

Nagycserkeszi Nyitnikék Óvoda és Konyha

Nagycserkesz
Vasvári Pál u. 101.
4445

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

hatályos: 2019. június 1.

Jóváhagyta:

Széchy Erzsébet
intézményvezető

I. BEVEZETŐ RENDELKEZÉSEK

A **Nagycserkeszi Nyitnikék Óvoda és Konyha** (továbbiakban: Intézmény) a feladatellátása során, az alaptevékenysége körében elengedhetetlenül szükséges személyes adatokat gyűjteni és kezelni. A begyűjtött adatok vonatkozhatnak a dolgozókra, az óvodás gyerekekre (azok gondviselőire), együttműködő partnerekre (vevők/szállítók képviselőire, kapcsolattartóira), és egyéb olyan személyekre, akikkel az alaptevékenység folytatása során kapcsolatba kerül.

Jelen rendelkezéseket az Intézmény többi szabályzatának előírásaival összhangban kell értelmezni. Amennyiben a személyes adatok védelmével kapcsolatosan ellentmondás áll fent jelen rendelkezések és a bármely más, jelen szabályzat hatálybalépése előtt hatályba lépett szabályzat előírásai között, úgy abban az esetben jelen rendelkezések az irányadók.

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 25/A. § (3) és a 30. § (6) bekezdésében kapott felhatalmazás alapján az intézményvezető a belső adatkezelési folyamatainak nyilvántartása és az érintettek jogainak biztosítása céljából az alábbi Adatvédelmi és Adatbiztonsági Szabályzatot adja ki:

Általános rendelkezések

Az Intézmény a tevékenységével összefüggésben felmerülő személyes adatok kezelésével járó folyamatai, eljárásai során biztosítja a személyes adatok védelmének megfelelő szintjét az Európai Parlament és a Tanács, 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 rendelete szerint (a továbbiakban: GDPR).

Az adatkezelési műveleteket az Intézmény úgy tervezi meg és hajtja végre, hogy az érintettek személyes védelme megfelelő módon biztosított legyen. Megteszi azokat a technikai és szervezési intézkedéseket, és kialakítja azokat az eljárási szabályokat, amelyek az adatbiztonság érvényre juttatásához szükségesek.

Az adatokat védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés, sérülés, az adatok károsodása és véletlen elvesztése, továbbá az esetleges technikai hozzáférhetetlenné válása ellen.

Vonatkozó jogszabályok

Info tv.	az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
Kjt.	a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény, a közfoglalkoztatásról és a közfoglalkoztatáshoz kapcsolódó, valamint egyéb törvények módosításáról szóló 2011. évi CVI. törvény
Mt.	a munka törvénykönyvéről szóló 2012. évi I. törvény
Mvt.	a munkavédelemről szóló 1993. évi XCIII. törvény
Sztv.	a számvitelről szóló 2000. évi C. törvény
Áht.	az államháztartásról szóló 2011. évi CXCV. törvény
GDPR	az Európai Parlament és a Tanács (EU) 2016/679 rendelete
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság

A szabályzat célja

Az Adatvédelmi és adatbiztonsági szabályzat (továbbiakban adatvédelmi szabályzat) célja az, hogy biztosítsa az Intézmény tevékenysége során a személyes adatok védelméhez fűződő jogok érvényesülését, továbbá, hogy a kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes és különleges adatok kezelése során irányadó adatvédelmi és adatbiztonsági szabályokat.

Továbbá az adminisztráció és ügyintézés során az érintettek személyes adatainak védelmét biztosítsa.

A jelen adatvédelmi szabályzatban rögzítésre kerülnek az Intézmény adatvédelmi elvei. A jelen szabályzat az adatvédelmi szabályoknak való megfelelést szolgálja.

Az Európai Parlament és Tanács (EU) 2016/679 Rendeletének (GDPR) megfelelően az Adatvédelmi és adatbiztonsági szabályzaton túl az alábbi belső szabályozók kerültek kialakításra a Hivatalnál:

- Adatvédelmi incidens kezelési szabályzat
- Adatvédelmi tisztviselő kijelölésének szükségességét mérlegelő dokumentum
- Nyilvántartások vezetésének szabályai (feladatok, felelősök)
- Nyilvántartások adatkezelésről
- Adatkezelési tájékoztatók
- Adatvédelmi hatásvizsgálat elvégzésének szükségességét mérlegelő dokumentum
- Érdedmérlegelési teszt szempontjainak meghatározása
- Informatikai Biztonsági Szabályzat

A személyes adatok védelméhez fűződő jogok érvényesülése, továbbá az Intézmény által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében az alábbi iratmintákat alkalmazzák:

- Adatkezelési tájékoztató
- közalkalmazottak, ellátottak tájékoztatása a személyes adatok kezeléséről
- Érintett hozzájáruló nyilatkozata

- közalkalmazottak/közfoglalkoztatottak/ellátottak hozzájárulása a foglalkoztatási jogviszonnyal nem kötelezően összefüggő adatkezeléshez
- Egyéb szervezeti sajátosságnak megfelelően kialakított dokumentumok.

A jelen adatvédelmi szabályzat biztosítja, hogy az Intézmény

- megfelel az adatvédelmi jogi követelményeknek, és megfelelő adatvédelmi gyakorlatot és operatív tevékenységet folytat
- védi és figyelembe veszi a munkavállalók, egyéb alkalmazottak, együttműködő partnerek és szállítók, valamint az ellátottak jogait és jogos érdekeit,
- nyilvánvalóvá teszi az egyes adatkezelési műveleteket (gyűjtés, őrzés, tárolás, törlés, továbbítás)
- szabályozza az adatvédelmi incidens megelőzésére vonatkozó teendőket
- szabályozza a teendőket adatvédelmi incidens esetére.

A Szabályzat célja továbbá az Intézmény kezelésében lévő közérdekű adatok, vagy közérdekből nyilvános adatok hozzáférhetőségének biztosítása.

Értelmező rendelkezések

A jelen szabályzat alkalmazásában:

1. **„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;
2. **„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;
3. **„az adatkezelés korlátozása”**: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;
4. **„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 helyzetéhez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előre jelzésére használják;
6. **„álnevesítés”**: a személyes adatok 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 személyzet ne lehessen kapcsolni;

7. **„adattörlés”**: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
8. **„adatmegsemmisítés”**: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;
9. **„nyilvántartási rendszer”**: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;
7. **„adatkezelő”**: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;
8. **„adatfeldolgozó”**: az a természetes vagy jogi személy, illetve 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;
9. **„címezett”**: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz.
10. **„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;
11. **„érintett”**: bármely információ alapján azonosított vagy azonosítható természetes személy;
12. **„azonosítható természetes személy”**: az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy egy, vagy több tényező alapján azonosítható;
13. **„személyes adat”**: az érintettre vonatkozó bármely információ
14. **„különleges adat”**: a személyes adatok különleges kategóriába 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;
12. **„az érintett hozzájárulása”**: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez;
13. **„adatvédelmi incidens”**: az adatbiztonság olyan sérülése, 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;
14. **adatbiztonság**: a személyes adatok jogosulatlan kezelése, így különösen megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások és eljárási szabályok összessége; az adatkezelésnek az az állapota,

amelyben a kockázati tényezőket – és ezzel a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a legkisebb mértékűre csökkentik;

14. **hardver eszköz:** valamennyi olyan eszköz, amelynek feladata az informatikai rendszer folyamatos működésének biztosítása, vagy amely biztonsági adatmentésre, avagy másolatok készítésére szolgál, valamint amely elektronikus vagy egyéb módon a számítógép külső behatás elleni védelmét szolgálja;
15. **hírközlő eszköz:** bármilyen technikai eszköz, technológiai eljárás, amely egy vagy több fogadó személy számára jelzések, adatok és információk továbbítására vagy fogadására alkalmas.
16. **információs önrendelkezési jog:** az Alaptörvény VI. cikkében biztosított személyes adatok védelméhez való jognak az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról.

Az adatvédelem jogi háttere

Az adatvédelemre vonatkozó alapvető szabályokat az Európai Parlament és Tanács (EU) 2016/679 Rendelete (2016. április 27.) szabályozza, mely 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 szól (általános adatvédelmi rendelet, a jelen szabályzatban a továbbiakban: GDPR).

GDPR Alapelvek

- **Célhoz kötöttség elve:** meghatározott, egyértelmű és jogszerű célból történhet a személyes adatok gyűjtése
- **Jogszerűség, tisztességes eljárás és átláthatóság elve**
- **Arányosság, szükségesség vagy adattakarékosság elve:** kizárólag az adatkezelés célja érdekében szükséges adatokra kell korlátozódnia
- **Pontosság elve:** a pontatlan személyes adatokat helyesbíteni, a téves adatokat törölni kell
- **Korlátozott tárolhatóság elve:** a cél megvalósulásáig szükséges az adatok tárolása
- **Integritás és bizalmasság elve:** intézkedni kell, hogy jogosulatlan, jogellenes adatkezelés, adatfeldolgozás nem fordulhasson elő
- **Elszámoltathatóság elve:** felelősség az alapelveknek való megfelelésért, és ezt igazolni is kell – megfelelő tájékoztatás, nyilvántartások, DPO kinevezése, IT biztonsági intézkedések.

Személyes adat akkor kezelhető, ha:

- Azt a törvény, vagy törvényi felhatalmazása alapján helyi önkormányzat rendelete közérdeken alapuló célból végzett feladat végrehajtásához szükséges adatkezelést elrendeli.
- Az adatkezelő, törvényben meghatározott feladatainak ellátásához feltétlenül szükséges és az érintett a személyes adatok kezeléséhez kifejezetten hozzájárul (Az Adatkezelőnél rendelkezésre kell állnia az érintett kifejezett írásbeli hozzájáruló nyilatkozatának mindaddig, amíg a személyes adatokat kezeli).

- A fent meghatározottak hiányában az az érintett vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges és azzal arányos, illetve, ha a személyes adatot az érintett kifejezetten nyilvánosságra hozta és az az adatkezelés céljának megvalósulásához szükséges és azzal arányos.

Az Intézmény a GDPR alapelveknek az alábbiak szerint tesz eleget:

1. Az Intézmény által a cél megvalósulásához szükséges mértékben és ideig csak olyan személyes és különleges adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas.
2. Az adatgyűjtés és kezelés kizárólag pontosan meghatározott célból és jogcím alapján történik.
3. Csak annyi adat kerül gyűjtésre és kezelésre, amennyi a célok eléréséhez feltétlenül szükséges, az adatkezelő kerüli a felesleges és irreleváns adatok gyűjtését és tárolását.
4. Az Intézmény munkavállalói és külső megbízottjai (a továbbiakban: alkalmazottai) a feladataik ellátása körében személyes és különleges adatot csak a vonatkozó jogszabályok előírásainak betartásával kezelhetnek.
5. A személyes adatok védelméhez való jog a természetes személyek Alaptörvényben biztosított alapjoga, amely garantálja az adatalanyok információs önrendelkezési jogát. Az információs önrendelkezési jog az érintettek beleegyezésének hiányában kizárólag törvényi felhatalmazás alapján korlátozható. Az információs önrendelkezési jog tiszteletben tartása érdekében az Intézmény alkalmazottja személyes adatot csak az alábbi esetekben kezelhet:
 - *az érintett előzetes, önkéntes és kifejezett hozzájárulása*
 - *szerződés teljesítése a teljesítéshez szükséges mértékben*
 - *az érintett vagy az Intézmény jogos érdekeinek érvényesítése*
 - *az Intézmény jogi kötelezettségének teljesítése*
 - *az érintett vagy más természetes személy létfontosságú érdeke.*
6. Személyes adat kezelésére csak a jelen szabályzat 5. pontjában meghatározott valamely célból, jog gyakorlása vagy kötelezettség teljesítése érdekében van lehetőség. Törvényben elrendelt adatkezelés esetén kizárólag a felhatalmazást adó törvényben meghatározott célból valósulhat meg adatkezelés. Az Intézmény által kezelt – vagy a más adatkezelő által rendelkezésre bocsátott – személyes adatok magáncélra való felhasználása tilos. Az adatkezelésnek mindenkor meg kell felelnie a célhoz kötöttség alapelveinek.
7. Az Intézmény törekszik arra, hogy az általa kezelt adatok pontosak és naprakészek legyenek.
8. Az Intézmény csak addig kezeli a személyes adatokat, ameddig az feltétlenül szükséges.
9. A szükségtelenné vált adatokat véglegesen és helyre nem állítható módon törlik.
10. Az adatok feldolgozására csak az érintett jogainak figyelembevételével kerül sor.
11. Az Intézmény minden tőle telhető és elvárható lépést megtesz az adatok védelme érdekében.

A szabályzat személyi, tárgyi és időbeli hatálya

A jelen szabályzat rendelkezései kötelező alkalmazása az alábbi személyi körre tejed ki:

- Intézmény vezetője
- az Intézmény valamennyi dolgozója
- az óvodai ellátásban részesülők (azok gondviselője)
- az Intézmény valamennyi beszállítója/szerződő partnere a vállalkozás érdekében vagy képviselőjében a vállalkozás kifejezett írásbeli engedélye szerint eljáró bármely más személy.

A szabályzat tárgyi hatálya kiterjed az Intézménynél folytatott valamennyi olyan folyamatra, amely során a GDPR 4. cikk 1. pontjában meghatározott személyes adat kezelése megvalósul.

A szabályzat időbeli hatálya 2019. június 1-jétől visszavonásig tart.

Kockázatok

A jelen szabályzat különösen az alábbi kockázatokkal szembeni védelmet hivatott elősegíteni:

- az adatok jogosulatlan személy vagy személyek általi megszerzése
- érintett adatokkal való rendelkezési jogának megsértése
- személyes adatok kezelésének és őrzésének szabálytalanságai
- érintetti jogok megsértése
- adattovábbítás megbízhatatlan adatfeldolgozóhoz
- hozzáférési jogosultságok nem szabályozottak
- nem teljes körű adatvédelem
- adatkezelési cél teljesülését követően az személyes adatokat nem törlik
- adatfeldolgozóval nincs megállapodás az adatkezelés biztonságáról
- adatok biztonsági rendszer megsértésével/ kijátszásával történő megszerzése

II. ADATKEZELŐ

Az Intézményt érintő adatkezelések esetében az adatkezelőt az intézmény vezetője képviseli.

Adatkezelő megnevezése és elérhetősége

Adatkezelő megnevezése:	Nagycserkeszi Nyitnikék Óvoda és Konyha
Adatkezelő székhelye:	4445 Nagycserkesz, Vasvári Pál u. 101.
Adatkezelő képviselője:	Széchy Erzsébet
Adatkezelő e-mail elérhetősége:	szechy.erzsebet@gmail.com
Adatkezelő telefon elérhetősége:	+36-42-715-583
Óvoda honlapja:	az irányítószerv honlapja: www.nagycserkesz.hu

Specifikus felelősségek

Az Intézmény valamennyi dolgozójának és együttműködő partnerének kötelessége annak biztosítása, hogy az adatok gyűjtése, kezelése és tárolása jogszerűen történjen. Az egyes részfeladatok és felelősségi körök az alábbiak szerint kerülnek meghatározásra:

1. Intézményvezető (adatgazda)

Az Intézményvezető rendelkezésére bocsátott valamennyi adatot megismerheti, felelős valamennyi adatkezelő és adatfeldolgozó tevékenységéért. A teljes jogszabályi és jogi megfelelés biztosítása az ő feladata.

Adatgazda feladata

- a használt információkat és adatokat elemzi, kezeli,
- a döntéseket előkészíti,
- meghatározza – a rendszergazdával – az adatokhoz/tevékenységekhez a hozzáférést, a szükséges, elégséges hozzáférési elv alapján (mindenki csak annyi jogot kapjon, amennyi a munkája elvégzéséhez feltétlenül szükséges),
- engedélyezi vagy megtiltja a hozzáféréseket a hatáskörébe tartozó adatokhoz, elektronikus információs rendszerekhez.

2. Adatvédelmi tisztviselő

Az adatvédelmi tisztviselő kijelölésére a szükségességét bizonyító belső elemzést készítettünk (mérlegelési dokumentumot), az Intézmény esetében az adatvédelmi tisztviselő szükségességét a közfeladat ellátás indokolja:

óvodai ellátás

Az adatvédelmi tisztviselő:

- neve: **Vári Pálné**
- elérhetősége: adatvedelem.nagycserkesz@gmail.com
+36-42/715-630

feladatai:

- GDPR-nek való megfelelés ellenőrzése (a rendeletnek való belső megfelelés vizsgálata, adatvédelmi szabályozás naprakészen tartása),
- információ gyűjtése az adatkezelési tevékenységek, folyamatok meghatározása érdekében,
- elemzi és ellenőrzi az adatkezelési tevékenységek megfelelőségét,
- logikai és fizikai védelem kialakításának ellenőrzése, együttműködés a rendszergazdával,
- tájékoztatást, szakmai tanácsad ad az adatkezelő vagy adatfeldolgozó részére,
- az intézményvezető tájékoztatása az adatvédelmi kötelezettségekről, kockázatokról és feladatokról,

- adatvédelmi hatásvizsgálat tekintetében ajánlást, tanácsot ad (kell-e, milyen módszereket kell követni, ki végezze, milyen biztosítékokat kell alkalmazni a kockázatok enyhítésére).

Ha az intézményvezető nem ért egyet az adatvédelmi tisztviselő ajánlásával, tanácsával, akkor a hatásvizsgálat dokumentációjában kifejezetten igazolni kell, hogy miért nem vették figyelembe.

Az adatvédelmi rendszer kialakításában, működtetésében az adatvédelmi tisztviselőnek az intézményvezetőt támogatnia kell:

- együttműködés és kapcsolattartás a felügyeleti hatósággal,
- adatvédelmi képzés és oktatás biztosítása a munkavállalóknak,
- az érintettek megkeresésére tájékoztatás nyújtása arról, hogy a Hivatal milyen adatait tárolja és kezeli.
- intézkedés adatvédelmi incidens esetére,
- harmadik féllel kötött olyan megállapodások vizsgálata, amely adatkezelési- és továbbítási kérdéseket vet fel.
- együttműködés a partnerek és beszállítók adatvédelmi tisztségviselőivel,
- ellátja a GDPR és az Infó törvény rendelkezéseiben meghatározott további feladatokat.

Az adatvédelmi tisztviselő akadályoztatása esetén az adatvédelmi incidens bejelentését az intézményvezetőnek kell bejelenteni a szechy.ertzsebet@gmail.com email címen.

3. A rendszergazda (vagy Informatikai biztonsági felelős) felelőssége:

- meghatározza az információbiztonsági követelmények megvalósításához szükséges informatikai eszközöket,
- feladatkörébe tartozó rendszereket felügyeli, üzemelteti,
- megszervezi az adatok biztonsági másolatának készítését és karbantartását,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságához, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- az adatgazdával együttműködve kialakítja és működteti a hozzáférési jogosultságok rendszerét,
- nyilvántartja – a jogszabályban definiált adattartalommal – a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- gondoskodik a folyamatos vírusvédelemről, vírusmentesítésről,
- ellenőrzi a rendszer adminisztrációt.

4. A dolgozók általános felelősségei

Valamennyi dolgozó, aki a jelen szabályzatban meghatározott adatokhoz hozzá fér a megszerzett adatokat kizárólag a munkavégzése körében és céljából kezelheti, rögzítheti, tarthatja nyilván

Felhasználó(dolgozók/ügyintézők) feladatai:

- jogosult a munkájához szükséges eszközök használatára, szoftverek, adatok jogosultsági szintje szerinti elérésére, valamint a munkavégzéshez szükséges informatikai, szakmai képzettséget köteles megfelelő szinten tartani,

- felelős a szabályok betartásáért, az információk bizalmosságának megfelelő kezeléséért, valamint a személyes használatba vett eszközök védelméért,
- tilos más felhasználó hozzáférési jogosultságainak használata,
- tilos az Intézmény számítógépeire szoftvereket telepíteni és azokat futtatni,
- a munkavégzés során megszerzett adatokat a munkavállaló erre vonatkozó külön írásos engedély nélkül nem oszthatja meg arra illetéktelen személyekkel, nem teheti közzé, adatot önkényesen nem kezelhet,
- a dolgozó köteles rendszeresen felülvizsgálni és aktualizálni a rendelkezésekre álló adatokat, annak érdekében, hogy személyes adat szükségtelenül ne kerüljön sem tárolásra, sem egyéb kezelésre. A már szükségtelenné váló adatok törlése a munkavállaló felelőssége.

Amennyiben a dolgozó bizonytalan a helyes adatkezelés, vagy az adatvédelmi szempontok tekintetében, úgy köteles tanácsért az aljegyzőhöz vagy az adatvédelmi tisztségviselőhöz fordulni.

Ha a dolgozó tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos, vagy időszerűtlen, köteles azt helyesbíteni, vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.

Az intézmény adatkezelését végző alkalmazottja felelősséggel tartozik a munkavégzése során tudomására jutott személyes adatok jogszerű kezeléséért, a nyilvántartásokhoz rendelkezésére álló hozzáférési jogosultságok jogszerű gyakorlásáért.

2. Adatfeldolgozók főbb adatai

Az adatok egyéb okból történő hozzáférhetővé tétele

Meghatározott feltételek mellett a GDPR Rendelet megengedhetővé teszi azt, hogy jogérvényesítési okokból az érintett hozzájárulása nélkül is más számára megismerhetővé tegye az egyes személyes adatokat.

Adatfeldolgozókra vonatkozó főbb információk:	
szervezet neve	Magyar Államkincstár Sz-Sz.-Bereg Megyei Igazgatóság
székhely	4400 Nyíregyháza, Mártírok tere 8.
Honlap	www.allamkincstar.gov.hu
telefonszám	36 42 314011
adatfeldolgozás célja	bér és munkaügyi adatok feldolgozása
Adatkezelőre vonatkozó főbb információk:	
szervezet neve	Kálmánházi Közös Önkormányzati Hivatal Nagycserkeszi Kirendeltség
székhely	4445 Nagycserkesz, Petőfi u. 10.
Honlap	www.nagycserkesz.hu
e-mail cím	attila.varga@nagycserkesz.hu
telefonszám	36 42 715-630
képviselő neve	Dr. Varga Attila (aljegyző)
adatfeldolgozás célja	könyvviteli adatfeldolgozás

Az adatok adatfeldolgozó részére történő átadása

Az Intézmény szervezetén kívül az alábbi okból és személyekkel osztja meg az érintettre vonatkozó személyes adatokat:

- könyvviteli szolgáltatások ellátása, analitikák vezetése, a költségvetés és beszámoló elkészítése, valamint a MÁK felé történő számviteli, pénzügyi adatszolgáltatások teljesítése végett.

Az adatkezelő az adatok továbbításának megkezdése előtt meggyőződik arról, hogy az adott partner az Európai Unió és magyarországi adatvédelmi szabályoknak megfelelően jár el. Az adatkezelő külső adatfeldolgozás esetén írásban az adatfeldolgozásra vonatkozó szerződést/megállapodást köt, melyben rögzítésre kerül:

- az adatkezelés módja
- az adatkezelés időtartama
- az adatvédelmi és adatbiztonsági garanciák.

III. ADATBIZTONSÁGI SZABÁLYOK

Adatbiztonság követelménye:

- Személyes adatokat is tartalmazó iratot az Intézményből kivinni – munkaköri feladat ellátásának kivételével – csak az intézményvezető egyetértésével lehet. A dolgozó ez esetben is köteles gondoskodni arról, hogy az ne vesszen el, ne rongálódjon, vagy ne semmisüljön meg, és tartalma illetéktelen személy, vagy szerv tudomására ne jusson.
- A fenti iratok elektronikus úton, illetve adatok telefonon csak kivételes esetben, intézményvezetői engedéllyel, az Intézmény technikai eszközeinek igénybevételével továbbíthatók.
- Akár dolgozónál, akár irattárban lévő iratba az intézmény közalkalmazottján kívül más személy – az ügyfél betekintési jogán és jogszabály kötelező előírásán túl – csak akkor tekinthet be, ha ezt az intézmény tevékenységével összefüggő feladatellátás/jogszabály szükségessé teszi. (pl.: ügyészség, rendőrség, kormányhivatal). Az érintett, vagy képviselője betekintési jogának gyakorlása során úgy kell eljárni, hogy ez által mások jogai ne sérülhessenek (a más személyre vonatkozó személyes adatok valamilyen módon ki kell iktatni, el kell takarni). Ugyanígy kell eljárni másolat, kivonat készítésekor is.
- Az intézmény alkalmazottja a nála lévő iratokat köteles munkaidőn túl – és amelyeket lehetséges munkaidőben is – szekrénybe zárva tartani, az asztalon és az irodában egyéb helyen hivatalos iratok csak a munkavégzés céljából és annak tartama alatt tárolhatók.

Informatikai és fizikai védelem

Az Intézmény az alábbi informatikai védelmi eszközöket és módokat alkalmazza:

- fizikai védelem
 - zárható iroda, csoport szoba
 - zárható szekrények
 - riasztó
 - „tisztá asztal-tiszta monitor elv” érvényesítése
- IT védelem
 - tűzfal
 - vírusírtó
 - biztonsági mentések
 - szabályozott hozzáférési jogosultságok
 - jelszavas belépés a programokba
 - e-szig. használata ASP programoknál
 - képernyőzár.

Adattárolás

A jelen bekezdés célja annak meghatározása, hogy az adatokat hol és milyen módon szükséges kezelni ahhoz, hogy az adatok biztonsága biztosítható legyen. Az adattárolásra vonatkozó további esetleges kérdésekkel a rendszergazdához, illetőleg az adatvédelmi tisztviselőhöz fordulhat a dolgozó.

Papír alapú adatkezelés

A papír alapon kezelt adatokat olyan biztonságos helyen szükséges tárolni, ahol arra jogosulatlan személy azokat nem ismerheti meg.

Azokat az elektronikus úton érkezett vagy kezelt adatokat, melyek valamely okból nyomtatásra kerülnek elzárt irattárolóban, illetőleg elkülönítetten szükséges kezelni. Az Intézmény munkatársai kötelesek gondoskodni arról, hogy a kinyomtatott iratokhoz arra jogosulatlan személyek ne férjenek hozzá. A kinyomtatott adatokat tartalmazó iratokat azonnal szükséges megsemmisíteni akkor, amikor a kinyomtatás oka megszűnik.

Az iratok kezelésére vonatkozóan az Intézmény külön rendelkezik Iratkezelési szabályzattal, melyben az adatvédelmi szabályoknak szintén érvényesülni kell. Az Iratkezelési szabályzatban az adatvédelemmel kapcsolatosan rögzíteni szükséges:

- ki jogosult az iratokat kezelni, iratokba betekinteni,
- hogyan történik az irattovábbítás,
- személyes adatokat tartalmazó iratok szervezeten belüli továbbítása (elektronikus vagy papír alapú – adatbiztonsági, hozzáférési jogosultságok szabályainak rögzítése),
- iratok tárolása (zárható szekrényben, kulcs hozzáférése szabályozott legyen – összhangban az adatkezelési jogosultsággal),

- iratok, dokumentumok napközbeni, munkavégzés során történő tárolása (jogosulatlan személy ne férjen hozzá személyes adatot tartalmazó dokumentumhoz).

Elektronikus adatkezelés

- Az elektronikusan tárolt adatokat védeni szükséges a jogosulatlan eléréstől, véletlen törléstől, és kémprogramokkal/vírusokkal/illetéktelen rendszerfeltörésekkel és rendszertámadásokkal szemben.
- Az adatokat erős jelszavakkal szükséges védeni. A jelszavaknak titkosnak kell lenniük, a dolgozók nem oszthatják meg azt sem egymás között, sem más személyekkel.
- Amennyiben az adat hordozható adattárolón (CD, DVD, pendrive, egyéb külső adattároló) kerül rögzítésre, ezeket az adattároló eszközöket a használatot követően biztonságos helyen, jogosulatlan személyek számára hozzáférhetetlenül szükséges tárolni.
- Valamennyi adattárolásra szolgáló szervert és számítógépet szükséges tűzfalal és vírusirtóval védeni.
- Az adattárolásra alkalmazott szoftvereket rendszeresen frissíteni szükséges.

Postai küldeményekre vonatkozó speciális szabályok

A postai küldemények átvételére az intézményvezető jogosult. Átvételre jogosult lehet más, az intézményvezető által meghatározott személy (az Iratkezelési szabályzatban foglaltaknak megfelelően). A postai küldemények átvételére vonatkozó részletszabályokat az Iratkezelési szabályzat tartalmazza.

Az adatok felhasználása

Az Intézmény az adatkezelés eltérő célja alapján ügyviteli és nyilvántartási célú adatkezeléseket végez. Az ügyvitelhez kapcsolódó adatkezelés a szerződés/megállapodás nyilvántartásához (iktatásához), feldolgozásához kapcsolódik.

Alapvető célja az adott szerződéshez/megállapodáshoz tartozó feladatok elvégzéséhez (szerződések teljesítése), az adatkezelés szereplőinek azonosításához és a szerződés lezárásához szükséges adatok biztosítása. Az ügyviteli célú adatkezelés során a személyes adatok kizárólag az adott szerződés irataiban és az ügyviteli segédletekben szerepelnek; kezelésük ebből a célból csak az alapul szolgáló irat selejtezéséig lehetséges.

A nyilvántartási célú adatkezelés az egyes adatfajtákból álló adatállományt hoz létre, az adatkezelés időtartama alatt biztosítva az adatok különböző jellemzők alapján történő visszakereshetőségét, lekérdezhetőségét.

Nyilvántartási célú adatkezelés:

- az adatkezelővel munkavégzésre irányuló jogviszonyban álló személyek személyes adataival,
- óvodai ellátásban részesülők (gondviselő) személyes adataival,
- az adatkezelővel szerződéses kapcsolatba került személyek személyes adataival, vagy azzal összefüggésben kezelt személyes adatokkal (ügyviteli célú adatkezelés);

- a hivatalos statisztika célját szolgáló személyes adatokkal,
- levéltári őrzésre átadott iratokkal összefüggésben valósul meg.

A személyes adatok kezelésének célja az Intézmény alaptevékenysége során történő felhasználása, ennek megfelelően az alábbi feladatok azonosíthatók:

- a személyes adatokkal dolgozó munkavállalók a munkaterület elhagyása során kötelesek a felhasznált eszközt képernyőzárral védeni, melyhez egyedi belépési azonosító, illetőleg kód kapcsolódik,
- személyes adat csak olyan levelezőrendszeren küldhető tovább, melynek biztonsága és zárt jellege garantált, továbbá olyan címzett számára, aki megfelelő és biztos módon beazonosítható olyan személyként, aki a fogadott személyes adatokat jogszerűen megismerheti
- az Intézmény működése során nem vihető ki személyes adatokat tartalmazó irat az intézmény épületéből. Amennyiben ez mégis szükségessé válna, úgy e tekintetben a dolgozók kötelesek azt bejelenteni, és egyedi jóváhagyást kérni az intézményvezetőtől.

A kezelt adatok pontossága

Az adatkezelő jogszabályi kötelezettsége az általa kezelt személyes adatok naprakész és pontos nyilvántartása.

Az Intézmény valamennyi munkatársa köteles azon lenni, hogy a személyes adatok naprakészek legyenek, és kötelesek az adatokat az ügyfél- és egyéb kapcsolatok során folyamatosan egyeztetni.

Amennyiben a kezelt adatok körében pontatlan adatok kerülnek elő, azt haladéktalanul pontosítani szükséges, így különösen, ha az érintett az általa megadott telefonszámon vagy elektronikus levelezési címen már nem érhető el. Az elektronikus levelezés mindaddig elérhetőnek tekinthető, ameddig az ügyfél a cím megváltozását nem jelenti be, vagy onnan a kézbesítés sikertelenségére vonatkozó rendszerüzenet vissza nem érkezik. Az érintett jelzésének hiányában is pontatlannak bizonyult adatot valamennyi rendszerből és adattárolóról a pontatlanság megállapítását követően haladéktalanul törölni szükséges.

Az „érintettek hozzáférési jogai”

Valamennyi érintett, akinek a személyes adatait kezelik jogosult:

- tájékoztatást kérni arról, hogy milyen okból és mely adatait kezelik,
- tájékoztatást kérni azon címzettekről vagy címzettek kategóriáiról, akikkel, illetve amelyekkel a személyes adatokat közölni fogják,
- adott esetben a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, az időtartam meghatározásának szempontjai
- kérheti az adatok helyesbítését, törlését vagy kezelésének korlátozását, tiltakozhat a személyes adatok kezelése ellen,
- ha az adatokat az Intézmény, nem az érintettől gyűjtötte, a forrásukra vonatkozó valamennyi fellelhető információ,
- a Hatósághoz fordulás lehetőségéről,
- tájékoztatást kérni arról, hogy hogyan érheti el az Intézmény által kezelt adatokat,

- tájékoztatást kérni arról, hogy az adatkezelő naprakészen tartja-e az adatait, és milyen intézkedéseket hozott a naprakészen tartás érdekében.

Az érintettnek joga van továbbá:

hozzájáruláson alapuló adatkezelés esetén

- a hozzájárulását visszavonni,
- tiltakozni a személyes adatai kezelése ellen,
- kérni az adatai más szerv/személy részére történő hiánytalan továbbítását (adathordozhatóság),
- az adatok helyesbítéséhez,
- az adatkezelés korlátozásához,
- az adatok törléséhez,
- az adatok hordozhatóságához

Az adatkezelő minden esetben pontosan azonosítja az adatkérő személyét a kért információ kiadását megelőzően.

Az intézményvezető az adatvédelmi tisztviselővel való egyeztetést követően- jogosult dönteni az érintett kérelméről. Ha dolgozóhoz érkezik a megkeresés, azt haladéktalanul köteles az intézményvezető részére továbbítani.

Tájékoztatási kötelezettség teljesítése

Az adatkezelő biztosítja, hogy az érintettek tisztában legyenek azzal, hogy a személyes adataik feldolgozásra kerülnek, és felvilágosítást kapjanak arról, hogy:

- hogyan használják/dolgozzák fel az adataikat
- hogyan érvényesíthetik a jogaikat.

A fenti okból az Intézmény adatkezelési tájékoztatót készít, és könnyen hozzáférhetővé teszi az érintettek számára, még az adatkezelés megkezdését megelőzően. Az adatkezelési tájékoztató minden adatkezelési művelet vagy műveletsorozat tekintetében külön- külön meghatározza:

- az adatkezelőt és elérhetőségeit
- az adatvédelmi tisztviselőt és elérhetőségeit
- adatfeldolgozókat és elérhetőségeit
- az adatkezelés célját;
- az adatkezeléssel érintettek körét
- kezelt személyes adatok körét
- adatkezelés jogalapját
- adatkezelés időtartamát
- adattárolás határidejét
- adattovábbítást
- adatok címzettjeit
- adatbiztonsági intézkedéseket
- az érintett személy jogait

Az adatkezelési tájékoztatás módja történhet:

- papír alapon, személyesen átadva (személyügyi adatkezelési tájékoztató)
- honlapon elérhető, letölthető módon, célonként

A tájékoztatást az érintettől való adatgyűjtés esetén a gyűjtés előtt kell megadni.

Amennyiben nem az érintettől származnak az adatok, a gyűjtést követő 30 napon belül meg kell történnie az érintett tájékoztatásának.

A személyes adatok törlése

Az adatkezelő törli a személyes adatokat, ha

- a személyes adatra nincsen szükség abból a célból, amelyből gyűjtötték vagy más módon kezelték,
- az érintett a hozzájárulását visszavonja, és az adatkezelésnek más jogalapja nincsen,
- a személyes adatok kezelése valamely okból jogellenesen történt – a személyes adatokat jogi kötelezettség teljesítése érdekében törölni kell
- az érintett tiltakozott az adatkezelés ellen.

A törlés szükségességének felismerése az ügyintéző feladata, aki azt- amennyiben a törlés szükségessége tekintetében bizonytalan- köteles az intézményvezetőnek jelezni.

Az adatok törlését megelőzően írásban az intézményvezetőt tájékoztatni kell.

A személyes adatok törlésére az intézményvezető írásos jóváhagyását követően kerülhet sor. Az adatok törlését végleges, és helyreállíthatatlan módon kell megvalósítani, melyet dokumentálni kell.

A személyes adatokat tartalmazó dokumentumok selejtezését az iratsejtezési eljárásrend szerint kell lefolytatni. A személyes adatokat tartalmazó egyéb iratok megsemmisítéséről szintén a szükséges biztonsági intézkedések mellett kell gondoskodni.

Az adatok helyesbítéséhez való jog biztosítása

- Az adatkezelő biztosítja, hogy az érintettek megfelelő tájékoztatás alapján és befolyásmentesen gyakorolhassák az adatok helyesbítésével kapcsolatos jogaikat.
- A helyesbítéshez való jog biztosítása során az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat.

Az adatok helyesbítéséért az adott ügy típusért felelős személy felel, az intézményvezető előzetes tájékoztatása mellett.

Az adatkezelés korlátozásához való jog biztosítása

- Az adatkezelő biztosítja, hogy az érintettek megfelelő tájékoztatás alapján és befolyásmentesen gyakorolhassák az adatkezelés korlátozásával kapcsolatos jogaikat.
- Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül korlátozza az adatkezelést az alábbiak esetében:

- ha az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát,
- amennyiben az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kérte azok felhasználásának korlátozását,
- az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényi azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez,
- az érintett tiltakozott az adatkezelés ellen, ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Az adatkezelő amennyiben az adatok korlátozásnak feltételei fennállnak indokolatlan késedelem nélkül elvégzi azok korlátozását az érintett rendelkezésének megfelelően.

Az adatok hordozhatóságára irányuló jog biztosítása

- Az adatkezelő biztosítja, hogy az érintettek megfelelő tájékoztatás alapján és befolyásmentesen gyakorolhassák az adatok hordozhatóságára irányuló jogaikat.

Amennyiben az adatok hordozhatóságának feltételei fennállnak, az adatkezelő indokolatlan késedelem nélkül az érintett rendelkezésének megfelelően:

- az érintett rendelkezésére bocsátja az adatokat tagolt, széles körben használt, géppel olvasható formátumban,
- az érintett által meghatározott adatkezelőnek közvetlenül továbbítja az adatokat.

Az adatkezelés elleni tiltakozás jogának biztosítása

- Az adatkezelő biztosítja, hogy az érintettek megfelelő tájékoztatás alapján és befolyásmentesen gyakorolhassák az adatkezelés elleni tiltakozás jogát.
- Amennyiben az adatkezelés elleni tiltakozási jog érvényesítésének feltételei fennállnak, az adatkezelő teljesíti a kérelmet, megszünteti az adatok kezelését, törli az adatokat.

Az adatokhoz való hozzáférési jog biztosítása

- Az adatkezelő biztosítja, hogy az érintettek megfelelő tájékoztatás alapján és befolyásmentesen gyakorolhassák az adatokhoz való hozzáférési jogukat.
- Ha az érintettre vonatkozó személyes adatokat az érintettől gyűjtik, az adatkezelő a személyes adatok megszerzésének időpontjában az érintett rendelkezésre bocsátja az információkat.

Az adatkezelés jogalapjának vizsgálata

Az adatkezelő folyamatosan vizsgálja az adatnyilvántartásba felvett valamennyi személyes adatkezelés dokumentációját, hogy az abban szereplő adatok kezelésére a GDPR és a belső szabályzat szerint került-e sor, az adatkezelések megfelelő jogalapja fennáll-e, az adott adatokat megfelelő jogalap alapján kezelik-e.

Az egyes adatkezelések során meg kell állapítani az adatkezelés jogalapját és azt, hogy az adatot adatkezeléshez szükséges jogalapot alátámasztó dokumentáció rendelkezésre áll-e.

- hozzájáráson alapuló adatkezelés esetén: az érintett vagy törvényes képviselőjének legalább teljes bizonyító magánokiratba foglalt nyilatkozata, amely tartalmazza az érintett akaratának önkéntes és határozott kinyilvánítását, amely megfelelő tájékoztatáson alapul (az adatkezelés célja, jogalapja, időtartama, az adatkezelő neve címe és az adatkezeléssel összefüggő tevékenység) és amellyel az érintett félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat – teljes körű vagy egyes műveletekre kiterjedő kezeléséhez.
- szerződés teljesítéséhez szükséges adatkezelés: az érintettel kötött szerződés – szerződéskötésre vonatkozó nyilatkozat (megjelölve a szerződésben a szükséges adatkezelés, vagy külön mellékletben megszövegezve, hogy az adatkezelés a szerződés mely rendelkezésének teljesítéséhez szükséges).
- jogi kötelezettség teljesítéséhez szükséges adatkezelés: az adatkezelést elrendelő vagy szükségessé tevő jogszabályi rendelkezés pontos megnevezése és szövege.
- az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges adatkezelés: az érdekmérlegelési teszt elvégzése szükséges
- közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges adatkezelés: a jogszabályi rendelkezés pontos megnevezése és szövege, valamint az e jogosítványból meghatározva az adott adatkezelés szükségessége.
- az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges adatkezelés: érdekmérlegelési teszt szükséges.

Különleges adatok kezelése

A személyes adatok különleges kategóriáinak kezelése esetén az adatkezelőnek minden adatkezelés során meg kell vizsgálnia, hogy a hozzájáruláson alapuló adatkezelésre, személyes adatok különleges kategóriáinak kezelésére az adatkezelési szabályok szerint került-e sor.

- az érintett kifejezett hozzájárulását adta a különleges kategóriába sorolt személyes adatok egy vagy több konkrét célból történő kezeléséhez, és az uniós vagy tagállami jog nem rendelkezik úgy, hogy az említett tilalom nem oldható fel az érintett hozzájárulásával.

Gyermekek jogainak biztosítása

A gyermekek jogainak biztosítása érdekében minden adatkezelés során meg kell vizsgálni, hogy a hozzájáruláson alapuló adatkezelésre, személyes adatok különleges kategóriáinak kezelésére a törvényes képviselői jog gyakorlójának hozzájárulása rendelkezésre áll-e.

Az adatkezelő a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvényben szabályozott feladatai ellátása során a 135-136. §-ban felsorolt adatkörben, az ott meghatározott célok teljesüléséhez elengedhetetlenül szükséges személyes adatokat kezelheti.

Adatszivárgás megelőzésének biztosítása

Az adatszivárgás megelőzése érdekében az alábbi intézkedéseket kell végrehajtani:

- indokolt esetben a személyes adtok álnevesítése és titkosítása
- folyamatos kontrollt kell kiépíteni a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének és az integritás biztosítása érdekében
- ki kell alakítani az informatikai biztonság keretében az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres kontrollját, a kontrollok értékelését
- a biztonság megfelelő szintjének meghatározására kockázatelemzést kell végezni a továbbított, tárolt vagy más módon kezelt személyes adtok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésekből felmerülő kockázatok azonosítására és azok súlyának az általuk okozható kár meghatározására.

Felelősök: folyamatgazdák, rendszergazda

Adatvédelmi hatásvizsgálat elvégzése

Adatvédelmi hatásvizsgálatra csak akkor van szükség, ha az adatkezelés „valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve”.

Az adatkezelőnek folyamatosan értékelni kell az adatkezelési tevékenységből eredő kockázatokat, hogy időben felismerhető legyen, ha az adatkezelés valamely fajtája magas kockázattal jár.

Felelősök a folyamatgazdák, belső kontroll koordinátor.

Intézkedések adatvédelmi incidens esetén

Az adatkezelő dolgozója, együttműködő Partnere adatvédelmi incidens esetén azonnal köteles értesíteni az adatvédelmi tisztviselőt, akiknek haladéktalanul vizsgálatot kell indítaniuk az incidens kockázatának felmérésére. Indokolt esetben a Kirendeltség rendszergazdáját is haladéktalanul értesíteni kell.

Amennyiben az adatvédelmi incidens kockázatot jelent az érintett jogaira nézve, úgy az adatkezelő legkésőbb 72 (hetvenkét) órán belül köteles azt bejelenteni a Nemzeti Adatvédelmi és Információszabadság Hatóság incidens- bejelentési nyilvántartási rendszerébe.

Az adatvédelmi incidens esetén követendő eljárásrendről az Intézmény külön szabállyal rendelkezik. (Adatvédelmi incidens kezelésének eljárásrendje)

Az Intézmény adatvédelmi szervezete

- Adatkezelő
- Adatvédelmi tisztviselő (DPO)
- Informatikai Biztonsági Felelős (IBF), rendszergazda
- Belső kontrollrendszer folyamatgazdái
- Közalkalmazottak, dolgozók (teljes foglalkoztatotti állomány)
- Adatfeldolgozók (külsősök, pl. Kirendeltség, MÁK stb.)

Ellenőrzés rendszere

- Átfogó felülvizsgálat – adatvédelmi megfelelőségi audit (3 évente) – felelős: **intézményvezető/külső szakértő**
- Folyamatba épített ellenőrzés (ellenőrzési nyomvonalban adatvédelmi, adatkezelési főfolyamat és részfolyamat meghatározása, kontrollpontok kiépítése) – folyamatos, éves felülvizsgálat – felelős: **folyamatgazdák**
- Integrált kockázatkezelés – adatvédelmi, adatkezelési kockázatok azonosítása, értékelése – folyamatos, éves felülvizsgálat – felelős: **folyamatgazdák**
- vezetői ellenőrzés – felelős: **intézményvezető**
- szakmai felülvizsgálat – folyamatos, évente, felelős: **adatvédelmi tisztviselő**

Adatvédelmi oktatás, ismeretmegújítás

Az Intézmény dolgozóinak adatvédelmi képzését, ismeretmegújításának szervezését az adatvédelmi tisztviselő végzi. Az oktatási ütemtervet az adatvédelmi tisztviselő állítja össze, az intézményvezető hagyja jóvá.

Önálló szabályozási körű adatkezelések

- A közérdekből nyilvános adatok közzétételének, a közérdekű adatok megismerésének részletes eljárási rendjét az Intézmény **Közérdekből nyilvános adatok közzétételének, a közérdekű adatokra vonatkozó szabályzata** tartalmazza.
- Az adatok informatikai biztonságával kapcsolatos részletes adatvédelmi eljárás rendet az **Informatikai Biztonsági Szabályzat** tartalmazza.
- Az Önkormányzat által üzemeltetett honlapon való adatok kezelésének és védelmének részletes eljárási rendet a **Honlap Szabályzata** tartalmazza.
- A papír alapú, személyes adatokat is tartalmazó dokumentumok, ügyiratok adatvédelmével, biztonságával kapcsolatos eljárásokat az **Iratkezelési Szabályzat** tartalmazza.

Nyilvántartások

A személyes adatok kezelésével kapcsolatosan az alábbi nyilvántartásokat kell vezetni:

- Adatvédelmi incidensek nyilvántartása (felelős: adatvédelmi tisztviselő)
- Adatfeldolgozók nyilvántartása (felelős: intézményvezető)
- Adatkezelési hozzájárulások nyilvántartása (felelős: intézményvezető)
- Adatkezelési tájékoztatások nyilvántartása (felelős: intézményvezető)

A nyilvántartásokat folyamatosan kell vezetni, évente felül kell vizsgálni.

Szabályzat felülvizsgálata

A jelen szabályzatot- amennyiben az ügymenetben és az adatkezelések módszertanában változás nem történik - évente felül kell vizsgálni.

A jelen szabályzatot kötelező felülvizsgálni olyan esetekben, amikor új kockázatértékelésre okot adó esemény, avagy az adatkezelés módjában és metodikájában egyéb lényeges változás történik.

Az új kockázatértékelés elkészítésére olyan okból, avagy eseményből kerül sor, amikor valószínűsíthető, hogy az adatok kezelése az érintettekre kockázatot jelenthet (így különösen új adatkezelési technológia bevezetése, alkalmazása, a korábbtól eltérő módon történő adatgyűjtés vagy adattovábbítás stb.)

Záró rendelkezés

E Szabályzat rendelkezéseit meg kell ismertetni az Intézmény valamennyi dolgozójával, és a munkavégzésre irányuló dokumentumokban (kinevezés, szerződés stb.) elő kell írni, hogy betartása és érvényesítése minden munkavállaló (foglalkoztatott) lényeges munkaköri kötelezettsége.

A „Munkaköri kikötés” a dolgozók személyügyi nyilvántartásában kerül elhelyezésre.

Nagycserkesz, 2019. május 30.

Széchy Erzsébet
intézményvezető