

Iktatószám: PIM/61-44/2020

**A Petőfi Irodalmi Múzeum főigazgatójának
22/2020. számú utasítása
a Petőfi Irodalmi Múzeum Adatvédelmi Szabályzata (GDPR szabályzat) kiadásáról**

1. A Petőfi Irodalmi Múzeum Adatvédelmi Szabályzatát (GDPR szabályzat) a jelen utasítás mellékletében foglaltak szerint határozom meg.
2. Jelen utasítás és melléklete 2021. január 1-jén lép hatályba.

Budapest, 2020. december 23.



Demeter Szilárd
főigazgató



**A PETŐFI IRODALMI MÚZEUM
ADATVÉDELMI SZABÁLYZATA
(GDPR SZABÁLYZAT)**

2020. december 22.

Tartalom

I. FEJEZET	3
ÁLTALÁNOS RENDELKEZÉSEK	3
1. A szabályzat célja	3
2. A szabályzat hatálya.....	3
3. Vonatkozó jogszabályok	3
4. Értelmező rendelkezések.....	4
II. FEJEZET	4
RÉSZLETES RENDELKEZÉSEK	4
I. A SZEMÉLYES ADATOK KEZELÉSÉRE VONATKOZÓ ELVEK	4
II. A SZEMÉLYES ADATOK VÉDELMÉVEL KAPCSOLATOS ELJÁRÁS	5
1. A személyes adatok védelme.....	5
2. Múzeumon belüli adatátadás.....	6
3. Adattovábbítás harmadik személy részére.....	6
3. Az Múzeum, mint adatfeldolgozó	7
4. Az adatvédelmi tisztviselő.....	7
5. Adatkezelési tevékenységek nyilvántartása.....	8
6. Az adatok védelme.....	8
7. Adatvédelmi incidensek	8
8. Adatvédelmi hatásvizsgálat	9
9. Az adatvédelmi incidens.....	10
a) Az adatvédelmi incidens észlelése és kezelése	10
10. Az adatfeldolgozás	11
11. Adatbiztonsági előírások.....	12
III. AZ ÉRINTETT JOGAI ÉS AZ ÉRINTETT JOGAINAK ÉRVÉNYESÍTÉSÉVEL ÖSSZEFÜGGŐ FELADATOK	12
III. FEJEZET	13
ZÁRÓ RENDELKEZÉSEK	13
IV. FEJEZET	13
IV. MELLÉKLETEK	13
1. számú melléklet: Bejelentő lap az adatvédelmi tisztviselő részére adatvédelmi incidens esetén... 14	
2. számú melléklet: Az érintett tájékoztatása az adatvédelmi incidensről	18

A Petőfi Irodalmi Múzeum (a továbbiakban: Múzeum) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.), valamint az EURÓPAI PARLAMENT ÉS ATANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (a továbbiakban: GDPR) alapján a személyes adatok védelmét, illetve közérdekű adatokkal kapcsolatos feladatok ellátásnak rendjét a következők szerint állapítja meg:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. A szabályzat célja

A szabályzat célja, hogy a Petőfi Irodalmi Múzeum (a továbbiakban: Múzeum) tevékenysége során a személyes adatok védelméhez fűződő jog érvényesülésének biztosítása, illetve a Múzeum által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági előírásokat a Múzeumban.

2. A szabályzat hatálya

- (1) A szabályzat szervei hatálya kiterjed a Múzeum minden olyan szervezeti egységére, amely tevékenysége során személyes adatot kezel.
- (2) A szabályzat személyi hatálya kiterjed a Múzeum valamennyi munkavállalójára, és a Múzeum feladatainak végrehajtásában polgári jogi jogviszonyban közreműködő azon személyekre, akik tevékenységük során ilyen adatot kezelnek.
- (3) A szabályzat tárgyi hatálya a személyes adatokkal kapcsolatos adatkezelésre terjed ki, beleértve az adattovábbítást is.
- (4) A szabályzat hatálya nem terjed ki az informatikai eszközökkel összefüggő technikai adatvédelemre, amelyről az Informatikai Biztonsági Szabályzat (IBSZ) rendelkezik.

3. Vonatkozó jogszabályok

- (1) Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.),
- (2) Az EURÓPAI PARLAMENT ÉS ATANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (a továbbiakban: GDPR),
- (3) A GDPR 29-es cikk szerint létrehozott Adatvédelmi Munkacsoport iránymutatásai,
- (4) A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlásai.

4. Értelmező rendelkezések

A szabályzat alkalmazásában

- a) **adatkezelő szerv:** a Múzeum;
- b) **adatbirtokos:** a Múzeum adatkör szerint érintett szervezeti egységének azon vezetője, aki önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja;
- c) **személyes adat:** a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: általános adatvédelmi rendelet) szerinti személyes adat;
- d) **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;
- e) **adatfeldolgozó:** az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége;
- f) **adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
- g) **üzleti titok:** az üzleti titok védelméről szóló 2018. évi LIV. törvényben meghatározott üzleti titok;
- h) **nyilvánosságra hozatal:** az adat bárki számára történő hozzáférhetővé tétele;
- i) **érintett:** bármely információ alapján azonosított vagy azonosítható természetes személy;
- j) **hozzájárulás:** az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozik vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez;
- k) **címzett:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz;

A szabályzatban szereplő fogalmakat a GDPR 4. cikkében és az Info tv. 3. §-ában meghatározott tartalommal kell értelmezni és alkalmazni.

II. FEJEZET RÉSZLETES RENDELKEZÉSEK

I. A SZEMÉLYES ADATOK KEZELÉSÉRE VONATKOZÓ ELVEK

A Múzeum a személyes adatok kezelése során az alábbi elveket alkalmazza:

a) **Jogszerűség, tisztességes eljárás és átláthatóság elve**

A személyes adatok kezelésére csak és kizárólag a megfelelő jogalap megléte esetén kerülhet sor. Az adatkezelésre vonatkozó jogszabályok betartásán túl, a Múzeum tiszteletben tartja az érintettek

személyes adataikhoz fűződő jogát és az emberi méltóságát az adatkezelés során. A Múzeum az adatkezelést átláthatóan végzi, az adatkezelésről hatékony és teljes körű tájékoztatást nyújt az érintettek részére.

b) Célhoz kötöttség elve

A Múzeum kizárólag előre meghatározott, jogszerű célból kezel adatokat, a céllal, célokkal összeegyeztethető módon.

c) Adattakarékosság elve

A Múzeum kizárólag annyi és olyan személyes adatot kezel, mely a meghatározott cél teljesüléséhez szükséges. A Múzeum az adatkezeléskor meghatározott cél megvalósulását követően – kivéve, ha jogszabály ezzel ellentétesen rendelkezik, vagy az adattárolás olyan adatkezelési cél elérése érdekében lehetséges, mely összeegyeztethető az eredeti adatkezelési céllal – a személyes adatokat törli.

d) Pontosság elve

A Múzeum az általa kezelt személyes adatok pontosságát az adatbirtokos folyamatos felülvizsgálata és az érintett helyesbítéshez való joga gyakorlásának biztosításával garantálja.

e) Korlátozott tárolhatóság elve

A Múzeum a személyes adatot tartalmazó dokumentumot az adatkezelési cél elérését vagy az adatkezelési idő leteltét követően – kivéve, ha jogszabály ezzel ellentétesen rendelkezik, vagy az adattárolás olyan adatkezelési cél elérése érdekében lehetséges, mely összeegyeztethető az eredeti adatkezelési céllal – törli vagy anonimizálja, amely révén az érintett a továbbiakban nem azonosítható.

f) Integritás és bizalmas jelleg elve

A Múzeum biztosítja a jogosultak számára, hogy az adatokhoz hozzáférjenek, továbbá gondoskodik a személyes adatok védelméről.

g) Elszámoltathatóság elve

A Múzeum valamennyi személyes adat kezelésével összefüggő tevékenységét visszakövethető módon dokumentálja, és ezáltal biztosítja az adatkezeléssel kapcsolatosan megtett intézkedések átláthatóságát.

II. A SZEMÉLYES ADATOK VÉDELMEVEL KAPCSOLATOS ELJÁRÁS

1. A személyes adatok védelme

(1) Amennyiben olyan adatot kell megszerezni, melyet közokirat tartalmaz, az eredeti okiratot vagy annak közjegyző által hitelesített másolatát be kell mutatni.

(2) Az adatot megszerző szervezeti egység legkésőbb a személyes adatok megszerzésének időpontjában –ha lehetséges még azt megelőzően -az érintettet köteles tájékoztatnia GDPR 13. illetve 14. cikkében és az Info tv.-ben meghatározott adatkezelés részleteiről.

(3) Hozzájáruláson alapuló adatkezelés esetén az adatot megszerző szervezeti egység köteles beszerezni az érintett hozzájárulását a GDPR 7. cikkének figyelembevételével.

2. Múzeumon belüli adatátadás

Az adatkezelőszervezeti egység személyes adatot – a szükséges mértékben és ideig – csak olyan adatkezelésre jogosult szervezeti egységhez továbbíthat, amelynek feladata ellátásához a személyes adatok megismerése és kezelése szükséges és az adatkezelésre megfelelő joggal rendelkezik. Amennyiben a két szervezeti egység között a személyes adat átadásával kapcsolatos bármely kérdésben véleményeltérés van, úgy – az adatvédelmi tisztviselő szakmai tanácsának figyelembevételével – közös felettesük dönt.

3. Adattovábbítás harmadik személy részére

(1) A Múzeum szervezeti egysége az adattovábbítás feltételeinek meglétét minden egyes személyes adattal összefüggésben köteles ellenőrizni, így különösen azt, hogy az igényelt adatokra vonatkozóan az adatok kezelőjének minősül-e.

(2) Adatvédelmi szempontból akkor tekinthető az adattovábbítás jogszerűnek, ha a személyes adatot kezelő szerv vagy személy jogosult annak továbbítására, az adattovábbítás címzettje (adatkérő) pedig rendelkezik az adat kezeléséhez szükséges joggal vagy az érintett írásos – a vonatkozó jogszabályi elvárásoknak megfelelő tartalmú – hozzájárulásával és az adatkérés célja mindezzel összhangban van. Az adattovábbítás feltételeinek megléte és a célhoz kötöttség a jogszerűség együttes követelménye.

(3) Harmadik személy vagy szerv által benyújtott adattovábbítási kérelem elbírálása – törvényben kötelezően előírt adattovábbítás esetét kivéve – a Múzeum főigazgatójának vagy az általa kijelölt vezetőnek a hatáskörébe tartozik, amellyel kapcsolatban kikérheti az adatvédelmi tisztviselő véleményét. Az adatigénylés abban az esetben teljesíthető, ha az tartalmazza:

- a) az adatigénylés célját, jogalapját;
- b) a kért adatok körének pontos meghatározását;
- c) az érintett személy azonosításához szükséges adatokat, több személyre vonatkozó adatigénylés esetén az érintettek azonosításához szükséges csoportképző ismérveket.

(4) Az adattovábbítás történhet kérelem alapján egyedi adatszolgáltatással, továbbá – törvény ilyen tartalmú rendelkezése vagy erre vonatkozó megállapodás alapján – közvetlen hozzáférés biztosításával.

(5) A személyes adat továbbítására irányuló adattovábbítás törvényben meghatározott feltételek fennállása esetén, ennek hiányában az érintett előzetes és önkéntes hozzájárulása alapján teljesíthető.

(6) Az elsődleges adatkezelő szervek – illetve feladatuk ellátásához szükséges módon és mértékben az elsődleges adatkezelő szervek által felhatalmazott szervezeti egységek – feladata az adattovábbítás végrehajtása. Az adattovábbítás előtt be kell szerezni az adatvédelmi tisztviselő egyetértését.

- (7) Közigazgatási szerv, bíróság, ügyészség, rendőrség vagy más nyomozóhatóság, továbbá nemzetbiztonsági szolgálat adatszolgáltatási tárgyú megkeresését a főigazgató részére kell felterjeszteni. A főigazgató jelöli ki az adatszolgáltatót.
- (8) Amennyiben az adatkezelő szerv olyan adatra vonatkozó megkeresést kap, melynek jogszerűségét nem tudja megítélni, köteles azt az adatvédelmi tisztviselő útján a főigazgatónak jelenteni. A főigazgató az adatvédelmi tisztviselő állásfoglalása ismeretében dönt a megkeresés teljesítéséről.
- (9) Személyes adatok továbbítása során, amennyiben az belső vagy külső küldeményként történik, biztosítani kell, hogy zártan kerüljön feladásra.
- (10) Személyes adatok elektronikus továbbítása során az Informatikai Biztonsági Szabályzat (IBSZ) szerint szükséges eljárni.

3. Az Múzeum, mint adatfeldolgozó

- (1) Azon jogviszonyokban, ahol a Múzeum, mint adatfeldolgozó vesz részt, az adatkezelés jogalapját az adatkezelővel megkötött adatfeldolgozási szerződés képezi a GDPR 28. cikkében meghatározottak szerint.
- (2) Az adatfeldolgozási szerződés keretein belül végzett személyes adatkezelésre, az érintett általi adatigénylésre a jelen szabályzat rendelkezésétől eltérően az adatkezelővel megkötött adatfeldolgozási szerződés rendelkezéseit kell megfelelően alkalmazni.

4. Az adatvédelmi tisztviselő

- (1) Az Adatvédelmi tisztviselő a jogszabályban meghatározott feltételeknek megfelelő személy lehet. Az adatvédelmi tisztviselőt a főigazgató jelöli ki, közvetlenül a főigazgatónak tartozik felelősséggel.
- (2) Az adatvédelmi tisztviselő feladatait a GDPR 39. cikke rögzíti.
- (3) Az adatvédelmi tisztviselő nevééről és elérhetőségéről a Múzeum munkatársait tájékoztatni kell, valamint a Hatóság nyilvántartásába be kell jelenteni.
- (4) A főigazgató biztosítja az adatvédelmi tisztviselő számára meghatározott feladata kapcsán eljárva a hozzáférést a feladatai végrehajtásához szükséges elektronikus rendszerekhez, iratokhoz, egyéb adathordozókhoz, valamint a szakmai ismeretei naprakészen tartásához szükséges feltételeket, jogosultságokat és erőforrásokat rendelkezésére bocsátja.
- (5) A Múzeummal foglalkoztatási jogviszonyban álló személyek a személyes adataik kezeléséhez és jogaik gyakorlásához kapcsolódó valamennyi kérdésben a hivatali út betartása nélkül, közvetlenül fordulhatnak az adatvédelmi tisztviselőhöz.
- (6) A Múzeum valamennyi foglalkoztatottja és szervezeti egysége köteles együttműködni az adatvédelmi tisztviselővel.

(7) Az adatvédelmi tisztviselő szakmai tanácsát az adatkezelő szervezeti egység az alábbi esetekben köteles kikérni:

- a) olyan megállapodás, szerződés, szabályzat esetén, mely érinti az Múzeum adatkezelési tevékenységét;
- b) adatkezelési tájékoztató tartalmával kapcsolatban az érintetteknek történő átadás előtt.

(8) Amennyiben az adatvédelmi tisztviselő adatvédelmi szempontból egyetért a (3) bekezdés szerinti dokumentummal, azt „**Adatvédelmi szempontból egyetértek**” szöveggel, dátummal és aláírással látja el. Egyet nem értés esetén a dokumentumot „**Adatvédelmi szempontból nem értek egyet**” szöveggel, dátummal és aláírással látja el.

5. Adatkezelési tevékenységek nyilvántartása

(1) A GDPR 30. cikkében meghatározott nyilvántartást az adatvédelmi tisztviselő vezeti.

(2) Az adatkezelő szervezeti egységek naprakész nyilvántartást vezetnek a GDPR 30. cikkében meghatározott adatokról, amelyet megküldenek az adatvédelmi tisztviselő részére, aki ezek alapján vezeti az (1) bekezdés szerinti nyilvántartást.

(3) Az adatkezelő szervezeti egységek kötelesek haladéktalanul tájékoztatni az adatvédelmi tisztviselőt, ha az általuk végzett adatkezelési tevékenységben – így különösen a kezelt adatok körében, az érintettek kategóriájában, az adatkezelés céljában, az adatkezelés időtartamában – változás következik be.

(4) A GDPR 30. cikkében meghatározott nyilvántartás elkészítésének határideje 2021. június 30.

6. Az adatok védelme

(1) A Múzeum minden ésszerű intézkedést megtesz annak érdekében, hogy az általa kezelt adatok illetéktelenek számára ne legyenek hozzáférhetőek.

Az Múzeum kiemelt figyelmet fordít az adatok bizalmas kezelésére.

(2) Az elektronikus adatokhoz korlátozott a hozzáférés működik.

(3) A fenti célok érdekében az Múzeum a kezelésében lévő elektronikus adatokat az Informatikai Biztonsági Szabályzatban foglaltak szerint tárolja.

(4) Az Múzeummal minden munkaviszonyban vagy megbízási jogviszonyban álló személy, aki személyes adat birtokába jut, illet munkaköre vagy megbízatása alapján kezel, köteles védeni és őrizni a személyes adatokat, és úgy eljárni, hogy azok megfelelő védelmét biztosítsák.

7. Adatvédelmi incidensek

(1) Adatvédelmi incidens gyanúja esetén minden múzeumi dolgozó köteles haladéktalanul értesíteni az adatvédelmi tisztviselőt, aki kivizsgálja, hogy valóban fennáll-e az adatvédelmi incidens. Az adatvédelmi tisztviselő a vizsgálatba bevonhatja az Múzeum bármely érintett szervezeti egységét.

(2) Amennyiben az adatvédelmi tisztviselő megállapítja, hogy az adatvédelmi incidens fennáll, a GDPR 33. cikk (1) bekezdésére figyelemmel megvizsgálja, hogy az valószínűsíthetően

kockázattal jár-e a természetes személyek jogaira és szabadságára nézve. E vizsgálatba bevonhatja a Múzeum bármely érintett szervezeti egységét.

(3) Amennyiben az adatvédelmi tisztviselő megállapítja, hogy az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságára nézve, azt a főigazgató előzetes tájékoztatása után –bejelenti a felügyeleti hatóságnak.

(4) Az adatvédelmi tisztviselő nyilvántartja az adatvédelmi incidenseket a GDPR 33. cikk (5) bekezdésében meghatározott tartalommal.

8. Adatvédelmi hatásvizsgálat

(1) A GDPR 35. cikke szerinti adatvédelmi hatásvizsgálatot az adatkezelő, illetve adatfeldolgozó szervezeti egységek végzik, melynek során az adatvédelmi tisztviselő szakmai tanácsát ki kell kérni.

(2) Az adatbirtokos abban az esetben végez előzetes hatásvizsgálatot tervezett vagy folyamatban lévő adatkezelésnél, ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, vagy az adatkezelés kockázatának és lényeges körülményének – különösen az adatkezelés technológiájának – megváltoztatása esetén.

(3) Az adatbirtokos a kockázatelemzési feladata kapcsán kikérheti a tervezett, illetve megváltozott adatkezelés által érintett személyek véleményét.

(4) Az adatbirtokos a kockázatelemzési feladata kapcsán kikéri a döntés végrehajtásáért felelős szakterület, az Informatikai osztály vezetőjének, mint az az elektronikus információs rendszer biztonságáért felelős szervezet vezetőjének vagy az elektronikus biztonságért felelős személynek és a rendszerek üzemeltetésében részt vevő szervezeteknek, valamint az adatvédelmi tisztviselőnek a véleményét.

(5) Ha a tervezett adatkezelés annak körülményeire, így különösen céljára, az érintettek körére, az adatkezelési műveletek során alkalmazott technológiára tekintettel – az adatkezeléssel várhatóan érintett személyek jogaira és szabadságaira nézve – valószínűsíthetően magas kockázatot nem azonosít, vagy megállapítást nyer, hogy az adatkezelés az adatvédelmi hatásvizsgálat lefolytatása alóli mentesítést tartalmazó valamely jogszabályban meghatározott kivételi körbe tartozik, úgy ennek tényét az adatbirtokos írásban rögzíti.

(6) Az adatbirtokos köteles az előkészített adatkezelés esetén az adatkezelési tevékenységek nyilvántartásáról szóló dokumentumot kitölteni és azt az adatvédelmi tisztviselőnek megküldeni. Az adatvédelmi tisztviselő a megküldött dokumentumot az adatkezelési tevékenységek nyilvántartásába bejegyzi.

(7) Amennyiben az adatbirtokos az adatkezeléssel várhatóan érintett személyek jogaira és szabadságaira nézve magas kockázatot azonosít, vagy jogszabályi rendelkezés alapján adatvédelmi hatásvizsgálattal kötelezően vizsgálandó adatkezelési tevékenységek esete áll fenn, –

a döntése alapjául szolgáló legfontosabb szempontokat írásban megjelölve – adatvédelmi hatásvizsgálat lefolytatását kezdeményezi a főigazgatónál.

(8) A főigazgató az adatbirtokos javaslatára elrendeli az adatvédelmi hatásvizsgálat lefolytatását, vagy írásban rögzíti mellőzésének okait és az adatvédelmi tisztviselő kapcsolódó álláspontját. Az adatvédelmi hatásvizsgálat lefolytatásáig vagy az annak elmaradásával kapcsolatos okok írásban történő rögzítéséig az adatkezelésről szóló döntés nem hozható meg.

(9) Az adatbirtokos és az adatkezelés által érintett személyek az adatvédelmi hatásvizsgálat eredményeiről összefoglaló jelentést készítenek, amelyet a főigazgató hagy jóvá.

(10) Az adatvédelmi tisztviselő a jelentés alapján az adatkezelést bevezeti az adatkezelési tevékenységek nyilvántartásába.

(11) Ha az adatvédelmi hatásvizsgálat arra az eredményre jut, hogy a tervezett adatkezelés jelentette kockázat nem mérsékelhető a rendelkezésre álló technológiák és a végrehajtási költségek szempontjából észszerű módon – vagy azt jogszabály kötelezően előírja –, akkor az adatkezelő szerv előzetes konzultációt kezdeményez a Hatóságnál.

9. Az adatvédelmi incidens

a) Az adatvédelmi incidens észlelése és kezelése

(1) A Múzeum adatkezelésében bekövetkezett adatvédelmi incidens gyanúját észlelő személynek a tájékoztatást haladéktalanul az adatvédelmi tisztviselőhöz és az informatikai rendszerek informatikai biztonságáért felelős szervezeti egység vezetőjéhez kell megtenni.

(2) A Múzeumhoz külső észlelő személytől származó, a Múzeum adatkezelésére vonatkozó adatvédelmi incidens gyanújának tárgyában érkezett tájékoztatást haladéktalanul továbbítani kell az adatvédelmi tisztviselőnek és az informatikai rendszerek informatikai biztonságáért felelős szervezeti egység vezetőjének.

(3) Ha a Múzeum ellenőrzésre jogosult szervezeti egysége a feladata ellátása során adatvédelmi incidens gyanúját észleli, haladéktalanul értesíti az adatvédelmi tisztviselőt és az informatikai rendszerek informatikai biztonságáért felelős szervezeti egység vezetőjét.

(4) Az adatvédelmi tisztviselő és az informatikai rendszerek informatikai biztonságáért felelős szervezeti egység vezetője (a továbbiakban: munkacsoport) megvizsgálja, hogy

- a) a tájékoztatás alapján fennáll-e a gyanúja az adatvédelmi incidens bekövetkezésének;
- b) az adatvédelmi incidens az informatikai rendszert érintően következett-e be;
- c) mely szervezeti egységeket kell bevonni az intézkedések megtételébe.

(5) A munkacsoport – amennyiben az incidens gyanúja felmerül – a döntés előkészítésére szolgáló anyagot megküldi az adatbirtokos számára.

(6) Az adatbirtokos vizsgálja a feladat- és hatáskörébe tartozó nem informatikai rendszert érintő adatvédelmi incidens gyanújával érintett tájékoztatásokat.

b) Eljárás adatvédelmi incidens esetén

(1) Ha az adatvédelmi incidens a rendelkezésre álló adatok alapján egyértelműen megállapítható, az adatbirtokos az 1. függelék szerint bejelentett adatokat megküldi az adatvédelmi tisztviselőnek, aki 72 órán belül intézkedik a hatósági nyilvántartásba való bejelentésről.

(2) Ha a rendelkezésre álló adatok alapján az adatbirtokos egyértelműen nem tudja megállapítani az adatvédelmi incidens bekövetkezését, de feltételezhető, hogy az esemény magas kockázattal járt, az adatvédelmi tisztviselő véleményének megkérése mellett haladéktalanul összehívja a munkacsoportot.

(3) A vizsgálat az adatvédelmi tisztviselő véleményének, szakértői tanácsának kikérésével és annak figyelembevételével történik.

(4) A munkacsoport a tájékoztatást megvizsgálja, a tájékoztatótól, valamint az adatfeldolgozótól szükség esetén további adatszolgáltatást kér, amelyet az érintettek kötelesek haladéktalanul teljesíteni.

(5) A munkacsoport gondoskodik az elsődleges intézkedések megtételéről. Ha a vizsgálat során a munkacsoport megállapítja az érintettek jogaival és szabadságaival kapcsolatban a magas kockázat fennállását, akkor az 1. függelék szerinti adatokat az adatvédelmi tisztviselő közreműködésével a Hatóság részére 72 órán belül megküldi az erre rendszeresített elektronikus felület igénybevételével.

(6) Az adatvédelmi tisztviselő a munkacsoport vagy az adatbirtokos által megküldött, 2. függelék szerinti adatvédelmi incidenst bevezeti a Múzeum adatvédelmi incidens-nyilvántartásába.

10. Az adatfeldolgozás

(1) A Múzeum adatfeldolgozót vehet igénybe. Az adatfeldolgozó az adatkezelési műveletekhez kapcsolódó technikai feladatokat végzi, és e minőségében gyakorolja az adatkezelő Múzeum által átruházott jogosultságokat, teljesíti kötelezettségeit.

(2) Az adatfeldolgozásra vonatkozó megállapodást írásba kell foglalni. Amennyiben az adatfeldolgozóként igénybe venni kívánt szervre vagy személyre az utasítás hatálya nem terjed ki, akkor a megállapodásban kell érvényesíteni az adatfeldolgozóval szemben e címben foglalt előírásokat.

(3) Adatfeldolgozó igénybevétele esetén az adatkezelés céljának meghatározására, az adatkezelésre vonatkozó érdemi döntések meghozatalára az adatkezelő jogosult.

(4) Az adatfeldolgozó tevékenységi körén belül, illetve az adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, továbbá minden olyan jogsértésért, amit az adatkezelő utasításának vagy

az adatfeldolgozással összefüggésben kötött megbízási szerződésben foglaltak megszegésével okozott.

11. Adatbiztonsági előírások

- (1) Az adatkezelő szerv, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról.
- (1) Az elektronikusan kezelt adatállományok tekintetében biztosítani kell, hogy a különböző nyilvántartásokban tárolt adatok – törvény eltérő rendelkezése hiányában – közvetlenül ne legyenek összekapcsolhatóak.
- (2) Az informatikai adatbiztonsági előírások részletes meghatározását külön szabályzat tartalmazza.

III. AZ ÉRINTETT JOGAI ÉS AZ ÉRINTETT JOGAINAK ÉRVÉNYESÍTÉSÉVEL ÖSSZEFÜGGŐ FELADATOK

1. Az érintettnek joga van írásban tájékoztatást kérni a Múzeum által kezelt személyes adatai vonatkozásában
 - a) a személyes adatok köréről,
 - b) az adatkezelés jogalapjáról,
 - c) az adatkezelés céljáról,
 - d) a címzettek vagy címzettek kategóriáiról, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják,
 - e) az adattárolás időtartamáról,
 - f) az adatok forrására vonatkozó minden elérhető információról, ha az adat nem az érintettől származik.
2. Az érintett írásban kérheti, hogy a Múzeum
 - a) módosítsa valamely kezelt személyes adatát,
 - b) törölje személyes adatait,
 - c) a rá vonatkozó, általa az adatkezelő szerv rendelkezésére bocsátott, bármilyen formában rögzített személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja.
3. A Múzeum – az adatvédelmi tisztviselő útján – a kérelemnek, ha jogszabály ellentétesen nem rendelkezik, legfeljebb 30 napon belül eleget tesz. A kérelem teljesítéséről vagy annak elutasításáról 30 napon belül köteles tájékoztatni az érintettet.
4. Az érintettet megillető jogok gyakorlására az érintettek adatainak védelmét szolgáló adatbiztonsági követelményeket szem előtt tartva csak a kérelmező megfelelő azonosítása, illetve kérelme tartalmának hitelesítése esetén van lehetőség. Nem biztosítható ezen jogok gyakorlása különösen az elektronikusan aláírással nem hitelesített, vagy a kérelmező személyének azonosítását nem biztosító elektronikus levél, valamint telefax útján érkezett kérelmek esetén.

5. A Múzeum az érintett részére nyújtandó bármely értesítést és tájékoztatást könnyen hozzáférhető és olvasható formában, lényegre törő, világos és közérthetően megfogalmazott tartalommal teljesíti. A Múzeum az információt írásban, elektronikus úton, illetve az érintett kérelmére szóban is megadhatja, amennyiben az érintett személyazonossága igazolt.
6. Az érintett hozzáférési jogának gyakorlása során a tájékoztatást és az adatról kért első másolatot díjmentesen kell biztosítani, kivéve, ha az érintett kérelme – annak ismétlődő jellege vagy jogszabályban, illetve a Hatóság joggyakorlata értelmében – túlzó. Ez esetben – eltérő jogszabályi rendelkezés hiányában – az adatkezelő szerv jogosult észszerű költségtérítést megállapítani a vonatkozó jogszabályok előírásai alapján.

III. FEJEZET ZÁRÓ RENDELKEZÉSEK

Jelen szabályzat 2021. január 1. napján lép hatályba.

Kelt: Budapest, 2020. december 22.



.....
Demeter Szilárd
főigazgató



IV. FEJEZET

IV. MELLÉKLETEK

1. számú melléklet: Bejelentő lap az adatkezelő részére adatvédelmi incidens esetén
2. számú melléklet: Az érintett tájékoztatása az adatvédelmi incidensről

1. számú melléklet: Bejelentő lap az adatvédelmi tisztviselő részére adatvédelmi incidens esetén

1. Az adatvédelmi incidenst bejelentő Tájékoztató adatai:

Név:

E-mail-cím:

Cím:

Telefonszám:

Kapcsolattartó megnevezése, elérhetősége (telefonszám, e-mail):

1.1. Az adatkezelőn kívüli felek részvétele az adatvédelmi incidenssel érintett szolgáltatásban:

1.2. Részt vesz-e az adatkezelőn kívül más az adatvédelmi incidenssel érintett szolgáltatásban:

1.3. Az adatkezelőn kívüli fél megnevezése és minősége:

2. Az adatvédelmi incidenssel kapcsolatos időpontok:

Kezdő időpont:

Záró időpont:

Az adatvédelmi incidens továbbra is fennáll:

Az incidensről való tudomásszerzés időpontja:

Az incidens észlelésének módja:

Az adatfeldolgozó általi értesítés időpontja:

A késedelmes tájékoztatás indokai:

Egyéb megjegyzések az incidens időpontját illetően:

3. Az adatvédelmi incidens adatai (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

3.1. Sérülés jellege:

– bizalmas jelleg:

– integritás:

– rendelkezésre állás:

3.2. Az adatvédelmi incidens jellege (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

– eszköz elvesztése vagy ellopása:

– informatikai rendszer feltörése (hackelés):

– papíralapú dokumentum nem megfelelő módon történő megsemmisítése:

– papíralapú dokumentum elvesztése, ellopása vagy olyan helyen hagyása, amely nem minősül biztonságosnak:

– rosszindulatú számítógépes programok (pl. zsarolóprogram):

– elektronikus hulladék (a személyes adatok rajta maradnak az elavult eszközön):

- személyes adatok téves címzett részére történő küldése:
- levél elvesztése vagy jogosulatlan felnyitása: – adathalászat:
- személyes adatok nagy nyilvánosság előtti jogellenes közzététele:
- személyes adatok jogosulatlan szóbeli közlése:
- egyéb:

4. Az adatvédelmi incidens okai (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- szervezeten belüli, rosszhiszeműnek nem minősülő cselekmény (belső szabályzat megsértése által):
- szervezeten belüli, rosszhiszemű cselekmény:
- külső, rosszhiszeműnek nem minősülő cselekmény:
- külső, rosszhiszemű cselekmény:
- egyéb:

5. Az adatvédelmi incidenssel érintett személyes adatok köre:

5.1. Személyes adatok (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- személyazonossághoz kapcsolódó adatok:
- elérhetőségi adatok:
- azonosító adatok:
- személyi szám:
- hivatalos okmányok:
- helymeghatározó adatok:
- gazdasági, pénzügyi adatok:
- büntetett előélettel, bűncselekményekkel vagy büntetéssel, intézkedéssel kapcsolatos adatok:
- különleges adatok:

5.2. Különleges adatok (legalább egy kiválasztása kötelező):

- faji eredetre, nemzetiséghez tartozásra vonatkozó adatok:
- politikai véleményre vonatkozó adatok:
- vallásos vagy más világnézeti meggyőződésre vonatkozó adatok:
- érdekképviselési szervezeti tagságra vonatkozó adatok:
- szexuális életre vonatkozó adatok:
- egészségügyi adatok:
- genetikai adatok:
- biometrikus adatok:
- még nem ismert:
- egyéb:

5.3. Az adatvédelmi incidenssel érintett személyes adatok becsült száma:

6. Az érintettek jellege (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- alkalmazottak:

- felhasználók:
- ügyfelek (jelenlegi és potenciális):
- kiskorúak:
- kiszolgáltatott személyek:
- hatósági eljárás vagy intézkedés alá vont, vagy azok által érintett személyek:
- még nem ismert:
- egyéb:

6.1. Az incidenssel érintett adatalanyok részletes leírása (pl. adatbázisokban szereplő foglalkoztatottak leírása):

6.2. Az adatvédelmi incidenssel érintettek becsült száma:

7. Az incidens bekövetkezését megelőző események leírása:

8. Következmények:

8.1. Bizalmas jelleg sérülése (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult:
- az adat összekapcsolhatóvá vált az érintett egyéb adataival:
- az adatot más célokból történő, tisztességtelen módon történő kezelése lehetséges:
- egyéb:

8.2. Integritás sérülése (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- az adat módosíthatóvá vált annak ellenére, hogy archivált vagy elavult volt:
- az adatot valószínűsíthetően módosították egyébként pontos adatokra, és azokat eltérő célokra használhatták:
- egyéb:

8.3. Rendelkezésre állás sérülése (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- az érintettek számára történő kritikus szolgáltatásnyújtás képességének módosulása:
- egyéb:

8.4. Az érintetteket ért fizikai, anyagi vagy nem vagyoni károk vagy egyéb jelentős következmények:

8.5. Az incidens valószínűsíthető hatásai az érintettekre (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- személyes adatok feletti rendelkezés elvesztése:
- érintett jogainak korlátozása:
- hátrányos megkülönböztetés:
- személyazonosság-lopás:
- személyazonossággal való visszaélés:
- pénzügyi veszteség:

- álnevesítés engedély nélküli feloldása:
- jó hírnév sérelme:
- szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése:
- egyéb:

8.6. A valószínűsíthető következmények súlyossága (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- elhanyagolható:
- korlátozott:
- jelentős:
- maximális:

9. Az incidens orvoslására megtett intézkedések:

9.1. Megtett intézkedések (az adatvédelmi tisztviselő vagy a bizottság tölti ki):

A megtett védelmi intézkedések leírása:

9.2. Az érintettek tájékoztatása (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

A tájékoztatás tervezett időpontja:

- még nincsen eldöntve:
- a tájékoztatás hiányának indokai:
- tényleges ideje, tartalma:
- érintetteknek javasolt intézkedések:
- intézkedések leírása, amelyek alapján az érintettek tájékoztatására nem került sor:
- tájékoztatott érintettek száma:
- az érintett tájékoztatásának formája:
- az érintetteknek szóló tájékoztatás tartalma:
- nyilvánosan közzétett információk vagy hasonló intézkedés:

10. Egyéb:

11. Egyéb bejelentések:

Más hatóságoknak (EU-tagállami) vagy tagállamnak bejelentette-e az adatvédelmi incidenst?:

2. számú melléklet: Az érintett tájékoztatása az adatvédelmi incidensről

1. Az adatvédelmi incidens időpontja:

2. Jellege:

3. Az adatvédelmi tisztviselő/kapcsolattartó neve:

Elérhetősége:

4. Az adatvédelmi incidensből eredő valószínűsíthető következmény(ek):

5. Az adatvédelmi incidens kezelésével kapcsolatban tervezett, illetve megtett intézkedések (ideértve a hátrányos következmények enyhítését célzó intézkedéseket):

6. Az érintett számára javasolt intézkedések megtétele a bekövetkezett kár enyhítése érdekében: