5. sz. melléklet

MARCALI MÚZEUM
H-8700 Marcali, Múzeum köz 2. | +36 85 510 520 | www.marcalimuzeum.hu | info@marcalimuzeum.hu

A MARCALI MÚZEUM ADATVÉDELMI És INFORMATIKAI SZABÁLYZATA

I. ÁLTALÁNOS RÉSZ

1. Bevezetés

1.1 A Marcali Múzeum tevékenysége során személyes, különleges, közérdekű és közérdekből nyilvános adatok kezelését is végzi, ezért az adatkezelésre vonatkozó előírások szabályzatban rögzítése indokolt.
1.2 Jelen adatvédelmi és informatikai szabályzat (a továbbiakban: Szabályzat) rögzíti az adatvédelemre és az informatikai rendszerek és szolgáltatások üzemeltetésére és használatára vonatkozó alapvető szabályait.

2. A Szabályzat célja és hatálya

2.1. A Szabályzat célja
a) meghatározni az intézmény informatikai rendszerei és szolgáltatásai kialakításának, üzemeltetésének, igénybevételének és ellenőrzésének rendjét,
b) biztosítani az intézmény szervezeti tevékenysége során a személyes adatok védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez fűződő, az Alaptörvény 6. cikkének (2) bekezdése szerinti információs önrendelkezési és információszabadságra vonatkozó jog érvényesülését,
c) meghatározni az intézmény által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében, a személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági szabályokat, valamint gondoskodni azok érvényesítéséről.

2.2. A Szabályzat hatálya kiterjed
a) az intézményben folytatott valamennyi informatikai tevékenységre;
b) minden olyan adatkezelésre és adatfeldolgozásra, amely az Infotv. szerinti személyes, különleges, közérdekű, vagy közérdekből nyilvános adatra vonatkozik, függetlenül attól, hogy az adatkezelés, illetve adatfeldolgozás teljesen vagy részben automatizált eszközzel vagy manuális módon történik;
c) a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül;
d) valamennyi, az intézményben, illetve telephelyein biztosított informatikai eszközre és azok műszaki dokumentációjára;
e) az informatikai folyamatokban szereplő összes dokumentációra;
f) a rendszer- és felhasználói alkalmazásokra;

g) az adatok felhasználására vonatkozó utasításokra;
h) az adathordozókra, azok tárolására és felhasználására.

2.3. A Szabályzat személyi hatálya kiterjed minden személyre, aki az intézmény informatikai, vagy azzal összefüggő rendszerét, szolgáltatásait igénybe veszi, informatikai struktúráját és annak eszközeit üzemelteti, vagy használja.
2.4. Az adatvédelmi és adatbiztonsági előírások alkalmazása szempontjából adatkezelő szerv vezetőjének kell tekinteni az igazgatót, szakmai területek tekintetében megjelölt vezetőket.
2.5. Az adatkezelő szerv vezetőjének felelősségi körébe tartozik
a) az SZMSZ szerint irányítása alá tartozó szerv, illetve szervezeti egység adatvédelmi és adatbiztonsági intézményrendszerének kiépítése és működtetése, ennek keretében a szerv, illetve szervezeti egység által — az ellátott ügykörhöz igazodóan — kezelt, védelmet élvező adatok biztonságát biztosító személyi, tárgyi és technikai feltételek biztosítását célzó, hatáskörébe tartozó intézkedések megtétele;
b) az irányítása alá tartozó szerv, illetve szervezeti egység tevékenységének rendszeres adatvédelmi ellenőrzése, az ennek során esetlegesen feltárt hiányosságok, esetleges jogszabálysértő körülmények megszüntetése, a személyi felelősség megállapításához szükséges eljárás kezdeményezése, illetve lefolytatása;

3. Értelmező rendelkezések

A Szabályzat alkalmazása során:
adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas; adatállomány: az informatikai rendszerben logikailag összetartozó, együtt kezelt adatok összessége;
adatátvevő: a személyes adatokat az adattovábbító adatkezelőtől átvevő adatkezelő;
adatátvitel: adatok informatikai rendszerek, rendszerelemek közti továbbítása; adatbiztonság: a személyes adatok jogosulatlan kezelése, így különösen megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni technikai, szervezési megoldások és eljárási szabályok összessége, az adatkezelésnek azon állapota, amelyben a fenyegetettséget jelentő kockázati tényezőket különböző műszaki, szervezési megoldások és intézkedések a lehető legkisebb mértékűre csökkentik;
adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adatokon végzik;
adatkezelés: az alkalmazott eljárástól függetlenül az adatokon 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 adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése; adathordozó: bármely alakban, bármilyen eszköz felhasználásával és bármilyen eljárással előállított, adat tárolására alkalmas, továbbá adatot tartalmazó anyag;
adatvédelem: a személyes adatok kezelésének normatív szabályozása az érintett információs önrendelkezési jogának biztosítása és érvényesítése érdekében;
alkalmazás: a szoftver és minden egyéb olyan számítógépes program, amelyet egy feladat vagy feladatkör végrehajtására terveztek;

authentikáció: az adatcsere során a kommunikációban résztvevő felek identitása megállapításának és ellenőrzésének folyamata; bizalmasság: az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek felhasználásáról; biztonság: a védeni kívánt rendszer olyan, a szervezet számára kielégítő mértékű állapota, amely zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet valósít meg; biztonsági esemény: az informatikai rendszer biztonságában beállt olyan kedvezőtlen változás, melynek hatására az informatikai rendszerben tárolt adatok bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása megsérült, vagy megsérülhet; érintett: bármely meghatározott, személyes adat alapján azonosított, vagy — közvetlenül vagy közvetve — azonosítható természetes személy; fájl: számítógépen tárolt információtárolási egység. Egy fájl tartalma a gép szempontjából vagy adat, vagy program, amely a processzor által végrehajtható utasításokat tartalmaz; felhasználó: meghatározott jogosultságokkal bíró olyan személy, aki az intézmény informatikai rendszerét, hálózatát, szolgáltatásait authentikációt követően igénybe veszi; hálózat: informatikai eszközök közti adatátvitelt megvalósító logikai és fizikai eszközök összessége; hitelesség: az adat olyan tulajdonsága, amely arra vonatkozik, hogy az adatbizonyítottan vagy bizonyíthatóan az elvárt forrásból származik; információs önrendelkezési jog: az Alaptörvény VI. cikkének (2) bekezdésében biztosított, mindenkit megillető, „személyes adatai védelméhez” való jognak azon alapvető tartalma, hogy minden természetes személy maga rendelkezik személyes adatainak feltárásáról és felhasználásáról, információs:ahadság: az Alaptörvény VI. cikkének (2) bekezdésében biztosított „a közérdekű adatok megismeréséhez és terjesztéséhez” való jognak azon alapvető tartalma, hogy mindenkinek joga van az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy tevékenységére vonatkozó, vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső közérdekű, illetve a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez; informatikai eszkö:: jelen Szabályzat tekintetében informatikai eszköz az asztali számítógép, monitor, hordozható számítógép, nyomtató, telekommunikációs eszközök (telefon, mobiltelefon, fax), adathordozók, mobil eszközök, valamint ezek kiegészítői; informatikai szolgáltatás: minden olyan informatikai rendszerhez történő definiált és dokumentált hozzáférési, felhasználási lehetőség, amelyet a rendszer üzemeltetői a felhasználók számára elérhetővé tesznek; közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli; közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétól, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat; különleges adat: a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat; b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint az Infotv. 3. 4. pontja szerinti bűnügyi személyes adat; spam-szűrés: a kéretlen reklámlevelek kiemelése a rendes levélforgalomból; személyes adat: az érintettel kapcsolatba hozható adat — különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret —, valamint az adatból levonható, az érintettre vonatkozó következtetés;

WiFi: a vezeték nélküli helyi hálózat angol elnevezésének rövidítése.

II. ADATVÉDELMI RENDELKEZÉSEK

1. Szervezetre vonatkozó előírások

1.1 Az intézmény igazgatója

a) kiadja az adatvédelmi és informatikai szabályzatot;
b) kiadja a Közérdekű adatok kötelező vagy saját döntésen alapuló elektronikus közzétételének rendjéről szóló szabályzatot;
c) felügyeli az adatvédelmi feladatok ellátását;
d) felelős a közérdekű, és közérdekből nyilvános adatok szolgáltatására vonatkozó kötelezettség teljesítéséért, annak teljességéért és hitelességéért.
e) ellenőrzi az adatvédelemmel kapcsolatos jogszabályok és belső szabályzatok rendelkezéseinek és az adatbiztonsági követelmények érvényesülését;
f) kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót.

1.2 Az adatkezelést végző személy

a) kezeli és megőrzi a feladata ellátása során birtokába került adatokat;
b) ügyel a nyilvántartások biztonságos kezelésére és tárolására;
c) tevékenységi körén belül felelős az adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, továbbá az adatok pontos, követhető dokumentálásáért;
d) gondoskodik arról, hogy az általa vezetett nyilvántartások adataihoz illetéktelen személy ne férhessen hozzá.

2. Az adatkezelés általános szabályai

2.1 A papír alapon kezelt adatokat indokolt esetekben keletkezésükkor megfelelő minőségű adathordozóra kell rögzíteni.

2.2 Az adatok olvashatóságáért az azokat felvevő, illetve rögzítő személy felel. Az adatok jogosulatlan megismerésének megakadályozása érdekében az adathordozókat folyamatos felügyelet alatt kell tartani, vagy el kell zárni.

2.3 Az adatok őrzési, törlési határidejét a jogszabályi előírásoknak megfelelően kell megállapítani, a személyes adatok esetén biztosítani kell a célhoz kötöttség elvének érvényesülését.

3. A személyes adatok kezelésére vonatkozó különös szabályok

3.1. Személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárul, vagy azt valamely jogszabály elrendeli, továbbá ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

3.2. Különleges adat kezelésére kizárólag akkor jogosult az intézmény, ha ahhoz az érintett írásban hozzájárul. Az érintett hozzájárulását vélelmezni kell, ha az adatkezeléssel összefüggő eljárás az érintett kérelmére indul meg. Erre a tényre az érintettet figyelmeztetni kell.

3.3. Az érintett az adatkezelőtől tájékoztatást kérhet személyes adatai kezeléséről, és az adatokba bele is tekinthet. A betekintést úgy kell biztosítani, hogy az érintett más személy adatait ne ismerhesse meg.
3.4. Az érintett kérelmére az adatkezelő tájékoztatást ad az általa kezelt adatairól, az adatkezelés céljáról, jogalapjáról, időtartamáról, továbbá arról, hogy kik és milyen célból kapták meg az adatokat.
3.5. Adatváltozás vagy téves adatrögzítés észlelése esetén az érintett írásban kérheti kezelt adatainak helyesbítését, illetve kijavítását. A téves adatot az adatkezelő 8 munkanapon belül helyesbíteni köteles.
3.6. Olyan adatkezelés esetén, amelynél számolni kell külföldre irányuló adattovábbítással, az érintettek figyelmét erre a körülményre már az adatok felvétele előtt fel kell hívni. Az érintett írásbeli felhatalmazása nélkül személyes adat külföldre nem továbbítható, kivéve, ha ezt törvény lehetővé teszi.
3.7. Az adattovábbítás papír alapon vagy elektronikus úton történhet. Abban az esetben, ha az adattovábbítás elektronikus adatfeldolgozással hatékonyabban teljesíthető, akkor az adattovábbításról az irattár részére kísérőlevelet kell készíteni, amely tartalmazza az adattovábbítást kéró megkeresésében felsorolt adatokat.

4. Közérdekű és közérdekből nyilvános adatok kérelemre történő megismerésének rendje
4.1. Az intézményre vonatkozó közérdekű adatok bárki számára megismerhetőek és hozzáférhetőek az Infotv-ben foglalt kivételekkel. Azon közérdekű adat megismerésére előterjesztett igény, amely adat nyilvánosságát jogszabály korlátozza nem teljesíthető.
4.2. A közérdekű adatok megismerése korlátozható az Infotv-ben foglalt esetekben.
4.3. A közérdekű adat megismerése iránt szóban, írásban vagy elektronikus úton bárki igényt nyújthat be. Az igény tudomásra jutásától számított legfeljebb tizenöt napon belül az igénylésnek — ha jogi akadály nem merül fel eleget kell tenni. Az igényelt adatokat tartalmazó dokumentumról vagy dokumentum részről, annak tárolási módjától függetlenül az igényló másolatot kaphat. A másolat készítéséért — az azzal kapcsolatban felmerült költség mértékéig terjedően — költségtérítés állapítható meg, amelynek összegéről az igénylőt a teljesítését megelózóen az intézmény tájékoztatja.
4.4. Az igény teljesítésének megtagadásáról, annak indokaival, valamint az igénylőt megillető jogorvoslati lehetőségekről való tájékoztatással együtt nyolc napon belül írásban vagy - ha az igényben elektronikus levelezési címét közölte - elektronikus levélben értesíti az intézmény az igénylőt.
4.5. Az adatigényló a közérdekű adatok megismeréséhez fűződő jogok gyakorlásával kapcsolatos jogsértés esetén a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (1024 Budapest, Szilágyi Erzsébet fasor 22/C.) is fordulhat.

5. Kötelezően közzéteendő közérdekű adatokra vonatkozó rendelkezések
Az intézmény a közzététel rendjéről a Közérdekű adatok kötelező vagy saját döntésen alapuló elektronikus közzétételének rendjéről szóló szabályzatban rendelkezik.

III. AZ INFORMATIKAI BIZTONSÁGHOZ KAPCSOLÓDÓ RENDELKEZÉSEK

1. Szervezetre vonatkozó előírások

1.1 az informatikus

a) felelős az intézmény működésével kapcsolatos informatikai üzemeltetési és fejlesztési feladatok ellátásáért;

b) elkészíti és karbantartja az informatikai terület üzemeltetési, informatikai biztonsági és fejlesztési folyamatainak szabályozását.

c) felelős azért, hogy a belépő új munkatársak számára a munkavégzéshez szükséges informatikai eszközök és jogosultságok igénylése határidőben megtörténjen,

2. Az intézmény működése szempontjából kritikus, kiemelt, normál és egyéb rendszerek 2.1. Az intézmény működése szempontjából kritikus az a rendszer, amely az intézmény egészére kiterjed. A kritikus rendszerek adatbiztonsági szempontból kiemelt védelmet igényelnek. E körbe tartoznak különösen az alábbi rendszerek:

a) bér- és munkaügyi rendszer;
b) gazdasági, ügyviteli rendszer;
c) iratkezeléssel összefüggő rendszerek;
d) támogatással, pályáztatással összefüggő rendszerek;
e) EU információs rendszer;
f) központi levelező kiszolgálók;
g) központi tárhelykiszolgálók;

3. Jelszavak

Az intézmény az authentikáció megfelelő működése érdekében a felhasználók számára a különféle hozzáférések biztosításához jelszavakat biztosít.

4. Adatbiztonság, adatkezelés

4.1. Az intézmény informatikai rendszerében adattárolásra az alábbi eszközökön van lehetőség:

a) asztali számítógép vagy hordozható számítógép merevlemeze
b) hordozható adathordozók (CD, DVD, pendrive, stb.)

4.2. Az intézmény informatikai eszközein és hálózati meghajtóin kizárólag a felhasználó munkakörével és munkájával kapcsolatos adatok tárolhatók.

4.3. A felhasználó felel az általa használt informatikai eszközökön tárolt adatok védelméért, így különösen köteles:

a) a bizalmas és belső használatú információkat hordozható eszközökön titkosítva tárolni;
b) tartózkodni a bizalmas és belső használatú információk kódolatlan külső hálózaton történő küldésétől;
c) tartózkodni a jelszavak titkosítás nélküli tárolásától;
d) a mobil eszközök valamennyi biztonsági szolgáltatását használni;
e) az asztali számítógépet és a hordozható számítógépet jelszóval védeni;
f) a felügyelet nélkül hagyott asztali számítógépet és a hordozható számítógépet zárolni.

5. Mentés archiválás

5.1. Az archiválásokat tartalmazó adathordozókon jól láthatóan és azonosíthatóan fel kell tüntetni a mentett rendszer (adatállomány) nevét, a mentés típusát és idejét, melyeket az archiválási nyilvántartásban is fel kell tüntetni.

5.2. Az archiválásokat tartalmazó adathordozókat a hálózati meghajtók és szerverek adatait tartalmazó adathordozókétól elkülönített helyiségben és épületben, zárt helyiségben vagy szekrényben kell órizni.

IV. ZÁRÓ RENDELKEZÉSEK

1. A szervezetünknél dolgozó személyek kötelesek a jelen szabályzat előírásait áttanulmányozni, értelmezni és az azokban foglaltak szerint a tőlük elvárható gondossággal eljárni.

2. Jelen szabályzat 2025. szeptember 03. napján lép hatályba.

Vidák Tünde
igazgató

Marcali Múzeum

Marcali 2025. 09. 02