Magyarországi Németek Általános Művelődési Központja

6500 Baja, Duna utca 33.

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

főigazgató

Hatályos: 2022. június 01-től

Tartalomjegyzék

A Magyarországi Németek Általános Művelődési Központja (székhely: 6500 Baja, Duna u. 33., OM azonosító: 027939) (a továbbiakban: Intézmény) a vonatkozó Európai Uniós (így különösen 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 szóló 2016/679. számú Európai Parlament és Tanács rendelete [továbbiakban: GDPR]), valamint hazai (így különösen az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [továbbiakban: Infotv.], kiemelten annak 25/A.§ (3) bekezdése; továbbá a nemzeti köznevelésről szóló 2011. évi CXC. törvény [továbbiakban: Nkt.] 43. § (1) bekezdése alapján) jogszabályoknak való megfelelés érdekében az Intézmény adatkezeléseire vonatkozó szabályokat az alábbiak szerint határozza meg.

Jelen Szabályzatban, egységes szerkezetbe foglalva az adatbiztonságra vonatkozó előírások is megtalálhatók.

I. Általános rendelkezések

1. A szabályzat célja

1.1. Figyelembe véve, hogy az Intézménynek a szokásos ügymenetében elengedhetetlenül szükséges személyes adatokat gyűjtenie és kezelnie, az Intézmény számára a legfontosabb célkitűzések között szerepel az általa végzett adatkezelési, adatfeldolgozási folyamatok jogszerűségének, átláthatóságának, hitelességének, pontosságának és bizalmi jellegének erősítése, az adatok integritásának megőrzése, illetve az érintettek joggyakorlásának elősegítése (különös tekintettel arra is, hogy az érintettek jelentős része gyermek) tisztességes eljárási keretek kialakításával és fenntartásával.

1.2. Az Intézmény elkötelezte magát amellett, hogy szabályozási, szervezetalakítási és dokumentálási eszközei révén megteremti a zárt, teljes körű, folyamatos és a kockázatokkal arányos adatvédelem jogszerű mechanizmusait, melyek különösen a következők:

a) az Intézményen belüli biztonságtudatos viselkedés előmozdítása;

b) a jogszabályoknak megfelelő eljárásrendek létrehozása, továbbá az eljárásrendeknek megfelelő adatvédelmi gyakorlatok és operatív tevékenységek kialakítása;

c) az átláthatóságot és elszámoltathatóságot biztosító dokumentáció elkészítése;

d) az Intézménnyel jogviszonyban álló dolgozók, gyermekek, tanulók, valamint ezen gyermekek, tanulók szüleinek/törvényes képviselőinek jogait és jogos érdekeit figyelembe vevő ügymenetek kialakítása;

e) a kezelt személyes adatok jogosulatlan felhasználásának megakadályozása;

f) az érintetti jogok biztosítása;

g) az adatvédelmi incidensek megelőzésére vonatkozó intézkedések meghozatala.

2. A szabályzat hatálya

2. A szabályzat hatálya kiterjed:

a) minden, az Intézménnyel munka-, vagy bármely egyéb foglalkoztatásra irányuló jogviszonyban álló személyre, különösen azokra, akik a munkahelyi feladataik ellátása során személyes adatokkal dolgoznak (továbbiakban: dolgozó);

b) az Intézmény teljes feladatellátására, az Intézmény minden adatkezelési folyamatára;

c) az Intézmény teljes szervezetére, minden szervezeti egységére;

d) az Intézményben kezelt minden olyan adatra, amely a GDPR és az Infotv. rendelkezései alapján a személyes adat kategóriájába esik.

3. Értelmező rendelkezések

3. Jelen szabályzat alkalmazásában:

a) adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

b) adatkezelés: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

c) adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

d) adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;

e) adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

f) adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

g) adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

h) álnevesítés: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;

i) címzett: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e; (azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek. Az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak);

j) érintett hozzájárulása: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

k) harmadik fél: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, 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 felhatalmazást kaptak;

l) nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;

m) nyilvántartási rendszer: a személyes adatok bármely módon – centralizált, decentralizált, funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

n) profilalkotás: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használnak;

o) személyes adat: azonosított vagy azonosítható természetes személyre (a jelen Szabályzatban: „érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható. Az Intézmény vonatkozásában adatkezelőnek jellemzően az Intézmény, érintettnek pedig foglalkoztatásra irányuló jogviszony esetén a dolgozót, nevelési-oktatási jogviszony esetén a gyermeket, tanulót, illetve az annak jogait gyakorló törvényes képviselőt (szülő, gyám) kell érteni.

p) személyes adatok különleges kategóriái: a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

4. Az érintettség vizsgálata

4.1. Az Intézmény belső vizsgálata során megállapította, hogy az Intézmény a GDPR hatálya alá tartozik, mivel személyes adatokat részben automatizált módon, illetve nem automatizált módon egy nyilvántartási rendszer részeként kezel, továbbá mint adatkezelő az Unión belül tevékenységi hellyel rendelkezik. Megállapításra került az is, hogy az Intézmény az Infotv. hatálya alatt áll, tekintve, hogy Magyarország területén automatizált eszközökkel és manuális módon folytat adatkezelést természetes személyek adataival kapcsolatban. Erre tekintettel a GDPR és az Infotv. előírásai az Intézmény valamennyi adatkezelési műveletére alkalmazandók, függetlenül azok formájától.

4.2. Az Intézmény kötelezettséget vállal arra, hogy minden egyéb magyarországi kötelező aktussal és jogszabállyal összhangban, azoknak megfelelve, az ágazati különös előírásokat is betartva folytatja az adatkezelési tevékenységét.

5. A szabályzat elsőbbsége

5. Az Intézmény minden belső szabályozó eszköz megalkotásakor figyelemmel van a jelen szabályzat rendelkezéseire. Az Intézmény egyéb belső szabályzóinak és jelen szabályzatnak az összeütközése esetén, azt a jelen szabályzat elsőbbségének kimondásával szükséges feloldani.

6. Az általános felülvizsgálat rendje

6.1. A Szabályzat általános felülvizsgálatára évente egy alkalommal kerül sor, továbbá minden olyan esetben, amikor a szabályozás időpontjában irányadó körülményekben jelentős változás történik. Jelentős változás különösen, ha a jogszabályi háttér, valamint az adatkezelési folyamatok vagy a kezelt adatok köre lényeges mértékben eltér a szabályozáskori állapotától. Szintén jelentős változásként értékelendő, ha az adatkezelési folyamat nem, de az alkalmazott informatikai rendszer vagy a tevékenységi hely fizikai környezete változik meg.

6.2. A fentiektől eltérő feltételek és határidők kerülhetnek megállapításra az egyes eljárásrendekkel és vizsgálatokkal kapcsolatban (különös felülvizsgálatok).

7. Az adatbiztonsági szervezetrendszer

7. Az Intézmény a felelősségi körök egyértelmű kijelölésével és azok betartásával törekszik előmozdítani az adatbiztonságot a szervezeten belül. A jogszabályi megfelelés biztosítása a főigazgató feladata.

8. Az adatvédelmi tisztviselő

8.1. Az Intézmény jogszabályi kötelezettségeinek eleget téve vizsgálatot folytatott le annak érdekében, hogy megbizonyosodjon róla szükséges-e adatvédelmi tisztviselőt kijelölnie.

8.2. A GDPR 37. cikk (1) bekezdés a) pont értelmében közhatalmi szervek, illetve egyéb, közfeladatot ellátó szervek kötelesek az adatvédelmi tisztviselő kijelölésére. Tekintettel arra, hogy az Intézmény főtevékenysége az Nkt. 74. § (1) és (2) bekezdése, a 4. § 14a. pontja alapján köznevelési feladatellátása, köznevelési közfeladatot ellátó szervnek minősül, a GDPR 37.cikk (1) bekezdés a) pontja alapján köteles adatvédelmi tisztviselő kijelölésére.

II. Dolgozókra vonatkozó általános felelősségi szabályok

1. A szabályzat megismerése

9. Az Intézmény vezetése kötelezettséget vállal arra, hogy minden tőle elvárható intézkedést megtesz annak érdekében, hogy a jelen szabályzatot, illetve annak tartalmát az Intézmény dolgozói megismerjék és megértsék az abban foglalt kötelezettségeiket.

2. Általános szabályok

10.1. Valamennyi dolgozó, aki az Intézményben feladata ellátása során a személyes adatokon műveleteket végez, vagy az Intézmény birtokában lévő személyes adatokhoz hozzáféréssel rendelkezik, köteles azokat kizárólag a munkavégzése körében és céljából kezelni, illetve feldolgozni, mely kötelezettség keretében:

a) a munkavégzés során megszerzett személyes adatok vezetői írásos engedély nélkül nem oszthatók meg harmadik személyekkel, illetve nem hozhatók nyilvánosságra;

b) mások személyes adatai nem kezelhetőek önkényesen;

c) az adatok kezelésekor az adatbiztonsági elvárásoknak megfelelő körültekintéssel és elővigyázatossággal kell eljárni. Személyes adatokon csak a vezetői utasításnak megfelelő adatkezelési tevékenységek végezhetők;

d) az Intézményen belüli jogosultsággal nem rendelkező személyekkel sem oszthatók meg a személyes adatok.

10.2. Minden dolgozónak kötelessége rendszeresen felülvizsgálni az általa kezelt adatokat, a szükségtelen és jogellenes adatkezelési műveletek megakadályozása érdekében, így különösen

a) a dolgozók a feladatkörükbe tartozó személyes adatok közül a jogalap, illetve cél nélkül kezelt adatokat törölni kötelesek. Ha az adatok törölhetőségével kapcsolatban kétség merül fel, feltétlenül a főigazgatóhoz kell fordulni;

b) amennyiben felmerül egy adattal kapcsolatban a pontosítás szükségessége – mert az hibás, hiányos vagy aktualitását vesztette – akkor azt haladéktalanul helyesbíteni, vagy ha ez nem lehetséges törölni kell.

10.3. A személyes adatokat a lehető legkevesebb adattároló helyen szükséges tárolni.

10.4. Az Intézmény egyetlen dolgozója sem készíthet vezetői engedély nélkül személyes adatokat tartalmazó nyilvántartást vagy egyéb forrást.

11. Abban az esetben, ha az Intézmény valamely dolgozója adatvédelmi incidens bekövetkezésének lehetőségét észleli, vagy az adatfeldolgozótól adatvédelmi incidensre vonatkozó értesítést kap késedelem nélkül, de legkésőbb a tudomásszerzést követő 12 órán belül köteles azt jelezni a főigazgató felé.

12. Az Intézmény minden dolgozója fegyelmi, kártérítési, szabálysértési és büntetőjogi felelősséggel tartozik a munkavégzése során tudomására jutott személyes adatok jogszerű kezeléséért.

III. Érintetti jogok

1. Előzetes tájékoztatás

13. Az Intézmény kötelezettséget vállal az érintetti jogok tiszteletben tartására és a gyakorlásuk elősegítésére, így az Intézmény tájékoztatja az érintetett arról, hogy folyamatban van-e rá vonatkozó adatkezelés. Amennyiben igen a következő információkhoz biztosít hozzáférést:

a) az adatkezelés célja;

b) személyes adatok kategóriái;

c) címzettek vagy címzettek kategóriái, ha van ilyen;

d) adattárolás tervezett időtartama vagy annak meghatározásának szempontjai;

e) ha az adatok nem az érintettől származnak, a forrásukra vonatkozó minden információ;

f) automatizált döntéshozatal, illetve profilalkotás ténye, módszere és következményei.

2. A hozzáféréshez való jog

14.1. Az Intézmény az adatkezeléssel érintett személyes adatok másolatát ingyenesen az érintett rendelkezésére bocsátja, feltéve, hogy az nem érinti hátrányosan mások jogait és szabadságait.

14.2. Az érintett által ismételten benyújtott, továbbá a nyilvánvalóan megalapozatlan vagy túlzó kérelmekért adminisztratív költségeken alapuló, ésszerű mértékű díj számítható fel.

3. A helyesbítéshez való jog

15.1. Kérésre az Intézmény indokolatlan késedelem nélkül helyesbíti az érintettre vonatkozó pontatlan személyes adatokat.

15.2. Figyelembe véve a célhoz kötöttség elvét, az érintett jogosult arra, hogy kérje a hiányos személyes adatok kiegészítését.

4. A törléshez való jog

16.1. Az érintett jogosult arra, hogy kérésére az Intézmény által kezelt személyes adatait töröljék.

16.2. A törlést a következő körülmények fennállása esetén kötelező végrehajtani:

a) nincs szükség a cél eléréséhez a személyes adatok kezelésére vagy a cél megvalósult;

b) az érintett visszavonja a hozzájárulását az adatkezeléshez és nincs más jogalap;

c) az érintett tiltakozik az adatkezelés ellen és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;

d) az adatok kezelése jogellenesen történik.

5. Az elfeledtetéshez való jog

17. Az elfeledtetéshez való jog értelmében, ha az Intézmény nyilvánosságra hozta az adatot, és azt törölni köteles, akkor észszerűen elvárható lépéseket tesz annak érdekében, hogy tájékoztasson más adatkezelőket a szóban forgó adatok törléséről.

6. Az adatkezelés korlátozásához való jog

18. Az Intézmény az érintett kérésére korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

a) ha az érintett vitatja a kezelt személyes adatok pontosságát, az adatkezelés korlátozható arra az időtartamra, amíg az adatok pontosságának ellenőrzése be nem fejeződik;

b) ha az adatkezelés jogellenesnek bizonyul, de az érintett ellenzi a kezelt személyes adatainak törlését;

c) ha az adatkezelés eredeti céljának eléréséhez már nincs szükség az adatokra, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;

d) ha az érintett tiltakozott az adatkezelés ellen és ennek kivizsgálása még folyamatban van a folyamat időtartamára korlátozható az adatkezelés.

7. Adathordozhatósághoz való jog

19. Amennyiben az adatkezelés jogalapja a GDPR 6. cikk a) vagy b) pontján (hozzájáruláson vagy szerződés teljesítésén) alapul és automatizált módon történik, az érintett jogosult arra, hogy az Intézmény által gyűjtött adatait tagolt, széles körben használt formátumban megkapja. A kapott adatokat jogosult más adatkezelőhöz továbbítani vagy az Intézmény által továbbíttatni.

8. Tiltakozáshoz való jog

20.1. Az érintett jogosult arra, hogy saját helyzetével kapcsolatos okokból bármikor tiltakozzon az olyan adatkezeléssel szemben, amely a GDPR 6. cikk (1) bekezdés e) pontján alapul, azaz a közérdekű feladat ellátásához szükséges. A megalapozott és megfelelő tiltakozás esetén az Intézmény megszünteti az adatkezelést, kivéve, ha arra olyan kényszerítő erejű jogos indokok vagy jogi igények érvényesítése, védelme miatt továbbra is szükség van, amelyek az érintett jogaival szemben elsőbbséget élveznek.

20.2. A tiltakozáshoz való jogról a fenti esetekben külön tájékoztatni kell az érintetett a kapcsolatfelvételkor.

9. Az Intézmény értesítési kötelezettsége

21. Az Intézmény minden címzettet tájékoztat valamennyi helyesbítésről, törlésről vagy korlátozásról, amellyel az érintett személyes adatait közölték, kivéve, ha az lehetetlennek bizonyul vagy aránytalan nehézséggel jár.

IV. Tájékoztatási eljárásrend

1. Előzetes tájékoztatás

22.1. Alapvető elvárás az Intézmény összes adatkezelésével kapcsolatban, hogy az érintettek felé kommunikált tájékoztatásnak tömörnek, átláthatónak és érthetőnek kell lennie, mindezt könnyen hozzáférhető, világos és közérthető formában kell megtenni. Különös figyelmet kell fordítani a szabályzat betartására gyermekeknek címzett bármely információ esetén.

22.2. A tájékoztatás történhet írásban – ideértve az elektronikus utat is – és szóban is, feltéve, hogy az érintett személyazonossága megfelelő módon igazolásra került.

23.1. Amennyiben a személyes adatok közvetlenül az érintettől származnak, a megszerzés időpontjában kell a tájékoztatási kötelezettség teljesítéséhez szükséges információkat az érintett rendelkezésére bocsátani.

23.2. Az érintettől gyűjtött személyes adatokra vonatkozó tájékoztatásnak tartalmaznia kell a következő információkat:
a) az adatkezelő megnevezése és elérhetősége;

b) az adatkezelés célja és jogalapja;

c) a személyes adatok címzettje, illetve címzettek kategóriái, ha van ilyen;

d) adattovábbítás ténye, feltételei és részletei;

e) a személyes adatok tárolásának időtartama vagy annak meghatározásának szempontja;

f) az érintetti jogok felsorolása és magyarázata;

g) a hatósághoz fordulás jogának kiemelése;

h) a személyes adat átadás elmaradásának következményei;

i) az adatkezelési tevékenység során esetlegesen alkalmazott automatizált döntéshozatal, illetve profilalkotás ténye, továbbá az alkalmazott módszer és az érintettre vonatkoztatva, a módszerből adódó következmények leírása;

j) ha az eredeti céltól eltérő célú további adatkezelés van kilátásban.

23.3. Abban az esetben, ha a személyes adatok nem az érintettől származnak:
a) a megszerzéstől számított ésszerű határidőben, de legkésőbb egy hónapon belül;

b) ha a személyes adatok az érintettel való kapcsolattartás céljából kerülnek felhasználásra, legalább a kapcsolatfelvételkor;

c) ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor az érintettet tájékoztatni kell.

23.4. Az érintettől különböző személytől gyűjtött személyes adatokra vonatkozó tájékoztatás többletkövetelményei:

a) a kezelt személyes adatok körének meghatározása;

b) a személyes adatok forrásának meghatározása, és adott esetben arra vonatkozó információ, hogy nyilvánosan hozzáférhető forrásból származnak-e.

V. Adatkezelési kérés- és panaszkezelési eljárásrend

24.1. Az előzetes tájékoztatást követően gondoskodni kell arról, hogy az érintett adatalanyok az elvárt hatékonysággal kapjanak információt és segítséget.

24.2. Az Intézmény oktatással és a munkaköri leírások megfelelő meghatározásával kiemelt figyelmet fordít arra, hogy az érintettek az előzetes tájékoztatás eljárásánál ismertetett módon és formában, az ott felsorolt információkat a kérelmeiknek megfelelően megkapják.

24.3. Az Intézmény az érintettek esetleges panaszait a tájékoztatási eljárásrendnek megfelelően kezeli, illetve szükség szerint meghozza és végrehajtja az érintetti panasznak megfelelő intézkedéseket. Abban az esetben, ha nem kerül sor intézkedések megtételére, az Intézmény késedelem nélkül, de legkésőbb 25 napon belül tájékoztatja erről az érintettet, az elmaradás okainak és a jogorvoslati lehetőségek megjelölésével együtt.

24.4. Az érintetti kérelmekre irányadó válaszadási határidőt, a jogszabályi elvárásoknak megfelelően, az Intézmény 25 napban maximálja. Szükség esetén, ha a kérelmek száma és összetettsége azt indokolja, az említett határidő két hónappal meghosszabbítható.

24.5. Az Intézmény az érintettek kéréseit a formájuktól és a választott kommunikációs csatornától függetlenül befogadja. Így azok érkezhetnek telefonon, elektronikus vagy hagyományos levélben, illetve akár személyesen szóban is. Ha elektronikus úton történt a kérelem benyújtása, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.

24.6. Az Intézmény az érintetti kérésekről és panaszokról naprakész nyilvántartást vezet.

VI. Az adatkezelési és adatfeldolgozási eljárásrend

1. Az Intézmény által kezelt adatok

25.1. Az Intézmény által közfeladata ellátása során kezelt, illetve feldolgozott adatok vonatkozhatnak dolgozóira, az oktatási-nevelési tevékenységgel érintett gyermekekre, tanulókra, azok szüleire, törvényes képviselőire, a fenntartóra, továbbá bármely olyan személyre, akivel az Intézmény közfeladata ellátása során vagy azzal összefüggésben kapcsolatba kerül.

25.2. Az Intézmény által folytatott adatkezelések adatkezelője az Intézmény. Ezen adatkezelési tevékenységek elsősorban az Intézmény saját dolgozóira, az oktatási- nevelési tevékenységgel érintett gyermekekre, tanulókra, azok szüleire, törvényes képviselőire vonatkoznak.

25.3. Az Intézmény adatkezelései ügyviteli, nyilvántartási, ellenőrzési, valamint egyéb céllal történnek,

a) az ügyviteli típusú adatkezelés egy jogviszony (szerződés, megállapodás, jogszabályi kötelezettség) létrejöttéhez, feldolgozásához és lezárásához kapcsolódik, így a meghatározott feladatok ellátásához, a résztvevők azonosításához és az elszámoláshoz szükséges adatokra kell, hogy korlátozódjon. Ennek megfelelően az ilyen adatkezelések esetén személyes adatok, csak a jogviszonyhoz kapcsolódó iratokban, kommunikációban, illetve segédletekben szerepelhetnek,

b) nyilvántartási célú adatkezelés során az egyes adatfajtákból létrejövő adatállományok teszik lehetővé az adatok visszakereshetőségét és azonosíthatóságát. Az ilyen jellegű nyilvántartásoknak mindig az ügyviteli típusú adatkezelésekhez kell igazodniuk,

c) az ellenőrzések lebonyolításához szükséges egy védendő és jogszerű érdek fennállása. Ellenőrzések irányulhatnak közvetlenül az adatalany tevékenységére, de elképzelhető, hogy az ellenőrzés tárgya eltérő, az adatalany annak csak véletlen/járulékos résztvevője,

d) az Intézmény egyéb adatkezelési célokkal is végezhet adatkezelési tevékenységet, ha annak jogszabályi feltételei egyébként fennállnak.

2. Az adatkezelés alapelvei

2.1. Jogszerűség, tisztességes eljárás és átláthatóság elve

26.1. A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. Ezen alapelv szerint az adatkezelés csak abban az esetben tekinthető jogszerűnek, ha az nemcsak az adatvédelmi tárgyú jogszabályoknak, hanem bármely egyéb személyes adatokat érintő normának is megfelel.

26.2. A jogszerű adatkezelés eléréséhez a következőkre kell különösen tekintettel lenni:

a) a személyes adatok védelméhez való jog a természetes személyek alapvető joga, amely biztosítja az érintettek információs önrendelkezési jogát;

b) az információs önrendelkezési jog tiszteletben tartása érdekében az Intézmény személyes adatot csak az alábbi jogalapok megléte esetén kezel:

ba) az érintett előzetes, önkéntes és kifejezett hozzájárulása;

bb) a szerződés teljesítése, a teljesítéshez szükséges mértékben;

bc) amennyiben az adatkezelés az Intézmény által ellátott közfeladat ellátásához szükséges;

bd) az Intézmény vagy harmadik fél jogi kötelezettségének teljesítése;

be) az érintett vagy más természetes személy létfontosságú érdeke.

26.3. Tisztességes az eljárás, ha az az érintetti jogokat magába foglalja és az érintettek jogérvényesítését aktívan (kérések és panaszok kezelése) és passzívan (előzetes tájékoztatás) is elősegíti.

26.4. Átláthatóság alatt mindenekelőtt az érintettek számára egyértelműen meghatározható adatkezelési folyamatok kialakítása értendő, de e mellett az Intézményen belüli gyakorlatok áttekinthetőségét, elhatárolhatóságát és nyomonkövethetőségét is jelenti.

2.2. Célhoz kötöttség elve

27.1. Személyes adatokat csak meghatározott, egyértelmű és jogszerű célból lehet kezelni vagy feldolgozni. Az adatokat az eredeti céllal össze nem egyeztethető módon tilos kezelni.

27.2. Az alapelv megköveteli, hogy személyes adatokat csak az előre meghatározott cél megvalósulásához szükséges mértékben és ideig lehet kezelni. Az Intézmény adatkezeléseinél fontos azt is figyelembe venni, hogy csak olyan adatok kezelhetők, amelyek az adatkezelés megvalósításához elengedhetetlenül szükségesek és a cél elérésére alkalmasak.

2.3. Adattakarékosság elve

28.1. Az adatkezelésnek mindig az említett céloknak megfelelőnek és relevánsnak kell lennie, továbbá szükséges mértékre kell, hogy korlátozódjon.

28.2. Az alapelvnek megfelelően kerülni kell a felesleges, értelmezhetetlen vagy előre meg nem határozott, jövőbeni célhoz kapcsolódó adatok kezelését.

2.4. Pontosság elve

29.1. Az adatokat a kezelésük során pontos és naprakész állapotban kell tartani, minden szükséges intézkedést meg kell tenni annak érdekében, hogy a pontatlan adatokat töröljék vagy helyesbítsék.

29.2. Az alapelv értelmében, ha a kezelt személyes adatok körében pontatlan (hiányos, hibás, sérült) adatok merülnek fel, azokat haladéktalanul pontosítani szükséges. Az érintett kérésének hiányában is az Intézmény a pontatlan adatokat pontosítani törekszik. A pontosítás meghiúsulása esetén, a pontatlan adatokat valamennyi informatikai rendszerből, adattárolóról és irattárból törölni kell.

29.3. Az Intézmény teljes szervezete, így valamennyi dolgozója köteles mindent megtenni annak érdekében, hogy a személyes adatok naprakészek legyenek.

2.5. Korlátozott tárolhatóság elve

30.1.A személyes adatok tárolása csak a cél megvalósításához szükséges ideig megengedett.

30.2. Az alapelvnek megfelelően a személyes adatok kezelésének időben mindig meghatározottnak kell lennie. Semmilyen személyes adat sem kezelhető előre meghatározott időkorlát nélkül, továbbá tilos a készletező adatkezelés. Így minden adatkezelési folyamattal érintett személyes adat tekintetében, meg kell állapítani az előirányzott törlési időt.

2.6. Integritás és bizalmas jelleg elve

31.1. Az adatkezelést oly módon kell végezni, hogy a megfelelő technikai és szervezési intézkedések alkalmazásával az adatok biztonsága adott legyen.

31.2. Az alapelv által megkövetelt adatbiztonságnak ki kell terjednie mind az elektronikus és a papír alapú adatkezelésekre is, továbbá ezeket fizikai, logikai és adminisztratív intézkedésekkel kell védeni.

2.7. Elszámoltathatóság elve

32.1. Az elveknek való megfelelést minden adatkezelési és feldolgozási folyamat tekintetében garantálni kell, továbbá az ennek igazolásához szükséges intézkedéseket is meg kell tenni.

32.2. Az Intézmény az elszámoltathatóság érdekében világosan meghatározza az adatkezelési irányelveit, átlátható tájékoztatási rendszert hoz létre, nyilvántartást vezet az adatkezelésekről és az esetleges érintetti kérésekről, illetve panaszokról, továbbá az adatvédelmi incidensekről.

3. Hozzájárulás szabályai

33.1. Az Intézmény hozzájáruláson alapuló adatkezelései csak akkor lehetnek jogszerűek, ha az érintett egyértelmű megerősítő cselekedettel, például írásbeli – ideértve az elektronikus úton tett – vagy szóbeli nyilatkozattal önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja saját személyes adatai kezeléséhez.

33.2. Hozzájárulással csak az előzetes tájékoztatási kötelezettség teljesítése és az érintett önkéntességének igazolása után kezdhető meg adatkezelés.

33.3. Az önkéntesség nem igazolható, ha az adatkezelés kizárólag az Intézmény érdekeit szolgálja és a hozzájárulást alá-fölérendeltségi viszonyban adták meg az érintettek. Hozzájárulás önkéntességének bizonyítása az Intézmény kötelezettsége, így azok megadásáról az Intézmény nyilvántartást vezet.

33.4. Hozzájárulás bármely olyan formában megadható, amely alapján az érintett azonosítása lehetséges és a hozzájárulás megtörténte rögzíthető.

4. Adatfeldolgozók igénybevétele

34.1. Az Intézmény bizonyos adatkezelési tevékenységek vonatkozásában adatfeldolgozót vehet igénybe. Az adatfeldolgozó az Intézmény megbízásából, annak utasításai szerint az Intézmény számára adatfeldolgozást végez.

34.2. Adatfeldolgozás történhet megállapodás, vagy jogszabályi előírás alapján. A megállapodás alapján történő adatfeldolgozást írásba kell foglalni. A jogszabályi előírás alapján történő adatfeldolgozást nem szükséges írásba foglalni, amennyiben az adatfeldolgozói jogviszonyt jogszabály teljes körűen szabályozza.

34.3. Adatfeldolgozói megállapodás minimális tartalmi követelményei az alábbiak:

a) az Intézmény, mint adatkezelő és az adatfeldolgozó megjelölése;

b) az adatfeldolgozó feladatai;

c) a feldolgozásra átadott személyes adatok típusa, az adatok, valamint az érintettek köre;

d) a szerződés teljesítésére és megszűnésére vonatkozó rendelkezések;

e) a felelősségi kérdések, illetve helytállási kötelezettségek harmadik személy irányába;

f) az adatkezelő utasítási jogköre;

g) az adatfeldolgozó joga további adatfeldolgozók igénybevételére;

h) az adatvédelmi incidensekkel kapcsolatos tájékoztatási kötelezettség;

i) az adatfeldolgozó titoktartási kötelezettsége;

j) az érintetti jogok biztosítására vonatkozó előírások;

k) az adatfeldolgozó adatbiztonsági megfelelőségére vonatkozó nyilatkozata.

5. Adatkezelési nyilvántartás

35.1. Az Intézmény az adatkezelési folyamatokról nyilvántartás vezet, melyben a következő információk kerülnek feltüntetésre:

a) az adatkezelő neve és elérhetősége;

b) az adatkezelés célja;

c) az érintetti kategóriák;

d) a személyes adatok fajtái;

e) a címzettek kategóriái;

f) adattovábbítás harmadik országba vagy nemzetközi szervezethez;

g) az egyes adatkategóriákra előírt törlési határidő;

h) technikai és szervezési intézkedések összegzése.

35.2. A nyilvántartást naprakész állapotban kell tartani.

VII. Az adatközlési eljárásrend

36.1. Adatközlések lehetnek adattovábbítások és adatküldések. Adattovábbítás megvalósulhat harmadik személyhez történő adatközléssel, külföldre történő adatközléssel, harmadik országba történő adatközléssel, vagy nyilvánosságra hozatallal.

36.2. Az Európai Gazdasági Térségen belüli adattovábbítás, így különösen a harmadik személyhez történő, valamint a külföldre történő adatközlés, csak szabályzat által meghatározott valamely jogalap fennállása esetén lehetséges.

36.3. Hozzájáruláson alapuló adatkezelések tekintetében történő adattovábbításra a hozzájárulásnak kifejezetten ki kell terjednie.

36.4. Harmadik országba vagy nemzetközi szervezet részére továbbított adatokra minden esetben a GDPR V. fejezetében található rendelkezéseket kell megfelelően alkalmazni.

36.5. Az adattovábbítás körülményeit a következő pontok szerint kell dokumentálni:

a) az adattovábbítás címzettje;

b) adattovábbítás célja, időpontja, jogalapja;

c) érintett személyek és adatok köre;

d) az adattovábbítás módszere.

37.1. Az Intézmény a gyermek, tanuló Intézmény által nyilvántartott adatai közül

a) a neve, születési helye és ideje, lakóhelye, tartózkodási helye, szülője neve, törvényes képviselője neve, szülője, törvényes képviselője lakóhelye, tartózkodási helye és telefonszáma, jogviszonya kezdete, szünetelésének ideje, megszűnése, egyéni munkarendje, mulasztásainak száma a tartózkodásának megállapítása, a tanítási napon a tanítási órától vagy az iskola által szervezett kötelező foglalkozástól való távolmaradás jogszerűségének ellenőrzése és a tanuló szülőjével, törvényes képviselőjével való kapcsolatfelvétel céljából, a jogviszonya fennállásával, a tankötelezettség teljesítésével összefüggésben a fenntartó, bíróság, rendőrség, ügyészség, települési önkormányzat jegyzője, közigazgatási szerv, nemzetbiztonsági szolgálat részére,

b) óvodai, iskolai felvételével, átvételével kapcsolatos adatai az érintett óvodához, iskolához, felsőoktatási intézménybe történő felvétellel kapcsolatosan az érintett felsőoktatási intézményhez,

c) a neve, születési helye és ideje, lakóhelye, tartózkodási helye, társadalombiztosítási azonosító jele, szülője, törvényes képviselője neve, szülője, törvényes képviselője lakóhelye, tartózkodási helye és telefonszáma, az óvodai, iskolai egészségügyi dokumentáció, a tanuló- és gyermekbalesetre, illetve a tanuló fizikai állapotára és edzettségére vonatkozó adatok az egészségi állapotának megállapítása céljából az egészségügyi, iskola-egészségügyi feladatot ellátó intézménynek,

d) a neve, születési helye és ideje, társadalombiztosítási azonosító jele, lakóhelye, tartózkodási helye, szülője, törvényes képviselője neve, szülője, törvényes képviselője lakóhelye, tartózkodási helye és telefonszáma, a gyermek, tanuló mulasztásával kapcsolatos adatok, a kiemelt figyelmet igénylő gyermekre, tanulóra vonatkozó adatok a veszélyeztetettségének megelőzése, feltárása, megszüntetése céljából a családvédelemmel foglalkozó intézménynek, szervezetnek, gyermek- és ifjúságvédelemmel foglalkozó szervezetnek, intézménynek,

e) az igényjogosultság elbírálásához és igazolásához szükséges adatai az igénybe vehető állami támogatás igénylése céljából a fenntartó részére,

g) az állami vizsgája alapján kiadott bizonyítványainak adatai a bizonyítványokat nyilvántartó szervezetnek a bizonyítványok nyilvántartása céljából, továbbá a nyilvántartó szervezettől a felsőfokú felvételi kérelmeket nyilvántartó szervezethez, továbbítható.

37.2. A gyermek, a tanuló

a) sajátos nevelési igényére, beilleszkedési, tanulási, magatartási nehézségére, tartós gyógykezelésére vonatkozó adatai, továbbá a gyermek, tanuló speciális köznevelési ellátásához elengedhetetlenül szükséges szakorvosi, iskolaorvosi diagnózisának adatai a pedagógiai szakszolgálat, a nevelési-oktatási intézmények és az egészségügyi szakellátó között,

b) óvodai fejlődésével, valamint az iskolába lépéshez szükséges fejlettségével kapcsolatos adatai a szülőnek, a pedagógiai szakszolgálat intézményeinek, az iskolának,

c) magatartása, szorgalma és tudása értékelésével kapcsolatos adatai az érintett osztályon belül, a nevelőtestületen belül, a szülőnek, iskolaváltás esetén az új iskolának, a szakmai ellenőrzés végzőjének,

d) diákigazolványa kiállításához szükséges valamennyi adata az Oktatási Hivatal, a diákigazolvány elkészítésében közreműködők részére továbbítható.

37.3. A dolgozók adatai vonatkozásában a közalkalmazotti alapnyilvántartás szerinti adatok, valamint a pedagógus oktatási azonosító száma, pedagógusigazolványának száma, a jogviszony időtartama, a heti munkaidő mértéke, az óraadó tanárok neve, születési helye, ideje, neme, állampolgársága, nem magyar állampolgárok esetén a tartózkodás jogcíme, a tartózkodásra jogosító okirat megnevezése, száma, lakóhelye, tartózkodási helye, végzettségével, szakképzettségével kapcsolatos adatok, oktatási

azonosító száma a célhoz kötöttség megtartásával továbbíthatók a fenntartónak, a kifizetőhelynek, a bíróságnak, rendőrségnek, ügyészségnek, a köznevelléssel összefüggő igazgatási tevékenységet végző közigazgatási szervnek, a munkavégzésre vonatkozó rendelkezések ellenőrzésére jogosultaknak, a nemzetbiztonsági szolgálatnak. A pedagógusigazolványra jogosultak esetében a pedagógusigazolvány kiállításához szükséges valamennyi adat az Oktatási Hivatal, a pedagógusigazolvány elkészítésében közreműködők részére továbbítható.

37.4. A Szabályzat 37.1-37.2., valamint a 37.3. pontjaiban meghatározott adattovábbítási eseteken kívüli egyéb adattovábbítások esetén, az adattovábbítást megelőzően ki kell kérni az adatvédelmi tisztviselő véleményét. Az adatok továbbítására kizárólag érdemi vizsgálatot követően, akkor van lehetőség, ha a vizsgálat eredményeként annak megállapítására kerül sor, hogy az adattovábbítás az adatvédelmi szabályok betartásával, az érintetti jogok tiszteletben tartása mellett megvalósítható.

38. Adatküldésnek minősül az Intézmény saját szervezetrendszerén belüli adatközlés, az adatok adatfeldolgozó részére történ átadása, valamint az érintett saját személyes adataihoz történő hozzáférése.

VIII. Az adatvédelmi hatásvizsgálat eljárásrendje

39.1. 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, akkor az Intézmény az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetők.

39.2. Az adatvédelmi hatásvizsgálat célja az adatkezelés jellegének feltárása, szükségességének és arányosságának vizsgálata, valamint a személyes adatok kezeléséből eredően a természetes személyek jogait és szabadságait érintő kockázatok kezelésének elősegítése, e kockázatok értékelésével és a kezelésükre szolgáló intézkedések meghatározásával.

39.3. Az adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

a) természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen, jelentős mértékben érintő döntések épülnek;

b) a személyes adatok különleges kategóriáira vonatkozó személyes adatok nagy számban történő kezelése; vagy

c) nyilvános helyek nagymértékű, módszeres megfigyelése.

39.4. A hatásvizsgálat kiterjed legalább:

a) a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az Intézmény közfeladata ellátásához fűződő közérdeket;

b) az adatkezelés céljaira figyelemmel, az adatkezelési műveletek szükségességi és arányossági vizsgálatára;

c) az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és

d) a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

39.5. Az Intézmény szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

39.6. Ha az adatvédelmi hatásvizsgálat azt jelzi, hogy a kockázat mérséklését célzó garanciák, biztonsági intézkedések és mechanizmusok hiányában, az adatkezelés magas kockázattal járna a természetes személyek jogaira és szabadságaira nézve, és a főigazgató véleménye alapján a kockázat nem mérsékelhető a rendelkezésre álló technológiák és a végrehajtási költségek szempontjából észszerű módon, akkor az adatkezelési tevékenység megkezdése előtt a felügyeleti hatósággal konzultálni kell.

IX. Incidenskezelési eljárásrend

40.1. Az Intézmény a természetes személyek jogaira és szabadságaira nézve kockázattal járó adatvédelmi incidenst indokolatlan késedelem nélkül, de lehetőség szerint a tudomásszerzéstől számított hetvenkét órán belül bejelenti az illetékes felügyeleti hatóságnak. Abban az esetben, ha a bejelentés akadályba ütközik, akkor a késedelem okát és minden egyéb fontos információt is meg kell küldeni a hatóságnak.

40.2. Ha bizonyítható, hogy az incidens nem jár kockázattal a természetes személyek jogaira és szabadságaira, akkor el lehet tekinteni a bejelentéstől.

40.3. A bejelentésért a főigazgató a felelős.

40.4. Az incidensről szóló bejelentésben legalább a következőket meg kell jelölni:
a) az incidens jellegét, az érintettek becsült számát és kategóriáit;

b) az érintett adatok becsült számát és kategóriáit;

c) az incidensből eredő valószínűsíthető következményeket;

d) a hátrányos következmények enyhítését célzó már megtett vagy tervezett intézkedéseket;

e) a kapcsolattartó nevét és elérhetőségeit.

40.5. Az Intézmény az adatvédelmi incidensekről nyilvántartást vezet, amiben felsorolja a kapcsolódó tényeket és körülményeket, a következményeket és hatásokat, illetve a megtett intézkedéseket.

40.6. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár, az Intézmény a hatóság mellett, indokolatlan késedelem nélkül értesíti az érintettet is. Az érintett számára a tájékoztatást világosan és közérthetően kell megadni, kitérve legalább az incidens jellegére, a következményekre és a megtett vagy tervezett intézkedésekre, illetve a kapcsolattartó megnevezésére. Ha a tájékoztatás megtétele aránytalan erőfeszítéssel járna, az érintettek nyilvánosan közzétett információkkal vagy hasonlóan hatékony intézkedéssel is tájékoztathatók.

X. Az adatbiztonságra vonatkozó alapvető rendelkezések

1.Az adatbiztonság alapkövetelményei

41.1. Az egyes adatbiztonsági intézkedéseket az Intézmény a kockázatokkal arányos módon, a tudomány és technológia állásának és a megvalósítás költségeinek figyelembevételével, valamint az adatkezelési és feldolgozási folyamatok jellegére, hatókörére és céljaira, továbbá a természetes személyek jogaira és szabadságaira tekintettel határozza meg.

41.2. Az elektronikus információs rendszerekben tárolt és feldolgozott adatok sértetlenségének megőrzése érdekében gondoskodni kell az ügyviteli és üzemeltetési folyamatok és szabályok megfelelő kialakításáról, így különösen:

a) az adatosztályozás során legalább a magas vagy kritikus biztonsági osztályba sorolt adatokat titkosítottan kell tárolni, kezelni és továbbítani;

b) a munkaállomás és a felhasználó folyamatos és egyértelmű azonosítását biztosítani kell;

c) az adatkezelési műveletekre használt informatikai rendszerelemeknek a biztonság elvárt fokának megfelelő módon bizalmasnak és sértetlennek kell lenniük, továbbá a szükséges mértékben rendelkezésre kell állniuk.

41.3. Adattovábbítás esetén, annak biztonságáról az Intézmény és a címzett szervezet között olyan megállapodást kell kötni, amely mindkét fél által támasztott követelményeknek megfelel.

41.4. Biztosítani kell az elektronikus üzenetekben továbbított információk biztonságát és rendelkezésre állását. Ehhez meg kell határozni azokat az eljárásokat, amelyeket az elektronikus üzenetek továbbítása során alkalmaznak.

41.5. A hardver eszközök selejtezése, megsemmisítése, vagy továbbértékesítése előtt a hardver eszköz adathordozóját visszaállíthatatlanul törölni kell.

2. Jogosultságkezelési eljárásrend

42.1. Az Intézmény kiemelten fontosnak tartja, hogy minden felhasználó csak azokhoz az erőforrásokhoz, információkhoz és adatokhoz férjen hozzá, amelyek a munkájához feltétlenül szükségesek.

42.2. A használatban lévő valamennyi informatikai rendszerben tárolt adathoz hozzáférni csak a személyazonosság és a jogosultság ellenőrzésével lehetséges, ezáltal elháríthatók a rendszerekhez való jogosulatlan hozzáférések.

42.3. Hitelesítés és azonosítás nélkül csak az Intézmény honlapjának publikus oldalai használhatók, egyéb felhasználói tevékenység nem végezhető.

42.4. Az egyes alkalmazásokban funkciónkként, illetve egyes adatkörökre vonatkozóan szükséges a hozzáférés korlátozása, illetve a jogosultsággal nem rendelkezők kizárása.

42.5. Az Intézmény egyes felhasználóinak hozzáférési szintje a belépéskor kerül meghatározásra és szükség szerint kell felülvizsgálni. Az Intézmény minden felhasználója csak a munkaköréhez feltétlenül szükséges adatokhoz férhet hozzá.

2.1. Jelszókezelés

43.1. Az Intézmény főszabály szerint nem használ külön fizikai hitelesítési eszközöket az információs rendszereihez való hozzáféréshez, csak a felhasználói név és jelszó párost.

43.2. Az Intézmény jelszókezelési előírásainak célja, hogy a felhasználók titokban tartsák és adott időközönként megváltoztassák a jelszavakat.

43.3. Az Intézmény a megfelelő jelszó használat érdekében, minden dolgozójától elvárja, hogy a jelszavaik a következő követelményeknek megfeleljenek:

a) a jelszavak bizalmasságát és titkosságát megőrizzék, azokat mindenki számára hozzáférhetetlen helyen tárolják;

b) tilos a jelszavakat szervezeten belül és azon kívül is megosztani;

c) a jelszavaknak legalább 8 karakterből kell állniuk, illetve vegyesen kis és nagybetűket, számokat, írásjeleket és lehetőség szerint ékezetes betűket is tartalmazniuk kell;

d) a felhasználói jelszavakat javasolt 6 havonta, de legalább évente meg kell változtatni;

e) tilos a munkahelyi/munkavégzési céllal használt jelszavakat, magáncélú bejelentkezési felületeken is használni;

f) tilos olyan módon meghatározni, hogy az, az adott felhasználóra jellemző legyen.

43.4. A jelszavak kezelésekor a titkosságot a felhasználónak meg kell őriznie, hogy az más tudomására ne juthasson, ennek megfelelően az elektronikus rendszerekbe való belépéskor, illetve a jelszó megváltoztatásakor a jelszavak azonosíthatatlanul kell, hogy megjelenjenek a képernyőn.

43.5. A jelszavakat tartalmazó fájlokat (illetve ezeknek a jelszavakat tartalmazó részét) visszafejthetetlen (egyirányú) kódolással kell tárolni, ezekhez az állományokhoz hozzáférési jogosultságot a főigazgató vagy az általa kijelölt személy kaphat.

43.6. A felhasználók hozzáférési jogait rendszeresen át kell tekinteni, hogy minden felhasználó csakis azokhoz az információkhoz férhessen hozzá, amelyek munkájához aktuálisan szükségesek.

44. Az Intézmény legalább évente egyszer felülvizsgálja a felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, a felelősségüket, továbbá ellenőrzi a Szabályzat vonatkozó rendelkezéseinek a megvalósulását, illetve betartását.

3. Oktatási eljárásrend

45.1. Az Intézmény valamennyi felhasználójának a munkakörének és a biztonsági szintnek megfelelő oktatáson kell részt vennie a szervezet biztonsági szabályairól és eljárásrendjeiről.

45.2. Az ismeretek rendszeres frissítéséről és bővítéséről gondoskodni kell a szervezettől elvárható mértékben.

45.3. Az adatvédelmi oktatásnak legalább a következőkre kell kiterjednie:

a) az adatbiztonsági szint eléréséhez szükséges követelmények ismeretére;

b) a szervezet és felhasználók jogi felelősségére;

c) az elhárító és kárenyhítő intézkedésekre

d) az információs rendszerek helyes használatára;

f) az Intézmény egyéb jogszabályi kötelezettségeire, kiemelten az adatkezelési rendelkezésekre és etikai szabályokra.

45.4. A biztonságtudatossági képzés elvégzését a dolgozónak aláírásával kell igazolnia. A képzés elvégzése az információs rendszer használatának szigorú feltétele, így azt azelőtt kell lefolytatni, hogy a felhasználó hozzáférést kapott volna a rendszerhez vagy a kezelt adatokhoz.

45.5. Az oktatások és képzések megszervezése, ütemezése és tárgyának megválasztása a vezetőség hatáskörébe tartozik. A vezetőség e körben az adatvédelmi tisztviselő bevonását kezdeményezheti.

4. Ellenőrzési eljárásrend

46.1. A Szabályzatban lefektetett eljárásrendek és előírások betartása nélkül a Szabályzat célját lehetetlen érvényesíteni, így ennek érdekében hagyományos vezetési eszközökkel eseti vagy rendszeres ellenőrzések tarthatók, az ellenőrzések során feltárt szabálysértésekért pedig, meg kell, hogy történjen a felelősségre vonás.

46.2. Az ellenőrzés lefolytatásához meg kell határozni az érintett területeket, és az ezekhez tartozó célkitűzéseket. A célkitűzéseknek megfelelően kell kijelölni az ellenőrzés eszközeit és tartalmi követelményeit. Az ellenőrzés eredményének értékelésével levonhatók a megfelelő következtetések az adatbiztonságra vonatkozóan.

46.3. Az Intézmény nem vesz igénybe a felhasználók megfigyelésére és ellenőrzésére, külön erre a célra fejlesztett célszoftvereket.

46.4. Az ellenőrzés során feltárt mulasztásos vagy tevőleges szabálysértések esetén fegyelmi eljárást jelen Szabályzat Adatvédelmi fegyelmi eljárásra vonatkozó rendelkezései szerint kell indítani.

46.5. Az Intézmény ellenőrzései során a következő területekre fektet nagy hangsúlyt:

a) a szervezet megfelel-e a jogszabályok által megkövetelt személyi, tárgyi és eljárási feltételeknek;

b) az informatikai biztonsági szint megfelel-e a kezelt személyes adatok által megkívánt adatbiztonsági elvárásoknak;

c) a Szabályzat rendelkezéseit az érintett dolgozók megfelelően ismerik és betartják-e azokat.

4.1. Az asztali munkaállomások, mobil eszközök ellenőrzése

47. Az Intézmény által a dolgozói részére munkavégzés céljából rendelkezésre bocsátott számítógépet, laptopot a dolgozó kizárólag munkaköri feladata ellátására használhatja. A magáncélú használatot az Intézmény megtiltja, ezen eszközökön a dolgozó semmilyen személyes adatot, magáncélú levelezést nem kezelhet és nem tárolhat. A munkáltató ezen eszközökön tárolt adatokat ellenőrizheti. A tényleges magánhasználat ellenőrzése céljából adatgyűjtésre kizárólag a dolgozó jelenlétében, illetve tájékoztatása mellett – személyiségi jogaira és az adatvédelemi előírásokra tekintettel – a nyilvánvalóan visszaélésszerű magánhasználat esetén van csak lehetőség.

5. Adatvédelmi fegyelmi eljárás

48.1. A Szabályzat előírásainak súlyos megsértésének minősül és fegyelmi eljárás folytatható le különösen a következő esetekben:

a) valamely rendszer hozzáférési adatainak illetéktelen személynek történő tudomására hozatalakor;

b) szabálysértés következtében személyes adatok illetéktelen személy birtokába kerülnek;

c) szabálysértés következtében személyes adatok elvesznek, megsemmisülnek, vagy bármely más módon nem tudnak megfelelni a rendelkezésre állási követelményeknek;

d) személyes adatok szándékos meghamisítása esetén;

e) szabálysértés következtében az Intézmény biztonsági rendszerének megoldásai illetéktelen számára megismerhetővé válnak;

f) a Szabályzat rendelkezéseinek ismételt szándékos vagy többszöri gondatlan megsértése esetén.

48.2. A fegyelmi eljárás megindításáért a főigazgató a felelős, lefolytatására az Intézménynél hatályban levő egyéb fegyelmi ügyekre vonatkozó szabályokat kell alkalmazni.

XI. Biztonsági intézkedések katalógusa

49. Az Intézmény összhangban a Szabályzat alapelveivel és szellemiségével törekszik a normatív szabályozáson túl a gyakorlatban megvalósítani az adatbiztonsági előírásokat. Ennek érdekében érthető és jól körülhatárolt munkahelyi magatartási szabályokat alkot, továbbá egyéb kötelező biztonsági intézkedésekről gondoskodik, amelyek a Szabályzat általános elvárásait ültetik át az Intézmény ügymenetébe. Az Intézmény folyamatosan gondoskodik a felhasználói tudatosságának növeléséről oktatások és képzések szervezésével, abból a célból, hogy tudatában legyenek a biztonsági fenyegetéseknek és elkötelezettek legyenek a Szabályzat előírásainak betartására.

1. Papír alapú adatkezelésekre vonatkozó szabályok

50.1. A papír alapon tárolt adatokat biztonságos, illetve jogosulatlanok számára hozzáférhetetlen helyen kell tárolni. A használatban lévő iratokhoz csak az arra jogosult dolgozók férhetnek hozzá.

50.2. Ha az elektronikus úton felvett adatokat a belső szabályok és gyakorlatok szerint nyomtatni szükséges, azokat legalább elkülönített és lehetőleg elzárt irattárolóban kell tárolni. Az Intézmény dolgozói kötelesek arról gondoskodni, hogy az ilyen iratokhoz illetéktelenek ne férhessenek hozzá. A kinyomtatás okának megszűntével a papír alapú iratokat haladéktalanul meg kell semmisíteni.

50.3. Az irattárba való iratokat zárható száraz, az állaguk megóvására alkalmas helyiségben kell tárolni, a tűz és vagyonvédelem biztosítása érdekében.

2. Elektronikus adatkezelésre vonatkozó szabályok

51.1. Az információs rendszerekben úgy kell tárolni az adatokat, hogy megfelelő védelmet tudjon biztosítani a jogosulatlan hozzáféréstől, szándékos és véletlen törléstől, illetve külső támadásokkal szemben. Külső támadások vonatkozásában különösen védelmet kell nyújtani a kémprogramokkal, vírusokkal és rendszerfeltörésekkel szemben.

51.2. A hozzáférés és hitelesítés érdekében a munkaállomásokat jelszavas beléptetéssel kell ellátni, továbbá a védendő adatokat erős jelszavakkal kell védeni.

51.3. A dolgozók a munkaállomás ideiglenes elhagyása esetén kötelesek a munkaállomást képernyőzárral védeni, amelyet úgy kell beállítani, hogy a munkamenet folytatásakor ismételten hitelesítse a dolgozót.

51.4. Amennyiben személyes adatok tárolására mobil eszközök kerülnek felhasználásra, azokat biztonságos helyen, illetéktelen személyektől elzártan kell tárolni. A személyes adatokat tároló mobil eszközöket, csak a főigazgató engedélyével és utasításainak megfelelően lehet az Intézmény területéről kivinni.

51.5. Az adatokat csak a vezető által meghatározott hardver egységeken lehet tárolni.

51.6. Felhő alapú tárolás esetén előzetesen meg kell győződni arról, hogy a külső tárhelyszolgáltató megfelel-e, az Intézmény által megkövetelt adatvédelmi jogi és technikai követelményeknek.

51.7. Az adattárolásra szolgáló munkaállomásokat folyamatosan vírusirtó szoftverrel és tűzfallal kell védeni.

51.8. Az Intézmény belső hálózatára kapcsolt információs rendszerekre tilos ellenőrizetlen szoftvereket letölteni és telepíteni.

51.9. Személyes adatokat csak olyan levelezőrendszer használatával szabad küldeni, amelynek biztonsága és zártsága igazolt a szolgáltató által.

2.1. Számítógép használati elvek

52.1. A felhasználók kötelesek arra, hogy csak az általuk, adott pillanatban ténylegesen használt papír alapú dokumentumokat és adatokat tartsák az asztalon, illetve jelenítsék meg a képernyőn. Kötelesek továbbá arra is, hogy a munkavégzés felfüggesztésekor vagy annak befejeztével a dokumentumokat és adatokat ne hagyják hozzáférhető helyen (clean desk policy).

52.2. A felhasználók kötelesek meggyőződni arról, hogy a munkavégzésük alatt jogosulatlanok nem nyernek betekintést a kezelt személyes adatokba vagy egyéb szenzitív információkba.

52.3. Külső támadások esetén különösen védelmet kell nyújtani a kémprogramokkal, vírusokkal és rendszerfeltörésekkel szemben.

52.4. Amennyiben személyes adatok tárolására mobil eszközök kerülnek felhasználásra, azokat biztonságos helyen, illetéktelen személyektől elzártan kell tárolni.

2.2. Fizikai védelem

53.1. A felhasználóknak tilos a munkaállomás hardver konfigurációját megváltoztatni, a hardver eszköz belsejébe bármilyen okból belenyúlni, burkolatukat megbontani, továbbá a külső perifériák csatlakozását megszüntetni.

53.2. Az Intézmény nyomtatóit úgy kell elhelyezni, hogy a kinyomtatott anyagok illetéktelen kezekbe ne kerülhessenek.

2.3. Szoftveres védelem

54.1. A felhasználóknak tilos bármilyen szoftvert előzetes jóváhagyás nélkül telepíteni a munkaállomásokra. A szoftver igényeket a főigazgató felé kell jelezni.

54.2. A munkaállomások operációs rendszereit úgy kell beállítani, hogy ha öt percen túl a rendszer használaton kívül van, az automatikusan lezárja a munkaállomást. Így a munka újbóli megkezdésekor a felhasználó a felhasználónév és jelszó páros megadásával ismét azonosíthatja magát.

54.3. A dolgozók továbbá kötelesek arra, hogy az általuk őrizetlenül hagyott berendezéseket, mobil eszközöket és alkalmazásokat saját maguk zárják le.

2.4. Távoli elérés

55.1. Távoli hozzáférés és munkavégzés csak indokolt esetben engedélyezhető, továbbá kizárólag akkor, ha a munkavégzés biztonsága legalább az Intézmény által elvárt szintet képes elérni.

55.2. A mobil eszközök használatakor ellenőrizni kell az eszközökhöz való hozzáférést, azok logikai és fizikai védelmét, az adatmentések megvalósulását és a biztonságos környezeten kívüli munkavégzés körülményeit.

55.3. A külső összeköttetések csak a Home Office típusú munkavégzés munkáltatói elrendelése esetén, valamint munkaidőn kívül feltétlenül szükségesen elérni kívánt rendszerekhez engedélyezettek.

55.4. A mobil eszközök szállítása során biztosítani kell, hogy az eszköz ne legyen kitéve erős rázásnak vagy ütésnek. A mobil eszközt tilos felügyelet nélkül hagyni.

55.5. A hordozható eszközökön külön engedéllyel tárolt személyes adatok és szenzitív információk védelmére hardveres és/vagy szoftveres titkosító eszközök használata szükséges. Ilyen esetben a titkosító kulcsokat külön eszközön kell tárolni.

55.6. A külső rendszerből a belső hálózatra kapcsolódni elsősorban titkosított Virtuális Magán Hálózati (VPN) kapcsolattal, vagy legalább *https* protokollú titkosított csatornán lehetséges.

2.6. Internethasználat

56.1. Tekintve, hogy az Intézmény ügymenete, feladatellátása szempontjából elengedhetetlen az internetkapcsolat a felhasználóknak a következő előírásokat kell követniük a munkájuk során:

a) tilos az internetet jogellenes célokra használni, illetve mások személyiségi jogait megsérteni;

b) tilos mások szerzői jogait megsérteni vagy tiltott haszonszerzésre irányuló tevékenységet folytatni;

c) tilos szoftvereket szándékosan jogellenes módon terjeszteni;

d) tilos másokat sértő módon használni az internetet;

e) tilos mások vallási, etnikai, politikai vagy egyéb érzékenységét sérteni;

f) tilos másokat zaklató tevékenységet folytatni;

g) tilos a szervezet tevékenységi körén kívül eső haszonszerzésre irányuló direkt üzleti tevékenység és reklámok terjesztése;

h) tilos a hálózatot nagymértékben és indokolatlanul megzavaró vagy veszélyeztető tevékenység;

i) tilos a hálózatot és erőforrásait szándékosan túlzott mértékben igénybe venni;

j) tilos az interneten a beszállítókat és szolgáltatókat, illetve azok termékeit vagy szolgáltatásait minősíteni;

k) tilos az Intézmény által képviselt értékek szerint méltatlan oldalak keresése vagy látogatása;

l) tilos olyan adatot, információt vagy szoftvert le vagy feltölteni, amely összeférhetetlen a Szabályzat előírásaival;

m) tilos az internetről ingyenesen letölthető szoftverek munkaállomásokra történő letöltése és telepítése;

n) internetezés közben el kell utasítani azokat a felbukkanó párbeszéd ablakokat, amelyek segédprogramok telepítésére, vagy egyes funkciók kikapcsolására ösztönöznek.

56.2. Az Intézmény fenntartja a jogot arra, hogy a felhasználók számára bármely weboldal látogatását a jövőben megtiltsa, vagy a böngészési tevékenységet olyan módon korlátozza, hogy taxatívan felsorolja, melyek azok az oldalak, amelyek látogathatók.

2.7. Elektronikus levelezés

57.1. A munkahelyi levelezés során kezelt minden postafiókkal kapcsolatban be kell tartani a Szabályzatot és a jogszabályok vonatkozó rendelkezéseit. Ennek elmaradása esetén munkajogi vagy egyéb szankció alkalmazandó.

57.2. Az Intézmény a hálózaton történő elektronikus levelezésére a felhasználók csak saját elektronikus levelezési címüket használhatják. A felhasználók postafiókjaikat minden körülmények között csak munkavégzésre használhatják.

57.3. A szervezet levelezőrendszerének megosztott postafiókjához a hozzáférés előre meghatározott jogosultság alapján történik.

57.4. Levelezéssel kapcsolatos különös tiltások:

a) tilos a közízlést, az Intézmény jó hírnevét veszélyeztető, erkölcstelen vagy politikai tartalmú e-mail küldése;

b) tilos a levelezőrendszert személyes adatok, egyéb szenzitív információk vagy dokumentumok kijuttatására használni;

c) tilos az Intézmény hivatalos ügyeit a nem munkavégzésre rendelt levélcímen intézni;

d) tilos feliratkozni nem szakmai jellegű hírlevél szolgáltatásra;

e) tilos olyan üzenetekre válaszolni, amely az Intézmény rendszeréről, a felhasználó hozzáférési adatairól vagy más védettnek minősített információról kér tájékoztatást;

f) tilos személyes adatokat tartalmazó dokumentumokat vagy adatbázisokat titkosítás nélkül továbbítani.

2.8. Közösségi média

58.1. A közösségi média használata nem válhat a munkavégzéssel kapcsolatos követelmények teljesítésének hátrányára.

58.2 A dolgozóknak tilos a közösségi média felületein olyan tartalom közzététele, amely alkalmas lehet az Intézmény jóhírnevének, jogos gazdasági érdekének veszélyeztetésére.

58.3. Tilos a közösségi médiát oly módon használni, ami mások zaklatására, félelemkeltésre, rágalmazásra vagy becsületsértésre alkalmas.

58.4. Tilos a közösségi médiában üzleti titoknak vagy bizalmasnak minősített információkat megosztani.

59.1. Amennyiben az adott közösségi médiaplatformon létrehozott intézményi csoport/oldal adminisztrátora, tagja az Intézmény valamely dolgozója, az a GDPR hatálya alá tartozik, azzal

kapcsolatban az Intézmény adatkezelői felelőssége fennáll. Ennek tudatában az Intézmény dolgozói csak azon intézményi csoportokba léphetnek be, olyan intézményi oldalak létrehozásában működhetnek közre, melyek az Intézmény hivatalos közösségi oldalának/csoportjának minősülnek.

59.2. Hivatalos közösségi oldalt/csoportot kizárólag az Intézmény szervezeti egység vezetői, vagy az általuk kijelölt személyek (így különösen osztályfőnökök) hozhatnak létre. Az Intézmény hivatalos közösségi oldalai/csoportjai létrehozásához a főigazgató jóváhagyása szükséges. Az Intézmény hivatalos közösségi oldalai/csoportjai működésének/működtetésének célja az Intézmény köznevelési közfeladata ellátásának bemutatása, az Intézmény, a nemzetiségi kultúra népszerűsítése, a közösségi élet pillanatainak bemutatása, a közérdekű információk megosztása, a tájékoztatás, a véleménynyilvánítás szabadságának érvényesítése.

59.3. A hivatalos közösségi oldal működése/működtetése céljának megfelelően az Intézmény hivatalos közösségi oldalain/csoportjaiban közzé tett tartalmakért az azokat létrehozó személyek a felelősek. Az Intézmény hivatalos közösségi oldalait/csoportjait létrehozó személyek kötelesek figyelemmel kísérni az oldalak/csoportok működését és az ott megosztott tartalmakat. Az Intézmény dolgozói által megosztott tartalmak tekintetében kiemelt figyelmet szükséges fordítani az adatvédelmi szabályok betartására. Az Intézmény a közösségi oldalai/csoportjai tekintetében felhasználói szabályzatot alkot, melyben rögzíti azokat a magatartás szabályokat, amelyeket elvár az oldal/csoport felhasználóitól és amelyeken keresztül az emberi méltóság tiszteletben tartása biztosított. Az Intézmény közösségi oldalai/csoportjai létrehozói felelnek a felhasználói szabályzatban foglalt rendelkezések betartatásáért.

59.4. Az Intézmény által működtetett hivatalos közösségi oldalak és csoportok működtetésének nem célja az Intézmény hivatalos kommunikációjának biztosítása. Ezeken a platformokon kizárólag közérdekű/személytelen információk oszthatóak meg (pl. esemény helyszíne, kezdetének időpontja, eseményről készült fényképek stb.), így az ügyintézést igénylő kérdésekben az Intézmény által dolgozói számára biztosított elektronikus levelezőszolgáltatás/levelezőláda (pl. dolgozovneve@mnamk.hu) használatos.

XII. Záró rendelkezés

60.1. Jelen szabályzat 2022. június 1. napján lép hatályba.

60.2. Jelen szabályzat hatályba lépésével a 2018. május 25. napjától hatályos „Magyarországi Németek Általános Művelődési Központja Adatvédelmi szabályzata" hatályát veszti.

Baja, 2022. június 1.

Magyarországi Németek Általános Művelődési Központja Ungarndeutsches Bildungszentrum H-6500 Baja, Duna u. 33. Pf. 58.

.....

Szauter Terézia, főigazgató
Magyarországi Németek Általános
Művelődési Központja

Záradék:

1. Jelen szabályzatot az Nkt. 43. § (1) bekezdése alapján a szülői szervezet véleményezte.

Baja, 2022. 05. 30.

.....

Gaugesz Éva
intézményi szülői szervezet elnöke
Magyarországi Németek Általános
Művelődési Központja

2. Jelen szabályzatot az Nkt. 43. § (1) bekezdés alapján az iskolai diákönkormányzat véleményezte.

Baja, 2022. 05. 30.

.....

Piricsi Richárd
iskolai diákönkormányzat elnöke
Magyarországi Németek Általános
Művelődési Központja

3. Jelen szabályzatot az Nkt. 43. § (1) bekezdés alapján a kollégiumi diákönkormányzat véleményezte.

Baja, 2022. 05. 30.

Francia Fábián
.....

Francia Fábián
kollégiumi diákönkormányzat elnöke
Magyarországi Németek Általános
Művelődési Központja