerint több módon megteheti:
a) Webes (Intranet) felületen, ahol a Bejelentő maga rögzíti az észlelt problémát az OTRS rendszerben a *Jegyek / Új jegy* menüpont alatt, a *„Címzett”* mezőben a hibára leginkább jellemző kategóriát kiválasztva.
b) E-mailben: informatikai hiba esetén a Bejelentő e-mailt ír a **support@titkarsag.mta.hu** e-mail-címre, az erre a címre érkező e-mail-ek automatikusan rögzítésre kerülnek OTRS rendszerben.
c) Telefonon: a 061-411-6224 telefonszámon, az IFO munkatárs a telefonos bejelentés alapján közvetlenül rögzíti az eseményt az OTRS rendszerben. Amennyiben az IFO-munkatárs nem tudja fogadni a hívást, a hívás hangpostára vált, ahol hangüzenet formájában kerül rögzítésre a bejelentés. A hangüzenetek automatikusan bejelentést generálnak az OTRS rendszerben.

(6) A bejelentés során meg kell adni legalább:
a) bejelentés dátumát, idejét,
b) bejelentés minősítését: informatikai hiba, adatvédelmi incidens, egyéb igény/bejelentés,
c) bejelentő nevét, munkaterületét,
d) incidens vagy informatikai hiba pontos helyét (fizikai és logikai értelemben is),
e) incidens vagy informatikai hiba minél részletesebb leírását,
f) érintett adatokat, eszközöket, folyamatokat és az ezekben keletkezett kár meghatározását,
g) az esetlegesen érintett társszakfőosztályok meghatározását,
h) bejelentő által az incidensre vagy informatikai hibára tett első reakció leírását.

6. §
Adatvédelmi incidens bejelentésének szervezeti vizsgálata

(1) A bejelentés adatvédelmi átvizsgálása
a) Amennyiben a bejelentést **adatvédelmi incidens**ként jelöli meg a bejelentő, úgy az IFO haladéktalanul – OTRS jegy keletkezésétől számítottan munkaidőben 1 órán belül – megküldi az érintett szervezeti egység vezetője számára az incidensről szóló jelzést, és egyidejűleg tájékoztatást küld a DPO és a Jogi és Igazgatási Főosztály (továbbiakban: JIF) felé is a lehetséges adatvédelmi incidensről.
b) Amennyiben a bejelentést **nem adatvédelmi incidens**ként jelöli meg a bejelentő, de adatvédelmi incidens gyanúja áll fenn, úgy az IFO haladéktalanul – OTRS jegy keletkezésétől számítottan munkaidőben 1 órán belül – megküldi az érintett szervezeti egység vezetője számára az incidensről szóló jelzést,

és egyidejűleg tájékoztatást küld a DPO és a JIF felé is a lehetséges adatvédelmi incidensről.

c) A DPO feladata – az Adatgazdával történt konzultáció után – annak megítélése, hogy történt-e adatvédelmi incidens, valamint az incidens kategorizálása. Erre vonatkozó megállapításairól tájékoztatja az Adatgazdát, az IFO-t és a JIF-et. Amennyiben egy eseményről a tudomásszerzés időpontjában nem lehet eldönteni, hogy adatvédelmi incidensnek tekinthető-e, akkor haladéktalanul előzetes vizsgálatot kezdeményez a DPO annak tisztázása érdekében, hogy az esemény megfeleltethető-e az Adatvédelmi Incidens fogalomnak. Az előzetes vizsgálat célja, hogy meg lehessen állapítani a következőket:
   – az adott esemény személyes adatokkal összefüggésben következett-e be,
   – ki lehet-e zárni annak lehetőségét, hogy az adott esemény személyes adatokat érintett.

d) Amennyiben az esemény személyes adatokkal összefüggésben következett be, vagy nem lehet kizárni annak lehetőségét, hogy az adott esemény személyes adatokat érintett, akkor az esemény Adatvédelmi Incidensnek minősül.

e) Amennyiben a kivizsgálás függetlensége vagy hatékonysága a Titkárságon belül nem biztosítható, akkor az adatvédelmi incidens kivizsgálásával külső szakértőt lehet megbízni.

f) Amennyiben a bejelentés adatvédelmi incidens és adatvédelmi megoldási folyamatokat igényel, úgy a DPO intézkedik – az IFO és JIF egyeztetést követően – a szükséges teendők elvégzéséről.

7. §
Adatvédelmi incidens hatósághoz történő bejelentése

(1) Az adatvédelmi incidenst a DPO tudomásszerzését követően haladéktalanul, legkésőbb az incidenst követő 72 órán belül bejelenti az illetékes felügyeleti hatóságnak (NAIH), kivéve, ha az adatvédelmi esemény a DPO szakmai véleménye szerint valószínűsíthetően nem jár kockázattal a természetes személyek személyes adataihoz fűződő jogaira és szabadságaira nézve.

(2) A bejelentési kötelezettséget a DPO – a minősített adatot tartalmazó bejelentés kivételével – a Hatóság által e célra biztosított elektronikus felületen, a NAIH által szabott adattartalommal teljesíti.

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

8. §
Az érintett tájékoztatása

(1) 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.

(2) Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell legalább:

a) az adatvédelmi incidens jellegét, beleértve az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

b) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

c) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

d) 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) Az érintettet nem kell az (1) pontban említettek szerint tájékoztatni, ha a következő feltételek bármelyike teljesül:

a) az adatkezelő az adatvédelmi incidenssel érintett adatok tekintetében az adatvédelmi incidenst megelőzően megfelelő – így különösen az adatokat a jogosulatlan személy általi hozzáférés esetére értelmezhetetlenné alakító, azok titkosítását eredményező – műszaki és szervezési védelmi intézkedéseket tett;

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 valósul meg;

c) 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 hatékony tájékoztatását;

d) törvény a tájékoztatást kizárja.

9. §
Informatikai hibára vonatkozó bejelentés vizsgálata

(1) <u>Bejelentés informatikai átvizsgálása</u>

a) Amennyiben a bejelentés kategóriája nem adatvédelmi incidens, úgy annak érdemi átvizsgálását az IFO végzi el. Az IFO-nak meg kell vizsgálnia azt is, hogy a bejelentés érinthet-e személyes adatot. Amennyiben érinthet személyes adatot, úgy a 6. § (1) a) pontja szerint kell eljárni.

b) Amennyiben a bejelentés nem érint személyes adatot, az IFO a bejelentés jellege szerint aktiválja az IT megoldási folyamatokat.

c) Amennyiben az átvizsgálás alapján egyértelműen megállapítható, hogy az adott esemény nem érintett személyes adatokat, akkor az eseményt nem kell adatvédelmi incidensként kezelni. Ebben az esetben is az előzetes vizsgálatban feltérképezi az IFO, hogy
   – mi volt az adott esemény oka, illetve
   – amennyiben az adott esemény kapcsán értelmezhető, hogyan lehet megelőzni azt, hogy a jövőben ne következzen be hasonló esemény.

(2) <u>IT megoldási folyamatok</u>

a) Biztonsági esemény bekövetkezésekor egy személy vagy szervezet elleni esetleges jogi fellépéshez kellő számú bizonyítékkal kell rendelkezni, ezért fontos a megoldási folyamatok során, hogy az IFO az

informatikai rendszerben üzemeltetői szerepkörben elérhető bizonyítékokat gyűjtse, és megőrizze az informatikai rendszerekben is. Ha a valamely esemény jogszabálysértést valósíthat meg, akkor haladéktalanul a JIF véleményét kell kérni.

b) Számítógép adathordozón rögzített bizonyíték esetében a hordozható adathordozók, valamint a háttértárolón és a központi tárolón talált információ másolatait a vizsgálat befejezéséig meg kell őrizni, és rendelkezésre állásáról gondoskodni kell.

c) Az IT megoldási folyamat egyes lépéseiről a Bejelentő felhasználó folyamatos tájékoztatást kap.

10. §
Bejelentés közös átvizsgálása

(1) Amennyiben a bejelentés kategóriája **adatvédelmi incidens**, és van IT relevanciája, a bejelentést az IFO vezető, a DPO, a JIF és az Adatgazda közösen vizsgálják át az észlelést követően a lehető legrövidebb időn belül, munkaidőben egy órán belül, és döntést hoznak a szükséges intézkedések tekintetében az alábbiak szerint.

(2) Az IFO Vezető meghatározza az informatikai érintettséget, és aktiválja a szükséges IT megoldási folyamatokat.

(3) A DPO átvizsgálja a bejelentést, és amennyiben szükséges, rendelkezik

a) az Adatvédelmi incidenssel kapcsolatos bejelentési (NAIH) folyamat elindításáról,

b) az Adatvédelmi incidenssel kapcsolatos tájékoztatási (Érintettek tájékoztatása) folyamat elindításáról,

c) az Adatvédelmi incidens megoldására, illetve megismétlődésének megakadályozására irányuló egyéb, adatvédelmi megoldási folyamatok aktiválásáról.

(4) Az Adatgazda átvizsgálja az érintett szakrendszer belső működését és a szervezeti egység munkafolyamatát és szükség szerint intézkedik a további adatvédelmi incidensek elkerülése érdekében.

11. §
Bejelentés lezárása

(1) A bejelentés lezárásra kerül, amennyiben a bejelentés:

a) nem adatvédelmi incidens és nincs is IT relevanciája,

b) IT relevanciával bír, és a szükséges IT megoldási folyamatokat lefolytatták,

c) Adatvédelmi incidensnek minősül, és a szükséges bejelentési és/vagy tájékoztatás elvégzésére vonatkozó és/vagy Adatvédelmi megoldási folyamatokat lefolytatták.

(2) A lezárás során az OTRS rendszer értesítést küld a Bejelentő számára, melyben tájékoztatja:

a) a lezárás tényéről

b) az elvégzett tevékenységekről

c) a munkavégzés időráfordításáról.

12. §
Adatvédelmi incidens nyilvántartása

(1) Az adatvédelmi incidens lezárását követően az incidenssel érintett szervezeti egység vezetője köteles a 1. számú mellékletben csatolt adatvédelmi incidens nyilvántartó űrlapot az IFO és a DPO közreműködésével kitölteni és megküldeni a JIF számára.

III. Az adatvédelmet sértő események megelőzésével és kezelésével kapcsolatos feladatok

13. §
Tanulás az eseményekből

(1) Amennyiben az adatvédelmi incidens IT rendszert érint, az IFO Vezető feladata az üzemeltetésért felelős rendszergazdák közreműködésével elemezni az eseményt, és a biztonsági események kezelése során nyert tapasztalatok felhasználásával a meglévő biztonsági rendszer – így a szabályozó elemek és technikai megoldások – felülvizsgálata és azok szükség esetén való tökéletesítése.

(2) Amennyiben az adatvédelmi incidens kezelése során adatvédelmi megoldás és/vagy bejelentés és/vagy tájékoztatás elvégzésére vonatkozó folyamatok aktiválása történt, akkor a DPO és az Adatgazda feladata elemezni az eseményt, és a nyert tapasztalatok alapján felülvizsgálni és fejleszteni az adatkezelést érintő szakrendszereket, folyamatokat.

14. §
Feladatok és felelősségek meghatározása

(1) A személyes adatok védelmét sértő események megelőzésére és kezelésére vonatkozó eljárásrend ellenőrzése, továbbá az adatvédelmi időszakos oktatás a DPO feladata.

(2) A felhasználók informatikai biztonsága tudatosságának növelése érdekében az időszakos oktatás az IFO feladata.

(3) A szabályzat szerinti szükséges intézkedések meghozatala a szervezeti struktúrában meghatározott szervezeti egységek vezetői hatáskörének, felelősségének és beszámoltathatóságának szabályozottságán keresztül valósul meg.

(4) Ennek érdekében a vezetők alapvető kötelezettsége, hogy

a) a szabályok betartását minden vezető folyamatosan kísérje figyelemmel, amely elsődleges feltétele az adatvédelmet sértő események megelőzésének,

b) adatvédelmet sértő esemény észlelése esetén minél gyorsabban kellően hatékony intézkedés történjen annak érdekében, hogy az adatvédelmet sértő esemény megszüntetésre kerüljön;

c) a helytelen alkalmazási gyakorlat megszüntetése mellett indokolt esetben a személyi felelősség megállapításra kerüljön, a szükséges intézkedések megvalósuljanak.

(5) Minden szervezeti egység vezetője felelős a feladatkörébe tartozó szakterületen észlelt, adatvédelmet sértő esemény ismételt előfordulásának megelőzéséhez szükséges intézkedések megtételéért, a bekövetkezett esemény feltárásáért, szükség esetén annak dokumentálásáért, továbbá a hiányosságok megszüntetésével kapcsolatos intézkedések kezdeményezéséért, és megvalósításuk ellenőrzéséért.

(6) A foglalkoztatottak konkrét feladatát, hatáskörét, felelősségét a munkaköri leírások tartalmazzák.

(7) Valamennyi dolgozó feladata és kötelessége az észlelt adatvédelmet sértő esemény jelzése a vezető felé a szolgálati út betartásával, és megszüntetésük érdekében javaslatok tétele, valamint az elrendelt intézkedések megvalósítása.

IV. Záró rendelkezések

(1) A jelen szabályzatban nem szabályozott kérdésekben a vonatkozó hatályos jogszabályok, és az akadémiai intézmények belső szabályzatai az irányadók, így különösen:
   a) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény;
   b) 2016. április 27-i (EU) 2016/679 számú a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló általános adatvédelmi rendelet;
   c) a Magyar Tudományos Akadémia Titkársága Informatikai Biztonsági Szabályzata;
   d) a Magyar Tudományos Akadémia és az MTA Titkársága adatvédelmi szabályzata.

(2) Az Akadémia és a Titkárság megbízott Adatvédelmi tisztviselőjének (DPO) feladata és felelőssége, hogy hatáskörében eljárva jelen szabályzatot évente, valamint minden olyan jogszabályi, szervezeti és technológiai változtatás után, amely az abban foglaltak végrehajtását lényegesen befolyásolja, felülvizsgálja, és a szükséges változások átvezetésére javaslatot tegyen.

(3) Jelen határozat 2020. június 1-én lép hatályba.

(4) A határozatot a Titkárság Intranetén a Dokumentumtár» Határozatok tára » Elnöki határozatok megnevezésű oldalon kell kihirdetni, valamint az Akadémiai Értesítőben közzé kell tenni.

Budapest, 2020. május 28.

Lovász László

1. sz. melléklet

Adatvédelmi incidens nyilvántartás

Incidens megnevezése és dátuma: .....

1. Az adatvédelmi incidens bekövetkezése előtt alkalmazott intézkedések: .....

2. Az adatvédelmi incidens jellege: .....

3. Az adatvédelmi incidens oka: .....

4. Az adatvédelmi incidenssel érintett személyes adatok típusa és mennyisége (legalább becsléssel): .....

.....

.....

Személyes adatok típusa: .....

Személyes adatok mennyisége: .....

5. Az érintettek száma: .....

6. Az érintettek kategóriái: .....

7. Az adatvédelmi incidens lehetséges vagy már megtörtént következményei, illetve azok súlyossága az érintettekre nézve:

.....

8. Amennyiben az Adatkezelő mellőzte az adatvédelmi incidens bejelentést, akkor ennek oka: .....

9. Amennyiben nem volt szükséges az érintettek tájékoztatása, akkor ennek oka: .....

10. Amennyiben szükséges lett volna, de az Adatkezelő mellőzte az érintettek tájékoztatását, akkor ennek oka: .....

11. Az adatvédelmi incidens orvoslására és az okainak megszüntetésére tett intézkedések: .....

Dátum:

……

önálló szervezeti egység megnevezése, vezetőjének aláírása

TÁJÉKOZTATÓ

a Magyar Tudományos Akadémia doktora cím odaítéléséről

SZABÓ MÁRTON

„Diszkurzív politikatudomány. Bevezetés a politika interpretatív szemléletébe és kutatásába” című munkája alapján

elnyerte a Magyar Tudományos Akadémia doktora címet a Magyar Tudományos Akadémia Doktori Tanácsa 2020. május 15-i ülésén hozott döntése szerint.

FOGADÓÓRA

Török Ádám, a Magyar Tudományos Akadémia főtitkára – figyelemmel a koronavírus-járvány okozta korlátozásokra – írásban fogadja a megkereséseket a fotitkar@titkarsag.mta.hu e-mail címen.

AKADÉMIAI ÉRTESÍTŐ, a Magyar Tudományos Akadémia hivatalos lapja
A szerkesztésért felelős: az MTA Titkárság Jogi és Igazgatási Főosztálya
1051 Budapest, Nádor u. 7.

A kiadásért felelős az Akadémiai Kiadó Zrt. igazgatója.
Budapest, 2020
Szerkesztő: Tóth Anikó – Termékmenedzser: Egri Róbert
Megjelent: 1,5 (A/5) ív terjedelemben – HU ISSN 0865-9303

Előfizetésben terjeszti a Magyar Posta Zrt. Hírlap Üzletág (Budapest VIII., Orczy tér 1.; postacím: 1008 Budapest).
Előfizethető valamennyi postán, kézbesítőknél, e-mailen (hirlapelofizetes@posta.hu)
és faxon (303-3440). További információ: 06 80/444-444.
Előfizetési díj egy évre 10 320 Ft áfával. – Példányszámonkénti ára: 860 Ft áfával.

Printed in EU