Iktatószám: SZM/347-5/2023/101

A Szépművészeti Múzeum főigazgatójának

5/2023. (VI. 8.) főigazgatói utasítása

a Szépművészeti Múzeum adatvédelmi, adatbiztonsági és incidenskezelési szabályzatáról

1. A Szépművészeti Múzeum adatvédelmi, adatbiztonsági és incidenskezelési szabályzatát – a Szépművészeti Múzeum Szervezeti és Működési Szabályzatáról szóló 1/2022. (VI. 29.) főigazgatói utasítás Melléklet III. fejezet 1.1.2. pontjának e) alpontja, valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 25/A. § (3) bekezdése alapján – a Mellékletben foglaltak szerint állapítom meg.

2. Az adatvédelmi incidensek kockázatértékelésére vonatkozó szabályokat a Szépművészeti Múzeum integrált kockázatkezelési szabályzatáról szóló 1/2020. (VI. 22.) főigazgatói utasítással, valamint a Szépművészeti Múzeum informatikai biztonsági szabályzatáról szóló 17/2021. (XI. 8.) főigazgatói utasítással összhangban kell alkalmazni.

3. Ez az utasítás 2023. július 1-jén lép hatályba.

4. Ezen utasítás hatálybalépésével egyidejűleg hatályát veszti a Szépművészeti Múzeum adatvédelmi és adatbiztonsági szabályzatáról szóló 7/2018. (VIII. 28.) főigazgatói utasítás.

Dr. Baán László
főigazgató

SZÉPMŰVÉSZETI MÚZEUM * 1. *

Melléklet az 5/2023. (VI. 8.) főigazgatói utasításhoz

I. A Szabályzat célja, hatálya és jogszabályi alapjai

1. A Szépművészeti Múzeum (a továbbiakban: Múzeum) jelen Szabályzatának (a továbbiakban: Szabályzat) célja, hogy a személyes adatok védelméhez fűződő jogok érvényesülésének biztosítása, továbbá a Múzeum által kezelt személyes adatok magyar és európai uniós jogszabályokkal összhangban történő kezelése érdekében meghatározza a Múzeum tevékenysége során irányadó adatvédelmi és adatbiztonsági előírásokat.

2. A Szabályzat létrehozásának jogszabályi alapja az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 25/A. § (3) bekezdése, mely szerint a Múzeumnak adatvédelmi és adatbiztonsági szabályzatot kell készítenie.

3. A Szabályzat hatálya kiterjed a Múzeum munkavállalói által megvalósított adatkezelésre.

4. A Szabályzatban foglaltakat
   a) az Európai Parlament és a Tanács (EU) 2016/679. sz. rendelete 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), valamint
   b) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.).

   rendelkezéseivel összhangban kell alkalmazni.

5. Fogalom meghatározások

Fogalom megnevezése	Definíció, magyarázat
adatbiztonság	A személyes adatok jogosulatlan kezelése, így különösen megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások, valamint eljárási szabályok összessége, az adatkezelés azon állapota, amelyben a kockázati tényezőket a szervezési, műszaki megoldások és intézkedések a minimálisra csökkentik.
adatfeldolgozás	Az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége.
adatfeldolgozó	Az a természetes vagy jogi személy, vagy jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel - az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel.

adatkezelés	Az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.
adatkezelés korlátozása	A tárolt adat zárolása az adat további kezelésének korlátozása céljából.
adatkezelő	Jelen szabályzat vonatkozásában a Múzeum, 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 végrehajtatja.
adatmegsemmisítés	Az adatot tartalmazó adathordozó teljes fizikai megsemmisítése.
adattovábbítás	Az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.
adattörlés	Az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges.
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.
azonosítható természetes személy	Az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító (név, azonosító szám, helymeghatározó adat, online azonosító stb.) vagy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.
álnevesítés	Személyes adat olyan módon történő kezelése, amely - a személyes adattól elkülönítve tárolt - további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely érintettre vonatkozik, valamint műszaki és szervezési intézkedések megtételével biztosítja, hogy azt azonosított vagy azonosítható természetes személyhez ne lehessen kapcsolni.
az érintett hozzájárulása	Az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez.

biometrikus adat	Egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat;
címzett	Az a természetes vagy jogi személy, vagy jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő vagy az adatfeldolgozó hozzáférhetővé tesz.
érintett	Bármely információ alapján azonosított vagy azonosítható természetes személy.
harmadik személy	Olyan természetes vagy jogi személy, vagy jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek.
Hatóság	Az általános adatvédelmi rendeletben a felügyeleti hatóság részére megállapított feladat- és hatásköröket gyakorló államigazgatási szerv, amely a Szabályzat hatályba lépésének napján a Nemzeti Adatvédelmi és Információszabadság Hatóság.
különleges adat	A személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.
nyilvánosságra hozatal	Az adat bárki számára történő hozzáférhetővé tétele.
profilalkotás	Személyes adat bármely olyan - automatizált módon történő - kezelése, amely az érintett jellemzőinek, különösen a munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy látogatói érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelésére, elemzésére vagy előrejelzésére irányul.
személyes adat	Az érintettre vonatkozó bármely információ.

II. Az adatvédelem szervezeti felépítése

1. Főigazgató

1.1. A Múzeumot érintő adatvédelmi döntések meghozataláért és a vonatkozó szabályzatok kiadásáért a Főigazgató a felelős.

1.2. A Főigazgató az adatbiztonsággal kapcsolatos feladatait a Jogi Főosztályon működő adatvédelmi tisztviselő útján látja el.

2. Adatvédelmi tisztviselő

2.1. Az adatvédelmi tisztviselő figyelemmel kíséri és ellenőrzi a személyes adatok kezelésére vonatkozó előírások, így különösen a jogszabályok és a Szabályzat érvényesülését, tájékoztatást nyújt a személyes adatok kezelésére vonatkozó jogi előírásokról és azok érvényesítésének módjáról a Múzeum vezető beosztással rendelkező munkavállalói (a továbbiakban együtt: Vezetők) és munkavállalói, továbbá az adatfeldolgozó és az általa foglalkoztatott, az adatkezelési műveleteket végző személyek részére.

2.2. Az adatvédelmi tisztviselő e feladatkörében eljárva
a) elősegíti az érintettet megillető jogok gyakorlását, így különösen részt vesz az érintett panaszainak kivizsgálásában és kezdeményezi a panasz orvoslásához szükséges intézkedések megtételét;
b) szakmai tanácsadással elősegíti és figyelemmel kíséri az adatvédelmi hatásvizsgálat lefolytatását;
c) együttműködik az adatkezelés jogszerűségével kapcsolatos eljárások lefolytatására jogosult szervekkel és személyekkel, így különösen kapcsolatot tart a Hatósággal az előzetes konzultáció és a Hatóság által lefolytatott eljárások elősegítése érdekében;
d) közreműködik az adatvédelmi és adatbiztonsági szabályzat megalkotásában és gondoskodik annak naprakészen tartásáról;
e) a szervezeti egységek által végzett adatkezelések vonatkozásában a rendelkezésére bocsátott információk alapján vezeti az adatkezelési nyilvántartást, továbbá (a szervezeti egységek bevonásával) évente felülvizsgálja és szükség esetén módosítja azt;
f) Részt vesz az adatvédelmi incidensekre vonatkozó kockázatértékelés összeállításában.

3. Az informatikai biztonsági felelős

3.1. Az informatikai biztonsági felelős feladat- és hatáskörét (a Múzeum mindenkor hatályos informatikai biztonsági szabályzatában foglaltakkal összhangban) az Informatikai Osztály vezetője látja el.

3.2. Az informatikai biztonsági felelős
a) azonosítja és értékeli a Múzeum működéséből eredő, így az adatvédelemmel is összefüggő (az adatvédelmi incidensekre vonatkozó kockázatokra is kiterjedő) informatikai biztonsági kockázatokat, a kockázatok mérséklése érdekében intézkedési javaslatot terjeszt elő a Főigazgató számára;
b) ellenőrzi az informatikai eszközöket abból a szempontból, hogy azok alkalmasak legyenek az adatok biztonságos tárolására;
c) a személyes adatok kezelése körében (az adatvédelmi jogi szempontokról az adatvédelmi tisztviselővel egyeztetve) felelős a biztonságos adattárolásra és adattovábbításra vonatkozó informatikai szabályok meghatározásáért és az információ-biztonsági követelményeknek való megfelelésért.

4. Vezetők

4.1. A Vezetők felelősek azért, hogy a vezető beosztásukból eredő vagy az általuk vezetett szervezeti egység feladatkörébe tartozó adatkezelés a jogszabályoknak és a Múzeum belső szabályzatainak

megfelelően történjen. Ennek keretében a Szabályzat VII. fejezetében foglaltak szerint gondoskodnak a harmadik személytől érkező, a vezető beosztásukból eredő vagy az általuk vezetett szervezeti egység feladatkörébe tartozó adatkezelést érintő megkeresések teljesítéséről, amelyek megválaszolásához szükség szerint az adatvédelmi tisztviselővel egyeztetnek.

4.2. A Vezetők az adatvédelmi tisztviselőt haladéktalanul értesítik az általuk végzett adatkezelést érintő változásokról, különösen, ha

a) az adatkezelés céljában, az érintett vagy a kezelt adatok körében, vagy az adatok törlésének idejében történik változás vagy ennek igénye merül fel;
b) adatok továbbítására kerül sor;
c) a kezelt adatokat érintően adatkezelési incidens következik be vagy ennek veszélye fenyeget.

4.3. Az adatvédelmi szabályok megsértésének észlelése esetén (szükség esetén az adatvédelmi tisztviselővel egyeztetve) intézkednek a jogsértés megszüntetéséről és szükség szerint kezdeményezik a felelősségre vonási eljárást.

4.4. Az adatvédelmi incidensek vonatkozásában felmerülő kockázatok azonosításában a Vezetők a VIII. 2.3 és 2.4. pontban foglaltak szerint az adatvédelmi tisztviselővel és az informatikai biztonsági felelőssel együttműködve vesznek részt.

5. Beosztott munkavállalók

5.1. A Múzeum beosztott munkavállalói a feladatuk ellátásával összefüggésben tudomásukra jutott személyes adatokat a megfelelő gondossággal kezelik és gondoskodnak arról, hogy az adatok illetéktelenek számára ne váljanak hozzáférhetővé, továbbá elvégzik az adattörlést, amennyiben jogszerű kezelésük III. fejezet szerinti feltételei már nem állnak fenn.

III. Adatkezelés jogalapja, valamint tartalmi és eljárási szabályai

1. A személyes adatok kezelése a Múzeumnál kizárólag akkor és annyiban jogszerű, amikor és amennyiben legalább az alábbi jogalapok egyike teljesül:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
d) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
e) az adatkezelés az adatkezelő vagy harmadik személy jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

2. A hozzájárulás

2.1. Ha az adatkezelés hozzájáruláson alapul, az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett a személyes adatainak kezeléséhez hozzájárult. Az érintett hozzájárulását az adatkezelést végző szervezeti egység – az adatkezelés jellege szerint – elektronikusan vagy papír alapon tárolja.

2.2. Jelölőnégyzet bejelölésével megadott hozzájárulás esetén a hozzájárulás és a visszavonás ténye az adott adatkezelést végző szervezeti egységnél az adatkezeléshez kapcsolódóan vezetett nyilvántartásban kerül mentésre.

2.3. Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Az érintett hozzájárulását tartalmazó nyilatkozat bármely része, amely sérti a jogszabályokat, kötelező erővel nem bír.

2.4. Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja, amit ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását. A hozzájárulás visszavonása nem érinti a visszavonás előtti, hozzájáruláson alapuló adatkezelés jogszerűségét, amiről a hozzájárulás megadása előtt az érintettet tájékoztatni kell.

2.5. A hozzájárulás megadása nem tekinthető önkéntesnek, ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel és nem áll módjában a hozzájárulás anélküli megtagadása vagy visszavonása, hogy ez kárára válna.

2.6. A hozzájárulás olyan egyedi esetekben sem szolgálhat az adatkezelés érvényes jogalapjaként, amelyekben az érintett és az adatkezelő között egyértelműen egyenlőtlen viszony áll fenn az érintett rovására (pl.: munkaviszony).

2.7. A beleegyezés nem tekinthető önkéntesnek, ha a szerződés teljesítését olyan adatkezeléshez való hozzájárulástól teszi függővé, amely adatkezelés nem szükséges a szerződés teljesítéséhez.

3. Szerződés teljesítése

3.1. Természetes személlyel kötendő szerződés esetén a természetes személy (mint szerződő fél) személyes adatainak kezeléséhez történő hozzájárulása a szerződés kötelező tartalmi eleme.

4. Közfeladat ellátása

4.1. A Múzeum munkavállalói a Múzeum közfeladatellátása során a szükséges mértékben személyes adatokat kezelnek.

4.2. A Múzeum egyes helyiségeibe történő belépéshez szükséges különleges adatnak minősülő személyes (biometrikus) adatok kezelése esetében a Szabályzat III. fejezet 1. pont *d)* alpontjában említett jogalapot, miszerint az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, együtt kell értelmezni a GDPR 9. cikk (2) bekezdés b) pontjában foglaltakkal, miszerint az adatkezelés az

adatkezelőnek vagy az érintettnek a foglalkoztatást szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges.

5. Az adatkezelő jogos érdekein alapuló adatkezelés

5.1. Amennyiben a Múzeum, mint adatkezelő az általa folytatott bármely adatkezelés jogalapjaként a III. fejezet 1. pont *f)* alpontjára kíván hivatkozni, úgy köteles a hivatkozási alapul szolgáló jogos érdek azonosítása mellett legalább az alábbi szempontok vizsgálatára kiterjedő ellenőrzési folyamatot (érdekmérlegelés) lefolytatni:
   a) az adatkezelés célja összhangban van-e a Múzeum jogszabályban vagy belső szabályzatokban meghatározott céljaival;
   b) elérhető-e az adott cél vagy jogos érdek a tervezett adatkezelés nélkül, és ha igen, úgy ez milyen erőforrás-igénnyel járna, összehasonlítva a tervezett adatkezelés lefolytatásával;
   c) a tervezett adatkezelés elmaradása milyen hátrányt eredményezhet a Múzeum számára;
   d) a tervezett adatkezelés az érintett mely alapvető jogait érinti, és milyen mértékben;
   e) a tervezett adatkezelés az érintett milyen adatait érinti, csökkenthető-e ezen adatok köre a tervezett adatkezelés célja és a Múzeum jogos érdekeinek a veszélyeztetése nélkül;
   f) a tervezett adatkezelés során igénybe vett technikai megoldások a technika aktuális szintjéhez képest milyen kockázatokkal járnak, milyen védelmet biztosítanak az érintett részére, valamint milyen további erőforrás-igénnyel járna a védelem szintjének esetleges növelése.

IV. Adatvédelmi hatásvizsgálat

1. A Főigazgató bármely adatkezelés vonatkozásában dönthet adatvédelmi hatásvizsgálat elvégzéséről, továbbá elrendeli az adatvédelmi hatásvizsgálatot abban az esetben, amennyiben 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.

2. Amennyiben az adatvédelmi tisztviselő a Múzeum valamely adatkezelése vonatkozásában adatvédelmi hatásvizsgálat elvégzését javasolja vagy a fentiek szerinti magas kockázatú adatkezelésről az adatkezelést végző Vezető értesíti az adatvédelmi tisztviselőt, az adatvédelmi tisztviselő – külső szakértő megbízása esetén a vonatkozó intézményi szabályzatok rendelkezései szerint – a Főigazgatónál kezdeményezi a hatásvizsgálat lefolytatását.

3. A hatásvizsgálat dokumentációjának összeállításában, továbbá a megállapítások értékelésében azok a Vezetők és beosztott munkavállalók is részt vesznek, akik az adott adatkezelés vonatkozásában érintettek.

4. Az adatvédelmi hatásvizsgálatot a Hatóság mindenkor közzétett vonatkozó ajánlása, valamint a EU adatvédelmi munkacsoportjának iránymutatása, ennek hiányában pedig a bevett szakmai gyakorlatok szerint kell lefolytatni.

5. A hatásvizsgálatnak ki kell terjednie legalább
   a) az adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;

b) az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
c) az adatvédelmi hatásvizsgálattal érintett jogait és szabadságait érintő kockázatok vizsgálatára; és
d) a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és a GDPR-ral való összhang igazolását szolgáló, az érintett és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

6. Az adatvédelmi hatásvizsgálatról részletes dokumentáció készül, amely a Múzeum irattárában megőrzésre kerül.

7. A Főigazgató az adatvédelmi tisztviselő útján a tervezett adatkezelés megkezdése előtt szükség szerint konzultációt kezdeményez a Hatósággal. A konzultáció kötelező, amennyiben az adatvédelmi hatásvizsgálat azt állapította meg, hogy az adatkezelés a kockázatok mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár. Az adatvédelmi hatásvizsgálat lefolytatója köteles a Hatóság előzetes konzultáció során beszerzett álláspontját az adatkezeléssel kapcsolatban érvényesíteni.

8. A Főigazgató szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést rendel el annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

V. Az adatkezelési tevékenységek nyilvántartása

1. Az adatvédelmi tisztviselő a Múzeum által végzett valamennyi adatkezelést az 1. számú függelék szerinti adatkezelői nyilvántartásban tartja számon, amely elektronikusan vezetett táblázat az Infotv. 25/E. § (1) bekezdésében megjelölt adattartalommal.

2. Az adatkezelői nyilvántartást az adatvédelmi tisztviselő a Vezetők bevonásával évente legalább egy alkalommal felülvizsgálja. Amennyiben az adatvédelmi tisztviselő a kezelt adatok körében ettől függetlenül további változásról szerez tudomást, a nyilvántartást ennek megfelelően módosítja.

3. Az adatkezelői nyilvántartás aktuális tartalommal történő vezetéséhez a Vezetők a vezető beosztásukból eredő vagy az általuk vezetett szervezeti egység feladatkörébe tartozó adatkezelést érintő változásról az adatvédelmi tisztviselőt a II. fejezet 4. pont 4.2. alpontja szerint értesítik.

VI. Adatfeldolgozás és adattovábbítás

1. Adatfeldolgozás

1.1. A Múzeum mint adatkezelő – a vonatkozó jogszabályok és belső szabályzatok betartásával – adatfeldolgozót vehet igénybe, aki a Múzeum nevében folytatja az adatkezelést és e minőségében gyakorolja a Múzeum által átruházott jogosultságokat és teljesíti a kötelezettségeit. A Múzeum kizárólag olyan adatfeldolgozókat vehet igénybe, amelyek megfelelő garanciákat nyújtanak az adatkezeléssel összefüggő jogszabályok követelményeinek való megfelelésére és az érintett jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

1.2. Amennyiben valamely szervezeti egység adatkezelése során adatfeldolgozó igénybevétele válik szükségessé, a szervezeti egység az adatfeldolgozásról egyeztet az adatvédelmi tisztviselővel és kezdeményezi az adatfeldolgozási szerződés megkötését Az adatvédelmi tisztviselő az adatfeldolgozási szerződés előkészítésében a Múzeum mindenkor hatályos szerződéskötési és szerződéskezelési szabályzata szerint vesz részt.

1.3. Az adatfeldolgozásra vonatkozó szerződést írásba kell foglalni és abban érvényesíteni kell az adatfeldolgozóval szemben jelen fejezetben megfogalmazott előírásokat. A szerződésben ki kell kötni, hogy az adatfeldolgozó további adatfeldolgozót csak akkor vehet igénybe, ha ezt jogszabály nem zárja ki, és ha további adatfeldolgozó igénybevételéhez a Múzeum eseti vagy általános felhatalmazást ad. Az adatfeldolgozó a további adatfeldolgozó személyéről és az általa végzendő műveletekről a Múzeumot tájékoztatja.

1.4. Az adatfeldolgozó tevékenységi körén belül és a Múzeummal létrejött adatfeldolgozásra irányuló szerződés által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, továbbá minden olyan jogsértésért, amit a Múzeum utasításának vagy az adatfeldolgozással összefüggésben kötött szerződésben foglaltak megszegésével okozott.

1.5. A Múzeum – esetleges kártérítésre történő kötelezése esetén – az adatfeldolgozó felelősségének megállapítását kezdeményezi, amennyiben a kár bekövetkezését az okozta, hogy az adatfeldolgozó nem tartotta be a szerződésben foglaltakat vagy a Múzeum utasításától eltért.

2. Harmadik személy részére történő adattovábbításra a Múzeum munkavállalója által csak az adatkezelési tevékenységek nyilvántartásában foglaltakkal összhangban kerülhet sor.

VII. Az érintett jogainak érvényesítésével összefüggő feladatok

1. Az érintett tájékoztatás iránti kérelme

1.1. Az érintett a jelen fejezet 1.6. pontjában foglalt módon írásban tájékoztatást kérhet a Múzeumtól személyes adatai kezeléséről és kérheti személyes adatainak helyesbítését, valamint – a kötelező adatkezelés kivételével – azok törlését („az elfeledtetéshez való jog"), jogosult továbbá a kezelt adataihoz hozzáférni, az adatok kezelésének korlátozását kérni, megilleti továbbá az adathordozhatósághoz való jog, valamint tiltakozhat személyes adatának kezelése ellen.

1.2. A tájékoztatást és intézkedést díjmentesen kell biztosítani. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, az adatkezelő (a kért tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre figyelemmel)
   a) ésszerű összegű díjat számíthat fel vagy
   b) megtagadhatja a kérelem alapján történő intézkedést.

1.3. A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása a Múzeumot terheli.

1.4. Az érintett tájékoztatás iránti kérelmét a jelen fejezet 1.6. pontjában foglaltak szerint az adatkezeléssel érintett Vezető vagy utasítására az adatkezelést végző munkatárs 30 napon belül köteles megválaszolni. A határidő a kérelem összetettségére tekintettel további 30 nappal meghosszabbítható, erről a válaszadásban érintett Vezető vagy utasítására az adatkezelést végző munkatárs közvetlenül, vagy a Kommunikációs Főosztály útján tájékoztatja az érintettet.

1.5. Az érintett részére rendelkezésre bocsátandó információk eltérőek lehetnek, annak függvényében, hogy a személyes adatokat az érintettől gyűjtik vagy ezeket az adatokat nem az érintettől, hanem egyéb forrásból szerezte meg a Múzeum.

1.6. Az érintett az adatkezelés megkezdésekor a Múzeum postacímére küldött levélben, az info@szepmuveszeti.hu e-mail címre küldött elektronikus levelében vagy személyesen kérheti az adatkezelésre vonatkozó tájékoztatást.
A személyes tájékoztatás során az adatkezelésért felelős Vezető vagy utasítására az adatkezelést végző munkatársa elsősorban szóban vagy (az érintett írásos válasz iránti kérelme esetén) a vonatkozó adatkezelési tájékoztató közvetlen vagy a Kommunikációs Főosztály útján történő megküldésével tájékoztatja az érintettet az adott adatkezelésről.
Amennyiben az érintett szükségesnek tartja, a válaszadásban érintett Vezető útján az adatvédelmi tisztviselőtől is kérhet tájékoztatást.

1.7. Az egyes adatkezelésekre vonatkozó általános tájékoztatást (tömör, átlátható és könnyen hozzáférhető formában) elsősorban a Múzeum honlapjain keresztül kell elérhetővé tenni. Ennek hiányában a tájékoztatást (szükség esetén) papír alapon, szóbeli tájékoztatással kiegészítve az adatkezelést megvalósító szervezeti egységnél és az adatvédelmi tisztviselőnél kell elérhetővé tenni.

2. A kezelt adatok helyesbítése

2.1. Ha a személyes adat a valóságnak nem felel meg és a valóságnak megfelelő személyes adat a Múzeum adatkezelést végző szervezeti egységénél rendelkezésére áll, a személyes adatot a Múzeum adott adatkezelést végző szervezeti egységének munkatársa helyesbíti.

2.2. A helyesbítést az érintett is kérheti a Múzeum postacímére küldött levélben vagy az info@szepmuveszeti.hu e-mail címre küldött elektronikus levélben. A kérésnek a Múzeum 2.1. pontban megjelölt munkatársa 30 napon belül tesz eleget.

2.3. Amennyiben a helyesbítés szükségességéről az adatkezelésért felelős Vezető (akár az érintett kérése, akár saját észrevétele alapján) tudomást szerez, haladéktalanul gondoskodik az adat helyesbítéséről és az érintett tájékoztatásáról. Ha az adatvédelmi tisztviselő értesül a helyesbítési kérelemről, ezt jelzi az adatkezelésért felelős Vezetőnek, aki intézkedik a helyesbítésről.

3. A kezelt adatok törlése

3.1. A személyes adatot törölni kell, ha
a) arra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását vagy a különleges adatok kezelésére adott kifejezett hozzájárulását, és az adatkezelésnek nincs más jogalapja;

c) az érintett tiltakozik az adatkezelés ellen és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
d) azt jogellenesen kezelték;
e) azt az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
f) azt közvetlenül gyermekektől, a számukra kínált, információs társadalommal összefüggő szolgáltatások nyújtása érdekében gyűjtötték.

3.2. Törlés helyett a Múzeum adatkezelésért felelős Vezetője vagy utasítására az adatkezelést végző munkatárs korlátozza a személyes adathoz történő hozzáférést, ha
a) az érintett vitatja a személyes adatok pontosságát, amely esetben a korlátozás arra az időtartamra vonatkozik, amíg az adatkezelő ellenőrzi a személyes adatok pontosságát;
b) az adatkezelés jogellenes, de az érintett (az adatok törlése helyett) azok felhasználásának korlátozását kéri;
c) az adatkezelőnek adatkezelés céljából már nincs szüksége a személyes adatokra, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez vagy
d) az érintett tiltakozott az adatkezelés ellen, amely esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

3.3. Az érintett kezelt adatának törlésére vagy korlátozására irányuló kérelmét a Múzeum postacímére küldött levélben vagy az info@szepmuveszeti.hu e-mail címre küldött elektronikus levélben terjesztheti elő. A kérelemre a Múzeum adatkezelésért felelős Vezetője vagy utasítására az adatkezelést végző munkatárs közvetlenül vagy a Kommunikációs Főosztály útján 30 napon belül köteles választ adni.

3.4. A 3.1. pontban írt esetekben az adatkezelést végző szervezeti egység munkatársa (a helyreállíthatatlanság biztosítása érdekében) logikailag és fizikailag is törli az adatot.

4. A tiltakozási jog gyakorlása

4.1. Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak kezelése ellen, ideértve a profilalkotást is, amennyiben az adatkezelés jogalapját az alábbiak képezik:
a) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
b) az adatkezelés az adatkezelő vagy harmadik személy jogos érdekeinek érvényesítéséhez szükséges.

4.2. Ebben az esetben a Múzeum a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

4.3. A tiltakozási jogra már az első kapcsolatfelvétel során kifejezetten fel kell hívni az érintett figyelmét és az erre vonatkozó tájékoztatást egyértelműen meg kell jeleníteni az adatkezelési tájékoztatóban.

4.4. Az érintett tiltakozási jogát a Múzeum postacímére küldött levélben vagy az info@szepmuveszeti.hu e-mail címre küldött elektronikus levélben gyakorolhatja.

4.5. Amennyiben az érintett gyakorolja tiltakozáshoz való jogát, a Múzeum megvizsgálja, hogy az érintett érdekeivel, jogaival és szabadságaival szemben az adat kezeléséhez fűződő érdek elsőbbséget élvez-e.
A vizsgálatot az érintett szervezeti egységek bevonásával az adatvédelmi tisztviselő, vagy a Múzeum megbízásából külső szakértő folytatja le. Amennyiben megállapításra kerül, hogy az adat kezelését meg kell szüntetni, az adatvédelmi tisztviselő ezt jelzi az adatkezelést végző szervezeti egységnek, amely intézkedik az adatkezelés megszüntetéséről, szükség szerint az adatok törléséről.

4.6. Az érintett tiltakozási jogának gyakorlásával kapcsolatos kérelmére az adatkezelésért felelős Vezető közvetlenül vagy a Kommunikációs Főosztály útján 30 napon belül köteles választ adni.

5. Amennyiben valamely adat törléséről vagy korlátozásáról az adatvédelmi tisztviselő szerez tudomást, jelzi ezt az adatkezelésért felelős Vezetőnek, aki gondoskodik az adat törléséről vagy korlátozásáról.

VIII. Adatvédelmi incidensek kezelése, értékelése és nyilvántartása

1. Adatvédelmi incidensek kezelésére vonatkozó szabályok

1.1. A Szabályzat hatálya alá tartozó személyek a tudomásukra jutott adatvédelmi incidensről haladéktalanul kötelesek tájékoztatni a Főigazgatót.

1.2. A Főigazgató köteles a tudomására jutott adatvédelmi incidenseket (az adatvédelmi tisztviselő és szükség szerint az adatkezelésért felelős Vezető bevonásával) kivizsgálni és azokkal kapcsolatban a jelen fejezetben meghatározott intézkedéseket meghozni.

1.3. Az adatvédelmi incidens kivizsgálásában az adatvédelmi tisztviselő, valamint szükség szerint az adatkezelésért felelős Vezető is részt vesz azzal, hogy a vizsgálat megállapításairól az adatvédelmi tisztviselő a jelen szabályzat 4. számú függeléke szerinti jegyzőkönyvet veszi fel.

1.4. Az adatvédelmi incidenst a Múzeum – az adatvédelmi tisztviselő útján - indokolatlan késedelem nélkül, lehetőség szerint a tudomásszerzéstől számított 72 órán belül bejelenti a Hatóságnak a www.naih.hu honlapon rendszeresített dokumentummal, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

1.5. A Hatóságnak történő bejelentés dokumentumát (az érintett szervezeti egységek és az informatikai biztonsági felelős bevonásával) az adatvédelmi tisztviselő készíti el és terjeszti elő a Főigazgató számára.

1.6. A bejelentésben

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek körét és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

1.7. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintett jogaira és szabadságaira nézve, a Főigazgató vagy utasítására az adatkezelésért felelős Vezető indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

1.8. Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell az incidensből eredő esetleges következményeket és azon intézkedéseket, amelyek az incidensből eredő hátrányos következmények minimalizálására, elhárítására irányulnak. Amennyiben az érintett maga is csökkentheti az incidens bekövetkezéséből eredő hátrányokat, a tájékoztatásban erre vonatkozó javaslat is megfogalmazható.

1.9. A tájékoztató levél tervezetét az érintett szervezeti egységek, különösen az informatikai biztonsági felelős bevonásával az adatvédelmi tisztviselő készíti el és terjeszti elő a Főigazgató számára.

1.10. Nem szükséges az érintettet tájékoztatni a magas kockázattal járó adatvédelmi incidensről, ha

a) a Múzeum a megfelelő technikai és szervezési intézkedéseket (különösen az adatok titkosítása) megtette annak érdekében, hogy az adatok az azok megismerésére fel nem jogosítottak számára értelmezhetetlenek legyenek;
b) a Múzeum olyan intézkedéseket tett, amelyek következtében az incidensből származó magas kockázat az érintettre nézve nem következett be;
c) az értesítés aránytalan erőfeszítéssel járna, amely esetben a Múzeum a nagyszámú érintett részére honlapjain keresztül nyilvános értesítést tehet közzé.

2. Az adatvédelmi incidensek értékelése (kockázatértékelés)

2.1. Annak eldöntésére vagy valószínűsítésére, hogy egy adatvédelmi incidens milyen mértékű kockázattal jár az érintett adataira és jogaira nézve, a Múzeum előzetesen azonosítja és értékeli a lehetséges kockázatokat.

2.2. Az adatvédelmi incidensek kockázatkezelésének mintáját a 3. számú függelék tartalmazza.

2.3. A felmerülő kockázatok azonosításában a Vezetők az adatvédelmi tisztviselővel együttműködve vesznek részt, míg a kockázatok informatikai biztonsággal összefüggő felmérése és értékelése az informatikai biztonsági felelős feladata.

2.4. A Szabályzat hatályba lépésének évében a kockázatértékelést 2023. augusztus 31-ig kell lefolytatni azzal, hogy a Vezetők és az informatikai biztonsági felelős által azonosított kockázatokat az adatvédelmi tisztviselő összesíti, majd felterjeszti főigazgatói jóváhagyásra.

2.5. A továbbiakban a kockázatkezelési tervet szükség szerint, de legalább évente egy alkalommal felül kell vizsgálni. A kockázatkezelési terv tartalmának érdemi felülvizsgálatát a Vezetők, valamint az informatikai biztonsági felelős végzi, a felülvizsgálat koordinálása az adatvédelmi tisztviselő feladata.

2.6. Az incidensek mérlegelésénél különösen az alábbi tényezőket kell együttesen figyelembe venni:

a) Az incidens jellege: alapvetően befolyásolja az érintettre vonatkozó kockázat megítélését, hogy milyen jellegű tevékenység vagy esemény következett be, mert az adatvesztés kevésbé hátrányos következményekkel jár az érintettre nézve, mint az adatokat érintő jogosulatlan hozzáférés.

b) A személyes adatok jellege: minél érzékenyebb adatok érintettek az incidensben, annál jelentősebb hátránnyal járhat az érintett számára. Figyelembe kell venni azonban az adatok összetettségét is, vagyis azt a szempontot, hogy egyazon incidens során az érintettre vonatkozóan milyen mennyiségű és típusú adat érintett.

c) Az érintett azonosíthatósága: vizsgálni szükséges, hogy az incidens következtében az érintett azonosítására milyen mértékben van lehetőség.

d) A következmények súlyossága: a hátrányok összessége.

e) Az egyén sajátosságai: az érintett valamely tulajdonságánál fogva magasabb védelemben részesül-e (pl. gyerekek).

f) Az érintettek száma: az adatvédelmi incidens milyen számú érintettre járhat hátrányos következményekkel.

2.7. A kockázatok értékelése során figyelembe kell venni bekövetkezésük valószínűségét és a személyes adatok biztonságos kezelésére gyakorolt kedvezőtlen hatását. Az e két tényezőre adott számszerűsített érték szorzata adja a kockázat értékét.

VALÓSZÍNŰSÉG						
Megnevezés	Érték					
A kockázat rendszeresen fennáll; ha vizsgáljuk, akkor általában tapasztaljuk is.	5	5	10	15	20	25
A kockázat rendszeresen előfordulhat, többször is ismétlődhet.	4	4	8	12	16	20
A kockázat többször, ismétlődően várható.	3	3	6	9	12	15
A kockázat ritkán, várhatóan egy-egy esetben fordul elő.	2	2	4	6	8	10
A kockázat ritkán, váratlanul fordul elő	1	1	2	3	4	5

		1	2	3	4	5	Érték
		Elenyésző	Számottevő, de alacsony	Közepes, lényeges	Jelentős	Súlyos	Megnevezés
							HATÁS

2.8. A 2.6. pontban foglaltak szerint megállapított kockázati érték alapján a kockázatot be kell sorolni a megfelelő kockázati szintbe:

a) Magas kockázat (17-25 pont): Nem elfogadható mértékű kockázat, amely minden esetben valamely kockázatkezelési stratégia alkalmazását teszi szükségessé és erős kontrollt, valamint folyamatos ellenőrzést és beszámoltatást igényel.

b) Közepes kockázat (10-16 pont): Tolerálható mértékű kockázat, amely folyamatos kontrollt igényel a Vezetők és az informatikai biztonsági felelős szintjén, és ha szükséges, a kockázati érték csökkentése érdekében a működés során megvalósuló adatbiztonsággal összefüggő technikai és szervezési intézkedéseken túl egyéb intézkedést igényel.

c) Alacsony kockázat (1-9 pont): Elfogadható mértékű kockázat, amely előzetes tervezést, intézkedést nem igényel, incidens bekövetkezés esetén egyedileg szükséges a kezelése.

2.9. A Múzeum által alkalmazott kockázati tűréshatár maximum értéke 16 pont. Az ezt meghaladó kockázati értékű kockázatok nem elfogadható mértékű kockázatoknak minősülnek és – az alábbi pontok szerinti kockázatkezelési stratégiák alkalmazásával – minden esetben intézkedést igényelnek.

2.10. A helyes kockázatkezelési stratégia megválasztása során figyelembe kell venni a Múzeum adott kockázattal szembeni tűrőképességét, amely alapján a Múzeumban 4 kockázatkezelési stratégia alkalmazható: a kockázat elviselése, áthárítása, saját hatáskörben történő kezelése, valamint a kockázatos tevékenység befejezése.

2.11. A kockázat elviselése esetén külön beavatkozásra nem kerül sor, ezért ez kizárólag akkor alkalmazható, ha a kockázat mértéke a Múzeum által alkalmazott kockázati tűréshatáron belül marad és a kockázatot a működési rend (különös tekintettel az informatikai működési rendre) maga kezeli.

2.12. A kockázat áthárítása esetén a Múzeum a kockázatot nem a valószínűség vagy a hatás csökkentésével, hanem a kockázatviselő személyének módosításával kezeli, így különösen biztosítás megkötésével vagy a tevékenység olyan partnernek történő átadásával, aki felkészült a kockázat kezelésére.

2.13. Amennyiben a kockázat nem hárítható át, úgy a Múzeum a kockázatokat saját hatáskörben meghozott szervezeti intézkedésekkel kezeli, amelyek képesek a bekövetkezési valószínűség csökkentésére vagy a kockázatra adott gyors és hatékony reagálást tesznek lehetővé.

2.14. Amennyiben a kockázat értéke egyik kockázatkezelési stratégia (kockázat elviselése, áthárítása vagy saját hatáskörben történő kezelése) révén sem csökkenthető a kockázati tűréshatár maximum értéke alá, úgy a kockázatot az adott tevékenység megszüntetésével is lehet kezelni. Erre azonban a Múzeum esetében (a jogszabályok és az alapító okirat által meghatározott feladatok ellátása körében) csak korlátozott mértékben van lehetőség.

3. Az adatvédelmi incidensek nyilvántartása

3.1. Az adatvédelmi tisztviselő a 2. függelékben foglaltak szerint gondoskodik a tudomására jutott adatkezelési incidensek pontos és naprakész nyilvántartásáról.

3.2. A nyilvántartásnak legalább az alábbiakat kell tartalmaznia:
a) az adatvédelmi incidens körülményei,
b) az adatvédelmi incidens hatásai,
c) az adatvédelmi incidens orvoslására tett intézkedések.

IX. Adatbiztonsági előírások

1. Az adatkezelési műveleteket úgy kell megtervezni és végrehajtani, hogy az adatkezelésre vonatkozó jogszabályok betartásával biztosítani lehessen az érintettek magánszférájának védelmét.

2. Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

3. A Vezetők és az informatikai biztonsági felelős – a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint az érintett jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével – kötelesek megtenni azokat a technikai és szervezési intézkedéseket, amelyek az Infotv., a GDPR, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
Az intézkedéseket úgy kell meghatározni, hogy azok garantálják a kockázat mértékének megfelelő szintű adatbiztonságot, így különösen
a) a személyes adatok álnevesítését és titkosítását;
b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatok-hoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

4. A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

5. A személyes adatok automatizált feldolgozása során biztosítani kell
a) a jogosulatlan adatbevitel megakadályozását;
b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;

c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;
d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;
e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és
f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

6. Az adatok biztonságos őrzésére vonatkozó követelmények tekintetében a jelen szabályzatban foglaltakat és a Múzeum informatikai biztonsági szabályzatában foglaltakat együtt kell értelmezni.

1. számú függelék:

Adatkezelési tevékenységek nyilvántartása (minta)

Adatkezelő neve, elérhetősége:
Adatvédelmi tisztviselő:

Adatkezelés célja	Adatkezelés érintettjei	Kezelt személyes adatok	Adatok címzettjei (akikkel az adatot közlik, vagy közölni fogják)	Adattovábbításra vonatkozó információk	Adat törlésének határideje	Adatbiztonsági intézkedések leírása	Adatkezelés jogalapja	Adatkezelési incidens bekövetkezése esetén annak hatása	Adatkezelési incidens bekövetkezése esetén az incidens kezelésére tett intézkedések	Az érintett hozzáférési jogának érvényesítését korlátozó vagy megtagadó intézkedések

2. számú függelék:

Adatvédelmi incidensek nyilvántartása (minta)

Sorszám	Adatvédelmi incidens bekövetkezésének időpontja	Hatóságnak történő bejelentés időpontja (amennyiben az incidens valószínűsíthetően magas kockázattal jár)	Adatvédelmi incidens jellege, az incidenshez kapcsolódó tények, körülmények	Érintettek köre	Érintettek száma	Érintett személyes adatok	Adatvédelmi incidens hatása (valószínű következményei)	Adatvédelmi incidensből eredő hatások következményeinek enyhítésére tett intézkedések

3 számú függelék

Adatvédelmi incidensek kockázatkezelése (minta)

Sorszám	Adatkezelési főfolyamat	Adatkezelési főfolyamat részeleme	Fő/részfolyamatban rejlő lehetséges adatvédelmi incidens	Valószínűség	Hatás	Kockázati érték	Kockázati szint	Érintett szervezeti egység	Tervezett kockázatkezelési feladat	Felelős	Javasolt műszaki és szervezési intézkedések

4 számú függelék:

Jegyzőkönyv adatvédelmi incidensről[i]

1. **Az incidenssel érintett személyes adatok köre** (személyes adatok[ii], különleges adatok[iii]):

2. **Az adatvédelmi incidens jellege[iv]:**

3. **Az adatvédelmi tisztviselő elérhetősége:**

4. **Az adatvédelmi incidens következményeinek enyhítésére és az érintettek tájékoztatására[v] tett intézkedések:**

5. **Az adatvédelmi incidenssel érintettek *köre* [vi] és száma:**

6. **Az adatvédelmi incidens időpontja (kezdő és záró időpont):**

7. **Az incidensről való tudomásszerzés időpontja, módja:**

8. **Az adatvédelmi incidens bekövetkezésének körülményei és hatása[vii]:**

9. **Az adatvédelmi incidenssel kapcsolatos egyéb adatok:**

Dátum, készítő neve

[i] A lábjegyzetekben található adatok, felsorolások alapja a NAIH által az Incidensbejelentési felületükön elérhetővé tett felhasználói kézikönyvben szereplő formanyomtatvány, és mentett képernyőrovatok.

[ii] Személyazonossághoz kapcsolódó iratok, személyi szám, elérhetőségi adatok, gazdasági / pénzügyi adatok, hivatalos okmányok, helymeghatározó adatok, büntetett előélettel / bűncselekményekkel / büntetéssel / intézkedéssel kapcsolatos adatok;

[iii] Faji eredetre / nemzetiségi tartozásra vonatkozó adatok, politikai véleményre vonatkozó adatok, vallásos vagy más világnézeti meggyőződésre vonatkozó adatok, érdek-képviseleti tagságra vonatkozó adatok, szexuális életre vonatkozó adatok, egészségügyi adatok, genetikai adatok, biometrikus adatok, egyéb adatok.

[iv] Eszköz elvesztése / ellopása, papír alapú dokumentum elvesztése / ellopása / olyan helyen hagyása amely nem minősül biztonságosnak, levél elvesztése vagy jogosulatlan felnyitása, informatikai rendszer feltörése (hackelés), rosszindulatú számítógépes programok (pl. zsarolóprogram), adathalászat, papír alapú dokumentum nem megfelelő módon történő megsemmisítése, elektronikus hulladék nem megfelelő kezelése (a személyes adatok rajta maradnak az elavult eszközön), személyes adatok nagy nyilvánosság előtti jogellenes közzététele, személyes adatok jogosulatlan megismerése, személyes adatok téves címzett részére történő elküldése, személyes adatok jogosulatlan szóbeli közlése, egyéb.

[v] Az érintettek tájékoztatásának / tervezett tájékoztatásának időpontja, tájékoztatott érintettek száma, az érintettek tájékoztatásának formája, az érintetteknek szóló tájékoztatás tartalma; ha a tájékoztatás még nem történt meg, annak okai, alapul szolgáló intézkedések; nyilvánosan közzétett információk.

[vi] Alkalmazott, felhasználó, feliratkozó, diák, katonai állomány tagja, jelenlegi ügyfél / potenciális ügyfél, páciens, kiskorú, kiszolgáltatott személy, hatósági eljárás vagy intézkedés alá vont / azok által érintett személy, egyéb.

[vii] *1 - Bizalmas jelleg sérülése* (szélesebb körű hozzáférés, mint ami szükséges vagy mint amihez az érintett hozzájárult, valamely adat összekapcsolhatóvá vált az érintett egyéb adatával, az adat más célból történő, tisztességtelen módon történő kezelése lehetséges, egyéb); 2 - *Integritás sérülése* (az adat módosíthatóvá vált annak ellenére, hogy archivált elavult adat volt; az adatot valószínűsíthetően módosították egyébként pontos adatokra és azokat eltérő célokra használhatták, egyéb); 3 - *Rendelkezésre állás sérülése* (az érintettek számára kritikus szolgáltatás-nyújtás képességének elvesztése, az érintettek számára történő kritikus szolgáltatás-nyújtás képességének módosulása, egyéb); *4 - Az érintetteket ért fizikai, anyagi, vagy nem vagyoni károk, vagy egyéb jelentős következmények* (az incidens valószínűsíthető hatásai az érintettekre, egyéb valószínűsíthető hatások, a valószínűsíthető következmények súlyossága).