2025.

Nagycserkeszi Szociális Szolgáltató Központ és Mini Bölcsőde

Adatvédelmi és adatbiztonsági szabályzat

Tartalom

I. Általános rendelkezések

A **Nagycserkeszi Szociális Szolgáltató Központ és Mini Bölcsőde (**továbbiakban: **Intézmény) és a** Kálmánházai Közös Önkormányzati Hivatal **Nagycserkeszi Kirendeltsége (**továbbiakban: **Kirendeltség) a** gazdasági feladatokat ellátó szervezet a rendes ügymenetéhez az alaptevékenysége körében elengedhetetlenül szükséges személyes adatokat gyűjtenie és kezelnie kell. A begyűjtött adatok vonatkozhatnak ellátottakra, ügyfelekre, együttműködő partnerekre (vevők/szállítók képviselőire, kapcsolattartóira), dolgozókra, és egyéb olyan személyekre, akikkel az alaptevékenység folytatása során kapcsolatba kerül.

Jelen rendelkezéseket az Intézmény és a Kirendeltség 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.

A Nagycserkeszi Szociális Szolgáltató Központ és Mini Bölcsőde és a Kálmánházai Közös Önkormányzati Hivatal Nagycserkeszi Kirendeltségének 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 és a Kirendeltség 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.

1. Vonatkozó jogszabályok (szabályzatban alkalmazott rövidítések)

Az Intézmény jogszabályi alapon kezelt adatait elrendelő jogalapok:

- a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény,
- a közfoglalkoztatásról és a közfoglalkoztatáshoz kapcsolódó, valamint egyéb törvények módosításáról szóló 2011. évi CVI. törvény
- a Munka Törvénykönyvéről szóló 2012. évi I. törvény
- 1993. évi III. törvény a szociális igazgatásról és szociális ellátásokról
- 9/1999. (XI.24.) SzCsM rendelet
- az adózás rendjéről szóló 2017. évi CL. törvény
- a személyi jövedelemadóról szóló 1995. évi CXVII. törvény
- a munkavédelemről szóló 1993. évi XCIII. törvény
- a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról szóló 1996. évi XXXI. törvény
- a kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény
- a társadalombiztosítási nyugellátásról szóló 1997. évi LXXXI. törvény
- a közokiratról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
- a munkavédelemről szóló törvény végrehajtásáról rendelkező 5/1993. (XII.26.) MÜM rendelet
- a kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény végrehajtásáról szóló 217/1997. (XII. 1.) Korm. rendelet
- munkaköri, szakmai, illetve személyi alkalmasság orvosi vizsgálatáról és véleményezéséről szóló 33/1998. (VI.24.) NM rendelet
- az egyes vagyonnyilatkozat-tételi kötelezettségekről szóló 2007. évi CLII. törvény
- az adóigazgatási eljárás részletszabályairól szóló 465/2017. (XII.28.) Korm. rendelet
- munkába járással kapcsolatos utazási költségtérítésről szóló 39/2010. (II.26.) Kormány rendelet

2. A szabályzat célja

Az *Adatvédelmi és adatbiztonsági szabályzat (továbbiakban: 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;
- az adminisztráció és ügyintézés során az érintettek személyes adatainak védelmét;
- rögzítse az Intézmény adatvédelmi elveit;
- erősítse a dolgozók adatvédelmi tudatosságát;

- támogassa az érintetti jogok érvényesülését.

A jelen adatvédelmi és adatbiztonsági szabályzat biztosítja, hogy az Intézmény
- megfelel az adatvédelmi jogi követelményeknek, és megfelelő adatvédelmi gyakorlatot és operatív tevékenységet folytat
- védi és figyelembe veszi a foglalkoztatottak, egyéb alkalmazottak, együttműködő partnerek és beszállítók, valamint a szolgáltatást igénybe-vevők 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.

Az Intézmény az alábbi stratégiai célokat és indikátorokat határozta meg az adatvédelem és adatbiztonság folyamatával kapcsolatosan:

- Megfelelni az új adatvédelmi és adatbiztonsági követelményeknek.
  teljesítménymérés: intézkedési terv teljesítésének nyomon követése
- A személyes adatok védelme, érintetti jogok ne sérüljenek.
  teljesítménymérés: belső szabályzatok elkészítése, kiegészítése adatbiztonsági feladatokkal, felelősökkel
- Adatvédelmi incidens, illetve integritást sértő esemény bekövetkezésének elkerülése.
  teljesítménymérés: adatvédelmi folyamatok kockázatainak azonosítása, intézkedések meghozatala, integritáskontrollok kiépítése és azok hatékonyságának érékelése
- Adatvédelmi tudatosság erősítése.
  teljesítménymérés: belső oktatások, képzések száma, résztvevők száma
- Informatikai biztonsági rendszer fejlesztése.
  teljesítménymérés: hozzáférések naplózása, archiválás, biztonsági mentések gyakoriságának felülvizsgálata, internet használat korlátozása (közösségi oldalak használatának tiltása, az Intézmény elektronikus levelezőrendszerének használata)
- NAIH bírság elkerülése.
  teljesítménymérés: bírságtételek összege, viszonyítás az árbevételhez

3. A szabályzat személyi, tárgyi és időbeli hatálya

Személyi hatály

A jelen szabályzat rendelkezései kötelező alkalmazása az alábbi személyi körre tejed ki:
- intézményvezető
- polgármester
- az Intézmény valamennyi dolgozója
- Kálmánházai Közös Önkormányzati Hivatal Nagycserkeszi Kirendeltségének köztisztviselői
- az Intézmény által nyújtott szolgáltatást igénybe-vevőkre

- az Intézmény valamennyi beszállítója/szerződő partnere a vállalkozás érdekében vagy képviseletében 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** 2025. január 01-től visszavonásig tart.

II. Értelmező rendelkezések

A jelen szabályzat alkalmazásában:

„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;
„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;
„az adatkezelés korlátozása”: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;
„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 előre jelzésére használják;
„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;
„adattörlés”: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
„adatmegsemmisítés:” az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;

„nyilvántartási rendszer”: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;
„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;
„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;
„címzett”: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz.
„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;
„érintett”: bármely információ alapján azonosított vagy azonosítható természetes személy;
„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;
„személyes adat”: az érintettre vonatkozó bármely információ
„különleges adat”: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személye 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;
„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;
„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;
„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;
„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;

„hírközlő eszköz”: bármilyen technikai eszköz, technológiai eljárás, amely egy vagy több fogadó személy számára jelzések, adatok és információk továbbítására vagy fogadására alkalmas.
„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.

Szervezeti specifikáció

- **adatkezelő és adattovábbító**: az Intézmény, melynek nevében a létesítő okiratban illetve a szakmai alapdokumentumban megjelölt képviselője jár el.
- **adatállomány:** a szolgáltatásban részesülők, az alkalmazottak jogviszonyával kapcsolatos, jogszabály által előírt módon és formában az Intézmény által kezelt, feldolgozott és tárolt valamint továbbított adat.
- **adattovábbítás:** az Intézmény adatfeldolgozónak vagy címzettnek adatfeldolgozás vagy más jogszabály által előírt központi adatállományokba történő továbbítása az adatoknak.
- **nyilvánosságra hozatal:** egyes személyes adatoknak az Intézmény kommunikációs felületein (honlap, faliújság, hirdetőtábla stb.) honlapján és más orgánumokon történő közlése.

III. 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).

1. GDPR Alapelvek

- **Célhoz kötöttség elve:** meghatározott, egyértelmű és jogszerű célból történhet a személyes adatok gyűjtése
- **Jogszerűség, tisztességes eljárás és átláthatóság elve**
  - az érintett hozzájárulását adta
  - szerződés teljesítéséhez szükséges
  - jogi kötelezettség teljesítéséhez szükséges
  - létfontosságú érdek védelme miatt szükséges
  - közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges
  - jogos érdek érvényesítéséhez szükséges

- **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 ne fordulhasson elő
- **Elszámoltathatóság elve:** felelősség az alapelveknek való megfelelőségért, és ezt igazolni is kell – megfelelő tájékoztatás, nyilvántartások, DPO kinevezése, IT biztonsági intézkedések.

Az Intézmény a GDPR alapelveknek az alábbiak szerint tesz eleget:
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.

Az adatgyűjtés és kezelés kizárólag pontosan meghatározott célból és jogcím alapján történik.
Csak annyi adat kerül gyűjtésre és kezelésre, amennyi a célok eléréséhez feltétlenül szükséges, az adatkezelő kerüli a felesleges és irreleváns adatok gyűjtését és tárolását.

Az Intézmény dolgozói és külső megbízottjai (a továbbiakban: alkalmazottai) a feladataik ellátása körében személyes és különleges adatot csak a vonatkozó jogszabályok előírásainak betartásával kezelhetnek.

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.*

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 alapelvének.***

Az Intézmény törekszik arra, hogy az általa kezelt adatok pontosak és naprakészek legyenek.
Az Intézmény csak addig kezeli a személyes adatokat, ameddig az feltétlenül szükséges.
A szükségtelenné vált adatokat véglegesen és helyre nem állítható módon törlik.
Az adatok feldolgozására csak az érintett jogainak figyelembevételével kerül sor.

Az Intézmény minden tőle telhető és elvárható lépést megtesz az adatok védelme érdekében.

2. Kockázatok és hatásvizsgálat

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

Az adatvédelmi kockázatok felmérése és kezelésére javaslattétel a folyamatgazdák és az adatvédelmi tisztviselő feladata.

adatkezelés folyamatában azonosított kockázatok:

- nem biztosítják az érintett számára, hogy visszavonhassa hozzájárulását *(abban az esetben, ha hozzájáruláson alapult az adatkezelés)*
- nem értesítik az érintettet az adatvédelmi incidensről
- bejelentés a Hatóság felé elmarad, vagy késedelmesen történik
- előzetes tájékoztatás elmarad a kamerával történő megfigyelésről
- érdekmérlegelési teszt nem készül *(30. v. 60.napos tárolás esetén)*
- nem vezetik a nyilvántartást
- személyes adatot tartalmazó iratokat nem zárható helyen tárolják
- munkaköri leírást nem egészítik ki az adatkezelési, adatvédelmi feladatokkal, felelősséggel
- nincs vírusírtó a számítógépeken
- adatmentéseket, adattárolást nem szabályozták
- nem megfelelően választották meg az adatkezelés jogalapját
- egyéb

Az adatvédelem folyamatainál azonosított kockázati tényezőket, kockázatokat az Intézmény integrált kockázatkezelési rendszerének részeként kell elemezni, értékelni.

Az ellenőrzési nyomvonal és kockázatkezelés ***felülvizsgálata*** folyamatos, de évente egyszer az Integrált kockázatkezelési szabályzatban meghatározott határidőben el kell végezni. Kiemelt terület az adatvédelmi kockázatok elemzése és kezelése.

A monitoring stratégia részeként az ***adatvédelmi tisztviselő nyomon követi a maradványkockázatok alakulását***, szükség esetén javaslatot tesz azok mérséklésére, vagy a kockázati tűréshatás felülvizsgálatára.
Továbbá ***belső ellenőrzés*** keretében az ***adatvédelmi és adatbiztonsági folyamatoknál kialakított kontrollrendszert felül kell vizsgálni***, legalább három évente. Hiányosság feltárása esetén gyakrabban.

Az ***intézményvezetőnek intézkedéseket kell hoznia*** a kockázatok mérséklése és elkerülése érdekében. Köteles gondoskodni az ***intézkedések végrehajtásának felülvizsgálatáról***. A „vezetői nyilatkozat" keretében ***értékelnie kell az adatbiztonság érdekében kialakított kontrollfolyamatokat***.

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.

Felelős: adatvédelmi tisztviselő
határidő: folyamatos (de legalább évente az integrált kockázatkezelés felülvizsgálatakor – határidő az integrált kockázatkezelési szabályzatban meghatározott időpont)

IV. Adatkezelő

1. Adatkezelő megnevezése és elérhetősége

Adatkezelő megnevezése:	**Nagycserkeszi Szociális Szolgáltató Központ és Mini Bölcsőde**
Adatkezelő székhelye:	4445 Nagycserkesz, Iskola u. 21.
Adatkezelő képviselője:	**Körmöndi Judit**
Adatkezelő e-mail elérhetősége:	judit.kormondi@nagycserkesz.hu
Adatkezelő telefon elérhetősége:	20/3999-477
Irányítószerv honlapja:	www.nagycserkesz.hu

Adatkezelő megnevezése:	**Kálmánházai Közös Önkormányzati Hivatal Nagycserkeszi Kirendeltsége (továbbiakban Nagycserkeszi Kirendeltség)**
Adatkezelő székhelye:	4445 Nagycserkesz, Petőfi u. 10.
Adatkezelő képviselője:	**Dr. Lekli-Székely Ágota aljegyző**
Adatkezelő e-mail elérhetősége:	agota.lekli-szekely@nagycserkesz.hu
Adatkezelő telefon elérhetősége:	+36-42/715-630

Az Intézményt érintő adatkezelések esetében az adatkezelőt a intézményvezető képviseli.

A Kálmánházai Közös Önkormányzati Hivatal Nagycserkeszi Kirendeltségét (gazdasági feladatokat ellátó szervezet) az aljegyző képviseli.

2. Feladatok és 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:

2.1 Intézményvezető/aljegyző (adatkezelő)

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

Az intézményvezető/aljegyző mint adatkezelő feladatai és felelőssége

- GDPR alapelvek érvényre jutásának biztosítása,
- adatvédelmi és adatbiztonsági intézkedések meghozatala,
- adatvédelmi szabályoknak megfelelő működés folyamatos biztosítása (tisztességes, átlátható és elszámoltatható adatkezelés)
- belső adatvédelmi és adatbiztonsági szabályok megalkotása,
- adatvédelmi tisztviselő kijelölése, hatósághoz bejelentése
- érintettek adatkezeléséről szóló előzetes tájékoztatás megadása,
- érintetti joggyakorlás elősegítése,
- érdekmérlegelési teszt, hatásvizsgálat elkészítése (amennyiben indokolt),
- adatfeldolgozóval megállapodás megkötése,
- adatvédelemmel, adatkezeléssel kapcsolatos nyilvántartások kialakítása, vezetésére felelős kijelölése,
- számon kérhetőség biztosítása (feladat és felelősségi körök egyértelmű meghatározása)
- 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.

2.2 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***:

Alaptevékenység államháztartási szakágazata:
841215 Szociális és jóléti szolgáltatások igazgatása

Alaptevékenység fő TEÁOR kódja:
8412 Egészségügy, oktatás, kultúra, egyéb szociális szolgáltatás igazgatása

Az adatvédelmi tisztviselő:

- neve: **Dr. Lengyel Levente Lajos**
- elérhetősége: info.nagycserkesz.adatvedelem@gmail.com
  +36 30/180 62 63

feladatai:

- közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
- tájékoztatást, szakmai tanácsod ad az adatkezelő vagy adatfeldolgozó, továbbá az adatkezelést végző Munkatársak részére kötelezettségeikkel kapcsolatban;
- ellenőrzi az Info tv., a GDPR, és az adatvédelemre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzat rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;
- kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére felhívja az Adatkezelő vagy az adatfeldolgozó figyelmét;
- elkészíti és folyamatosan karbantartja az Adatvédelmi Incidenskezelési Szabályzatot;
- közreműködik jelen szabályzat előkészítésében;
- felelős a számára kijelölt belső adatvédelmi nyilvántartások vezetéséért;
- gondoskodik az adatvédelmi ismeretek oktatásáról;
- az intézményvezető/aljegyző 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);
- együttműködik az adatkezelés jogszerűségével kapcsolatos eljárások lefolytatására jogosult szervekkel és személyekkel;
- köteles részt venni a NAIH által szervezett adatvédelmi konferenciákon;
- jogviszonyának fennállása alatt és annak megszűnését követően is titoktartási kötelezettsége van az adatvédelmi tisztviselőként tudomására jutott és kezelt személyes adatok, minősített adatok illetve a törvény által védett titoknak minősülő adatok tekintetében, melyek az adatkezelő vagy törvény előírásai szerint nem nyilvánosak.

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/aljegyzőt támogatnia kell:

- együttműködés és kapcsolattartás a felügyeleti hatósággal,
- adatvédelmi képzés és oktatás biztosítása a dolgozóknak,

- az érintettek megkeresésére tájékoztatás nyújtása arról, hogy az Intézmény 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 adatvédelmi incidens kivizsgálásával kapcsolatos részletes feladatait az „Adatvédelmi incidensek kezelésének eljárásrendje" tartalmazza.

Az adatvédelmi tisztviselő akadályoztatása esetén az adatvédelmi incidens bejelentését az aljegyzőnek kell bejelenteni az agota.lekli-szekely@nagycserkesz.hu **email címen.**

2.3 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.

2.4 A dolgozók általános felelősségei

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

Felhasználó (dolgozók) 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 bizalmasságának megfelelő kezeléséért, valamint a személyes használatba vett eszközök védelméért,
- tilos más felhasználó hozzáférési jogosultságainak használata,
- tilos az Intézmény számítógépére 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 dolgozó felelőssége, az intézményvezető előzetes tájékoztatását követően.

Amennyiben a dolgozó bizonytalan a helyes adatkezelés, vagy az adatvédelmi szempontok tekintetében, úgy köteles tanácsért az intézményvezetőhöz/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.

V. Adatfeldolgozók

Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel; (Rendelet 4. cikk 8.) Az adatfeldolgozó igénybevételéhez nem kell az érintett előzetes beleegyezése, de szükséges a tájékoztatása.

1. 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.

2. Az adatok adatfeldolgozó részére történő átadása

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

- könyvelő, a számviteli és az adózási kötelezettségek teljesítése,
- a bérszámfejtési feladatok elvégzése végett.

Az Intézmény minden esetben, valamennyi együttműködő partner tekintetében az adatok továbbításának megkezdése előtt meggyőződik arról, hogy az adott partner az Európai Uniós és magyarországi adatvédelmi szabályoknak megfelelően jár el. Az Intézmény valamennyi Partnerrel írásban az adatfeldolgozásra vonatkozó szerződést köt, melyben rögzítésre kerül:

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

3. Adatfeldolgozókra vonatkozó szabályok

Az intézményvezető megbízásából adatfeldolgozói tevékenységet végző természetes vagy jogi személyekre, illetve jogi személyiséggel nem rendelkező szervezetekre vonatkozó adatvédelmi kötelezettségek az adatfeldolgozóval kötött megbízási szerződésben érvényesítendők vagy annak kiegészítéseként az adatfeldolgozói megállapodásban.

Az adatfeldolgozó megállapodásban rögzíteni kell:

- az adatkezelést, amelybe az adatkezelő az adatfeldolgozót bevonta;
- az adatfeldolgozó által ellátott adatkezelői tevékenységet;
- az adatfeldolgozás időtartamát, jellegét és célját;
- az adatfeldolgozásra átadott adatok típusát;
- az adatfeldolgozással érintettek kategóriáit;
- az adatkezelő jogait és kötelezettségeit;
- az adatfeldolgozó jogait és kötelezettségeit.

Az Adatkezelő (intézményvezető/aljegyző) csak olyan adatfeldolgozóval köt szerződést adatfeldolgozói feladatra, aki a szerződésben vállalja, hogy:

- a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli;
- az általa személyes adatok feldolgozásában résztvevő személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;
- biztosítja a GDPR 32. cikk szerinti adatbiztonsági szabályokat;
- adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vesz igénybe;
- az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az Adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;
- adatvédelmi incidens esetén az incidens tudomására jutása pillanatában azonnal értesíti az Adatkezelő képviselőjét, adatvédelmi tisztviselőt és együttműködik az adatvédelmi incidens kezelésében;
- az adatfeldolgozási szolgáltatás nyújtásának befejezését követően az Adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az Intézményhez, valamint a személyes adatokról készült másolatokat ezzel egyidőben megsemmisíti vagy törli;
- lehetővé teszi a GDPR 30.cikk (2) bekezdése szerinti adatfeldolgozói nyilvántartást.

4. Adatfeldolgozók főbb adatai

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
szervezet neve	**Róka Zoltánné ev.**
e-mail cím	rone7408@gmail.com
adatfeldolgozás célja	könyvviteli adatfeldolgozás
szervezet neve	**Keczkó Amália ev.**
e-mail cím	keczk.amalia@gmail.com
adatfeldolgozás célja	könyvviteli adatfeldolgozás

Az Intézmény szervezetén kívül, külső adatfeldolgozó részére adatkezelés céljából a szakmai dokumentációk kezelése során az érintettre vonatkozó személyes adatok nem kerülnek átadásra.

VI. ADATBIZTONSÁGI SZABÁLYOK

1. Adatbiztonság követelménye:

- Személyes adatokat is tartalmazó iratot az Intézmény hivatalos helyiségeiből 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 dolgozóján 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, adatvédelmi hatóság, ellenőrző szerv az ellenőrzés tárgyával kapcsolatosan). Az érintett, vagy képviselője betekintési jogának gyakorlása során úgy kell eljárni, hogy ez által mások jogai ne sérülhessenek (a más személyre vonatkozó személyes adatot 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. A napközbeni munkavégzés során munkáját úgy kell végeznie, hogy a személyes adatokat tartalmazó dokumentumokba illetéktelen személy ne tekinthessen be.

2. Informatikai és fizikai védelem

Az Intézmény az alábbi informatikai védelmi eszközöket és módokat alkalmazza:

- fizikai védelem
  - zárható iroda
  - zárható szekrények
  - riasztó
  - kamera a folyosókon (vagyonvédelem végett)
  - „tiszta asztal-tiszta monitor elv” érvényesítése

- IT védelem
  - tűzfal
  - vírusírtó
  - biztonsági mentések
  - szabályozott hozzáférési jogosultságok
  - jelszavas, illetve személyi igazolványos belépés a programokba
  - képernyőzár.

2.1 Informatikai védelmi intézkedések az informatikai nyilvántartások tekintetében az adatbiztonság megvalósulásához:

- az adatkezelés során használt számítógépek az Adatkezelő tulajdonát képezik;
- a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal lehet csak hozzáférni, a jelszavak cseréjéről az informatikai biztonsági felelős/rendszergazda rendszeresen gondoskodik;
- az adatokkal történő minden számítógépes rekord nyomon követhetően naplózásra kerül;
- a hálózati kiszolgáló gépen (szerveren) tárolt adatokhoz csak az informatikai biztonsági felelős/rendszergazda férhet hozzá;
- a hálózaton tárolt adatok biztonsága érdekében mentésekkel, archiválásokkal kell elkerülni az adatvesztést;
- a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodik az Adatkezelő;

Az Adatkezelő az informatikai biztonsági intézkedéseinek érvényre jutását az informatikai biztonsági felelős vagy rendszergazda által valósítja meg.

2.2 Adatszivárgás megelőzésének biztosítása

Az adatszivárgás megelőzése érdekében az alábbi intézkedéseket kell végrehajtani:

- indokolt esetben a személyes adatok 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 hozzáférésből felmerülő kockázatok azonosítására és azok súlyának az általuk okozható kár meghatározására.

Felelősök: ***folyamatgazdák, informatikai biztonsági felelős/rendszergazda***

A szabályzatok és nyilvántartások elkészítését követőn indokolt egy IT biztonsági elemzés. felelős: ***informatikai biztonsági felelős/rendszergazda***

IT biztonsági elemzés keretében:

- sérülékenység vizsgálat
- informatikai infrastruktúrával szemben támasztandó követelmények
- IT biztonsági elvárások
- folyamati szabályozások
- hozzáférés kockázatainak csökkentésére javaslatok kidolgozása
- IT biztonsági kockázat elemzés
- IT fejlesztési terv

3. Adattárolás

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

3.1 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 meg kell megsemmisíteni, amikor a kinyomtatás oka megszűnik, illetve több példány került kinyomtatásra, mint amennyi a feladat elvégzéséhez szükséges.

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).

3.2 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 tűzfallal és vírusirtóval védeni.
- Az adattárolásra alkalmazott szoftvereket rendszeresen frissíteni szükséges, az olvashatóságot ellenőrizni kell.

3.3 Postai küldeményekre vonatkozó speciális szabályok

Adatvédelmi és adatbiztonsági szempontból biztosítani kell, hogy illetéktelen személy ne vehessen át postai küldeményt.
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.

4. 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.

<u>Nyilvántartási célú adatkezelés</u>:

- az adatkezelővel munkavégzésre irányuló jogviszonyban álló személyek személyes adataival,
- közszolgáltatás ellátásához kapcsolódóan az ingatlanhasználók, szolgáltatást igénybe vevők, díjhátralékosok 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.

5. 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.

6. 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.

VII. Az érintett személy jogai

1. Tájékoztatáshoz való jog

1.1 Az érintett tájékoztatása az adat felvételéhez kapcsolódóan

Abban az esetben, amennyiben az adatkezelés során a személyes adatokat az Intézmény közvetlenül az érintettől szerzi meg, úgy a személyes adatok megszerzésének időpontjában alábbiakról tájékoztatja az érintettet:

- az adatkezelő pontos megnevezése, elérhetőségei
- az adatvédelmi tisztviselő neve, elérhetőségei
- az adatkezelés célja
- az adatkezelés jogalapja
- amennyiben az adatkezelés célja az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítése, úgy annak közlése
- amennyiben a személyes adatokat az Adatkezelő harmadik fél számára átadja, a személyes adatok címzettjei, illetve a címzettek kategóriái
- a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,
- az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat a személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való joga
- a hozzájárulás visszavonására irányuló jog gyakorlásának szabályai, amennyiben az adatkezelés jogalapja az érintett hozzájárulása
- a Nemzeti Adatvédelmi és Információszabadság Hatósághoz címzett panasz benyújtásának jogáról
- annak ténye, hogy a személyes adat kezelése, szolgáltatása jogszabályon, szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele és az érintett köteles-e a személyes adatokat megadni, valamint a lehetséges következmények, amennyiben az érintett személyes adatait nem adja meg
- az automatizált döntéshozatal ténye, valamint legalább az ennek során alkalmazott logika és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

Amennyiben a személyes adatot nem közvetlenül az érintettől szerzi meg az Adatkezelő, úgy az érintettet tájékoztatni kell fent felsoroltakon kívül a személyes adat forrásáról, annak jogszabályi előírásáról, a személyes adat megszerzésének időpontjáról.

1.2 Tájékoztatás időpontja

<u>Nem közvetlenül az érintettől beszerzett személyes adatok esetében:</u>

- a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül,
- ha az Adatkezelő a személyes adatokat az érintettel való kapcsolattartás céljára használja, az érintettel való első kapcsolatfelvétel alkalmával,

- ha az Adatkezelő az adatokat várhatóan más címzettel is közli, legkésőbb a személyes adatok első alkalommal történő továbbításakor.

Amennyiben nem közvetlenül az érintettől szerzi meg az Adatkezelő a személyes adatokat, nem kell tájékoztatni az érintettet, ha:

- az érintett már rendelkezik az ezen pontokba foglalt információkkal,
- a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényelne,
- az adat megszerzését vagy közlését kifejezetten előírja uniós vagy hatályos magyar jog, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről is rendelkezik,
- a személyes adatoknak valamely uniós vagy a hatályos magyar jogban előírt szakmai titoktartási kötelezettség alapján bizalmasnak kell maradnia.

Az Intézmény a személyes adatokkal kapcsolatos átlátható, előzetes tájékoztatási kötelezettségének „Adatkezelési tájékoztatókban” tesz eleget.

1.3 A tájékoztatók nyilvánosságra hozatalának szabályai:

- a tájékoztatónak minden esetben az adatkezelés megkezdése előtt az érintett számára megismerhetőnek kell lennie,
- minden olyan folyamat során, amikor az adat felvétele papíralapon történik, az adat felvételének helyén elérhetőnek kell lennie az adott tájékoztatónak,
- minden olyan folyamat során, amikor az adat felvétele technikai eszköz útján történik, a technikai eszköz segítségével elérhetőnek kell lennie a tájékoztatónak,
- amennyiben feltételezhető, hogy az érintett maga fogja kezdeményezni az adatkezelést, ezen adatkezelések tájékoztatójának elérhetőknek kell lenniük az Intézmény honlapján az érintett előzetes tájékoztatása érdekében,
- a tájékoztatót úgy kell nyilvánosságra hozni, hogy az Intézmény (mint adatkezelő) minden esetben bizonyítani tudja, hogy az érintett azokat az adatkezelés megkezdése előtt megismerhette.

2. Az „érintettek hozzáférési jogai”

<u>Valamennyi érintett, akinek a személyes adatait kezelik jogosult:</u>

- 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:
<u>hozzájáruláson alapuló adatkezelés esetén</u>

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

3. A helyesbítéshez való jog

Az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat.

Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését is.
Ezen szabályokat a Rendelet 16. cikke tartalmazza.

<u>Az adatok helyesbítéséhez való jog biztosítása</u>

- 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 feladatot/munkafolyamatot végző dolgozó felelős, az aljegyző előzetes tájékoztatása mellett.

4. A törléshez való jog („az elfeledtetéshez való jog”)

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje ha

- a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
- az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- az érintett tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,
- a személyes adatokat jogellenesen kezelték;
- a személyes adatok gyűjtésére közvetlenül az ellátottnak kínált, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

A törléshez való jog nem érvényesíthető, ha az adatkezelés szükséges

- a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;
- az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;
- a népegészségügy területét érintő közérdek alapján;
- a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben a törléshez való jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést; vagy
- jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

A törlés szükségességének felismerése az ügyintéző feladata, aki azt- amennyiben a törlés szükségessége tekintetében bizonytalan- köteles az aljegyzőnek 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 iratselejtezési eljárásrend szerint kell lefolytatni. A személyes adatokat tartalmazó egyéb iratok megsemmisítéséről szintén a szükséges biztonsági intézkedések mellett kell gondoskodni.

5. Az adatkezelés korlátozásához való jog

Az adatkezelés korlátozása esetén az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

Az érintett jogosult arra, hogy kérésére az Adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

- 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;

- az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és e helyett kéri azok felhasználásának korlátozását;
- az Adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
- 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 adatkezelés korlátozásának feloldásáról az érintettet előzetesen tájékoztatni kell.
- A vonatkozó szabályokat a Rendelet 18. cikke tartalmazza.

A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség:
Az adatkezelő minden olyan címzettet tájékoztat valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.
E szabályok a Rendelet 19. cikke alatt találhatók.

6. Az adathordozhatósághoz való jog

A Rendeletben írt feltételekkel az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha

- az adatkezelés, hozzájáruláson vagy szerződésen alapul; és
- az adatkezelés automatizált módon történik.

Az érintett kérheti a személyes adatok adatkezelők közötti közvetlen továbbítását is.

Az adathordozhatósághoz való jog gyakorlása nem sértheti a Rendelet 17. cikkét (A törléshez való jog („az elfeledtetéshez való jog”).
Az adtahordozhatósághoz való jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges. E jog nem érintheti hátrányosan mások jogait és szabadságait.
A részletes szabályokat a Rendelet 20. cikke tartalmazza.

7. A tiltakozáshoz való jog

Az Érintett jogosult arra, hogy bármikor tiltakozzon személyes adatinak kezelése ellen, ha

- a személyes adatok kezelése kizárólag az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez, vagy az Adatkezelő, vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, ideértve az e célból történő profilalkotást is,

- az adatkezelés célja közvetlenül üzletszerzés – ideértve az ehhez kapcsolódó profilalkotást is -,
- az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.

Az Adatkezelő az érintett tiltakozásának jogszerűségét megvizsgálja, és ha a tiltakozása megalapozott, az adatkezelést megszünteti és a kezelt személyes adatokat indokolatlan késedelem nélkül törli,
kivéve:

- ha az Adatkezelő megindokolt válaszában előadja, hogy az adatkezelést olyan kényszerítő erejű jogos érdek indokolja, amely bizonyos korlátozott körben elsőbbséget élvez az érintett érdekeivel, jogaival és szabadságával szemben,
- ha a személyes adatok kezelése jogi igények előterjesztéséhez vagy védelméhez kapcsolódnak.

Tiltakozás érvényesítése esetén a tiltakozásról és az annak alapján tett intézkedésekről az Adatkezelő értesíti mindazokat, akik részére a tiltakozással érintett személyes adatok korábban továbbításra kerültek, kivéve, ha ezen lépések megtétele a tudomány és technológia állása és a megvalósítás költségeire tekintettel lehetetlen vagy jelentősen nagy nehézségeket telepítene az Adatkezelőre.

8. Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

Ez a jogosultság nem alkalmazandó abban az esetben, ha a döntés:

- az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges;
- az érintett kifejezett hozzájárulásán alapul.

Az előbbi esetekben az adatkezelő köteles megfelelő intézkedéseket tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek legalább azt a jogát, hogy az adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.
A további szabályokat a Rendelet 22. cikke tartalmazza.

9. Korlátozások

Az adatkezelőre vagy adatfeldolgozóra alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel korlátozhatja jogok és kötelezettségek (Rendelet 12-22. cikk, 34. cikk, 5. cikk) hatályát, ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát.
E korlátozás feltételeit a Rendelet 23. cikke tartalmazza.

10. A felügyeleti hatóságnál történő panasztételhez való jog (hatósági jogorvoslathoz való jog)

Az érintett jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál – különösen a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban –, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti a Rendeletet. Az a felügyeleti hatóság, amelyhez a panaszt benyújtották, köteles tájékoztatni az ügyfelet a panasszal kapcsolatos eljárási fejleményekről és annak eredményéről, ideértve azt is, hogy az ügyfél jogosult bírósági jogorvoslattal élni.
E szabályokat a Rendelet 77. cikke tartalmazza.

A felügyeleti hatóság elérhetőségei:

Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)

- elektronikus úton a Hatóság elektronikus levelezési címén, az
  e-mail cím: ***ugyfelszolgalat@naih.hu***
  Hivatali tárhely rövid neve: **NAIH**
  Hivatali kapu azonosítója (KR ID): **429616918**

- írásban a Hatóság postacímén (***1055 Budapest, Falk Miksa u 9-11.***), továbbá telefonon ügyfélszolgálati napokon, ügyfélszolgálati időben – kedden és csütörtökön – 9:00-16:00 és pénteket 9:00-14:00 óra között
  +36 (30) 683-5969
  +36 (30) 549-6838 telefonszámon.

11. A felügyeleti hatósággal szembeni hatékony bírósági jogorvoslathoz való jog

Az egyéb közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben.

Az egyéb közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden érintett jogosult a hatékony bírósági jogorvoslatra, ha az illetékes felügyeleti hatóság nem foglalkozik a panasszal, vagy három hónapon belül nem tájékoztatja az érintettet a benyújtott panasszal kapcsolatos eljárási fejleményekről vagy annak eredményéről.

A felügyeleti hatósággal szembeni eljárást a felügyeleti hatóság székhelye szerinti tagállam bírósága előtt kell megindítani.

Ha a felügyeleti hatóság olyan döntése ellen indítanak eljárást, amellyel kapcsolatban az egységességi mechanizmus keretében a Testület előzőleg véleményt bocsátott ki vagy döntést hozott, a felügyeleti hatóság köteles ezt a véleményt vagy döntést a bíróságnak megküldeni.
E szabályokat a Rendelet 78. cikke tartalmazza.

12. Az adatkezelővel vagy az adatfeldolgozóval szembeni hatékony bírósági jogorvoslathoz való jog

A rendelkezésre álló közigazgatási vagy nem bírósági útra tartozó jogorvoslatok – köztük a felügyeleti hatóságnál történő panasztételhez való jog – sérelme nélkül, minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak e rendeletnek nem megfelelő kezelése következtében megsértették az e rendelet szerinti jogait.

Az adatkezelővel vagy az adatfeldolgozóval szembeni eljárást az adatkezelő vagy az adatfeldolgozó tevékenységi helye szerinti tagállam bírósága előtt kell megindítani. Az ilyen eljárás megindítható az érintett szokásos tartózkodási helye szerinti tagállam bírósága előtt is, kivéve, ha az adatkezelő vagy az adatfeldolgozó valamely tagállamnak a közhatalmi jogkörében eljáró közhatalmi szerve.
E szabályokat a Rendelet 79. cikke tartalmazza.

VIII. Adatkezelésről tájékoztatás

1. 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.

2. 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 adatvédelmi tisztviselő feladata, aki azt- amennyiben a törlés szükségessége tekintetében bizonytalan- köteles az intézményvezetőnek/aljegyzőnek 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 iratselejtezési 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/aljegyző előzetes tájékoztatása mellett.

Az adatkezelés korlátozásához való jog biztosítása

- Az adatkezelő biztosítja, hogy az érintettek megfelelő tájékoztatás alapján és befolyásmenetesen 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.

IX. 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.

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.

1. Hozzájáruláson alapuló adatkezelés

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.

Különleges szabályok: önkéntesnek, konkrétnak, tájékoztatáson alapulónak és egyértelműnek kell lennie. Az Adatkezelő biztosítja, hogy az Érintett a hozzájárulását bármikor visszavonhassa.

Önkéntes: a hozzájárulás akkor önkéntes, ha az Érintettnek tényleges választási lehetősége áll fenn a hozzájárulás megadása vagy meg nem adása közötti döntés meghozatala során.

Konkrét: akkor, ha az egy meghatározott adatkezeléshez kapcsolódik, pontosan meghatározza az adatkezelés célját, hozzájárulást a konkrétan meghatározott adatkezelési célhoz kér, valamint világosan elválasztja a személyes adatok kezeléséhez való hozzájárulás kérést valamennyi más információtól.

Tájékoztatáson alapul: ahhoz, hogy a tájékoztatáson alapulónak minősüljön, az érintettnek legalább tisztában kell lennie az adatkezelő kilétével és a személyes adatok kezelésének céljával.

Egyértelmű: ha az Érintett egyértelműen kifejezi, hogy hozzájárul a személyes adatainak kezeléséhez erre vonatkozó nyilatkozatban vagy más egyértelműen hozzájárulásként azonosítható cselekedettel.

2. 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.
Csak akkor alkalmazható ez a jogalap, ha a szerződés egyik szerződő fele az érintett.

3. Jogi kötelezettség teljesítéséhez szükséges adatkezelés

Amennyiben az adatkezelés jogalapja a jogi kötelezettség, úgy e jogi kötelezettséget csak és kizárólag Európai Unió vagy Magyarország hatályos és alkalmazandó jogszabályának kell megállapítania.
Jogi kötelezettséget állapíthat meg önkormányzati rendelet is.
A kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.

4. Az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges adatkezelés:

A jogos érdekből alkalmazott jogalap esetén az adatkezelés megkezdése előtt az érintettek magánszférájának, érdekeinek és alapvető jogainak biztosítása érdekében érdekmérlegelési tesztet kell elvégezni. A konkrét adatkezelési folyamat során az Adatkezelő megfelelő tájékoztatást nyújt az érintettek számára az adatkezelés jogalapjáról.
Jelen jogalapot a szükségesség-arányosság elve alapján alkalmaz

5. Az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges adatkezelés

6. Közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges adatkezelés

X. Adatvédelmi incidens kezelése

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 (Rendelet 4. cikk 12.).

1. Incidens észlelése, jelentése

Az adatkezelő dolgozója, együttműködő Partnere adatvédelmi incidens esetén azonnal köteles értesíteni az adatvédelmi tisztviselőt, akinek haladéktalanul vizsgálatot kell indítania az incidens kockázatának felmérésére. Indokolt esetben az informatikai biztonsági felelőst/rendszergazdát 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 tisztviselő az eljárásrendben foglaltak szerint kivizsgálja és értékeli a bejelentett incidenst, és tájékoztatja az Adatkezelőt (intézményvezetőt).

A bejelentett adatvédelmi incidensekről nyilvántartást kell vezetni.
Felelős: ***adatvédelmi tisztviselő***

2. Az érintett tájékoztatása az adatvédelmi incidensről

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelőnek indokolatlan késedelem nélkül tájékoztatnia kell az érintettet az adatvédelmi incidensről.

E tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a következőket:

- az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

- az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
- az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

A további szabályokat a Rendelet 34. cikke tartalmazza.

Az adatvédelmi incidens esetén követendő eljárásrendről az Intézmény külön szabályzattal rendelkezik. (Adatvédelmi incidens kezelési szabályzat)

XI. Adatvédelem szervezeti rendje

1. Az Intézmény adatvédelmi szervezete

- adatkezelő (képviselője: intézményvezető)
- adatvédelmi tisztviselő (DPO) (intézményvezető által kijelölt vagy megbízott szermély)
- informatikai biztonsági felelős (IBF), rendszergazda
- belső kontrollrendszer folyamatgazdái
- dolgozók (teljes foglalkoztatotti állomány)
- adatfeldolgozók (Kirendeltség, MÁK, megbízott könyvelő)

2. Szervezési és műszaki intézkedések, kontrollok kialakítása

Intézkedési terv készítése, végrehajtás nyomon követése

- helyzetfelmérés, auditálás
- meglévő szabályzatok felülvizsgálata, kiegészítése az adatvédelmi és adatbiztonsági feladatokkal
- új (adatvédelemmel kapcsolatos) szabályzatok elkészítése, feladatok és felelősök meghatározása
- adatvédelmi tisztviselő kijelölése, bejelentése a hatósághoz
- adatvagyon-leltár elkészítése
- adatkezelési tájékoztatók elkészítése (adatkezelési célonként)
- informatikai biztonsági fejlesztések (hardver, szoftver fejlesztés)
- nyilvántartási rendszer kialakítása, vezetéséért felelős kijelölése

Felelősök - kontrolltevékenységek

intézményvezető – felülvizsgálati-, jóváhagyó kontroll
(információ begyűjtésének elrendelése, felelősök kijelölése, a kész adatvagyon leltár felülvizsgálata, jóváhagyása)
belső kontrollrendszer folyamatgazdái – felülvizsgálati kontroll

(információk biztosítása – saját folyamatainak áttekintése, annak érdekében, hogy hol kezelnek személyes adatokat)
iratkezelésért felelős – felülvizsgálati, egyeztető kontroll
(adattisztítás elvégzéséhez a vonatkozó jogszabálynak megfelelő őrzési idő felülvizsgálata, meglévő dokumentumok – személyes adatot tartalmazó – egyeztetése, felülvizsgálata)
adatkezelést végző munkatársak – egyeztető-, felülvizsgálati kontroll
(egyezteti, felülvizsgálja a bekért adatokat – pontosság, célhoz kötöttség szempontjából)
adatvédelmi tisztviselő – felülvizsgálati kontroll

3. 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***
- monitoring vizsgálat – ***belső ellenőr***

4. Beszámoltatás rendje

Adatvédelmi tisztviselő köteles folyamatosan tájékozódni az adatvédelmi jogszabályokról, az Intézmény folyamatairól. Egyeztet a megfelelésért felelőssel.

- Az adatvédelmi rendszerről félévente jelentés formájában köteles az intézményvezető részére beszámolni. A jelentés elkészítésének és megküldésének határideje minden év június 30. és december 31.
- Adatvédelmi incidensekről az incidenskezelési szabályzatban foglaltak szerint van beszámolási és tájékoztatási kötelezettsége az intézményvezető felé.

Rendszergazda: köteles az informatikai rendszer (hardver, szoftver) állapotáról, biztonsági megfelelőségéről beszámolni az intézményvezetőnek/aljegyzőnek és az adatvédelmi tisztviselőnek.

- a beszámolás formája: tájékoztató levél,
- gyakorisága: negyedévente *(minden év március 31., június 30., szeptember 30., december 31.).*

Az ellenőrzési feladatokat ellátók (3.pontban meghatározottak) a felülvizsgálat, a vezetői kontroll eredményéről írásban tájékoztatni kötelesek az intézményvezetőt.

5. Adatvédelmi oktatás, ismeretmegújítás

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

felelős: **adatvédelmi tisztviselő**
határidő: minden év április 30-ig

Az oktatásokról nyilvántartást kell vezetni, melyeben az oktatás címét/tárgyát és a résztvevő dolgozókat fel kell tüntetni.

6. Adatvédelemi és adatbiztonság szabályozása

Az Európai Parlament és Tanács (EU) 2016/679 Rendeletének (GDPR) megfelelve az ***Adatvédelmi és adatbiztonsági szabályzaton*** túl az alábbi belső szabályzatok, mérlegelési dokumentumok kerültek kialakításra az Intézménynél:

- Adatkezelési szabályzat
- Adatvédelmi incidenskezelési szabályzat
- Kameraszabályzat
- Nyilvántartások vezetésének szabályzata (feladatok, felelősök)
- Informatikai Biztonsági Szabályzat
- Adatvédelmi tisztviselő kijelölésének szükségességét mérlegelő dokumentum
- Adatvédelmi hatásvizsgálat elvégzésének szükségességét mérlegelő dokumentum
- Érdekmérlegelési teszt szempontjainak meghatározása

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

- adatkezelési tájékoztatók adatkezelési célonként (feladatellátáshoz kapcsolódóan)
- az Intézménnyel foglalkoztatási jogviszonyban állók, és az Intézmény által nyújtott szolgáltatást igénybevevők tájékoztatása a személyes adatok kezeléséről
- érintett hozzájáruló nyilatkozata
- dolgozók hozzájárulása a foglalkoztatási jogviszonnyal nem kötelezően összefüggő adatkezeléshez
- egyéb szervezeti sajátosságnak megfelelően kialakított dokumentumok.

7. 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 Intézmény által üzemeltetett honlapon való adatok kezelésének és védelmének részletes eljárási rendjét a **Honlap Szabályzata** tartalmazza.

- A papír alapú, személyes adatokat is tartalmazó dokumentumok, ügyiratok adatvédelmével, biztonságával kapcsolatos eljárásokat az **Iratkezelési Szabályzat** tartalmazza.

8. Nyilvántartások

A személyes adatok kezelésével kapcsolatosan az alábbi nyilvántartásokat kell vezetni:

a) adatkezelési tevékenységek nyilvántartása
b) adatvédelmi incidensek nyilvántartása
c) adattovábbítás nyilvántartása
d) belső adatvédelmi oktatások nyilvántartása
e) adatfeldolgozók nyilvántartása
f) érintetti hozzájárulás nyilvántartása
g) az érintett hozzáférési jogával kapcsolatos intézkedések nyilvántartása

Adatvédelmi nyilvántartások szabályzat részletesen rögzíti az egyes nyilvántartások tartalmi elemeit, nyilvántartást vezető személyt, nyilvántartáshoz hozzáférési jogosultsággal rendelkezőket, nyilvántartás vezetésének gyakoriságát, felülvizsgálat határidejét, vezetői ellenőrzésre jogosult személyt, egyéb.

adatkezelési tevékenységek nyilvántartása (adatkezelési célonként, adatforrás, adatkörök, címzettek, adatkezelés időtartama, adatbiztonsági intézkedések)

- munkavállalók személyes adatkezelése
- vendég étkeztetési szolgáltatás
- folyékony hulladékszállítási szolgáltatás
- könyvtári és közművelődési szolgáltatások
- ingatlan bérbeadás
- temetkezési nyilvántartások
- helyi újság – lapkiadással kapcsolatos feladatok, hirdetés szervezés
- iratkezelés
- közérdekű adat igénylés
- munkahelyi ellenőrzések
- panaszkezelés
- elektronikus megfigyelőrendszer (kamera) miatti személyes adatkezelés (ügyfelek)
- rendezvények szervezése miatti adatkezelés
- online, elektronikus kapcsolatfelvétel
- ügyféladatok, szerződésen alapuló adatkezelés

érintetti hozzájárulás nyilvántartás

- az Intézmény által szervezett, meghirdetett rendezvények, programok dokumentálása és nyilvánosságra hozatala

- a foglalkoztatási jogviszonnyal nem kötelezően összefüggő adatkezelés
- egyéb hozzájárulás alapján kezelt személyes adatok

adatfeldolgozók nyilvántartása (az Intézmény, mint adatkezelő megbízása alapján külsős szolgáltatókról vezetett nyilvántartás – a megbízott olyan feladatot lát el, mely során személyes adatokat is kezel -)

adatvédelmi incidensek nyilvántartása (a bejelentett, feltárt adatvédelmi incidensek kivizsgálását követően nyilvántartásba kell venni az incidenssel kapcsolatos adatokat)

adatok hozzáféréséről nyilvántartás (hozzáférési jogosultságokról vezetett nyilvántartás)

adattovábbítás nyilvántartása (a továbbított adatokról, címzettekről vezetett nyilvántartás)

az érintett hozzáférési jogával kapcsolatos intézkedések nyilvántartása

belső adatvédelmi oktatások nyilvántartása (oktatás időpontjáról és tárgyáról, résztvevőkről vezetett nyilvántartás)

Nyilvántartások vezetéséért felelősök:

- Adatkezelések nyilvántartása (adatvagyon leltár) (felelős: folyamatgazdák)
- Adatkezeléshez való hozzájárulások nyilvántartása (felelős: titkárságvezető)
- Adatvédelmi incidensek nyilvántartása (felelős: adatvédelmi tisztviselő)
- Adatfeldolgozók nyilvántartása (felelős: gazdasági igazgató helyettes)
- Adatok hozzáféréséről nyilvántartása (felelős: informatikai biztonsági felelős)
- az érintett hozzáférési jogával kapcsolatos intézkedések nyilvántartása (felelős: adatvédelmi tisztviselő)
- adattovábbítás nyilvántartása (felelős: gazdasági igazgató helyettes)

9. 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, legkésőbb 30 napon belül.
felelős: ***intézményvezető***

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 korábbitól 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.

Az Adatvédelmi és adatbiztonsági szabályzat hatályba lépésének dátuma: **2025. január 01.**
A szabályzatot változást követő 30 napon belül, de legalább évente egy alkalommal felül kell vizsgálni, a módosítások át kell vezetni.

A szabályzat megismertetése és a honlapon való közzététel az intézményvezető felelőssége.

Nagycserkesz, 2025. január 20.

Körömöndi Judit
intézményvezető