BELSŐ ADATKEZELÉSI ÉS ADATBIZTONSÁGI SZABÁLYZAT

Szentesi Családsegítő Központ

Jelen szabályzat az intézmény 2013.11.01-én hatályba lépett, valamint 2015.05.14-én és 2017.10.01-én módosított Adatkezelési Szabályzatának ismételten felülvizsgált és a mai napra aktualizált szabályzatának tekintendő.

Hatályos

2020.03.01.

Felülvizsgálandó: Szükség szerint, de legkésőbb 2022.02.28-ig.

…….

Gál Antal

igazgató

Tartalom

I. Jogszabályi háttér, alkalmazandó jog

A Szentesi Családsegítő Központ (továbbiakban: Intézmény) Adatvédelmi és Adatbiztonsági szabályzata rendelkezéseinek alapjául különösen az alábbi jogszabályok szolgáltak:

1) 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 az Európai Parlament és a Tanács 2016/679 rendelete (Általános adatvédelmi rendelet)
2) az információs önrendelkezési jogról és az információ szabadságról szóló 2011. évi CXII. törvényben (továbbiakban: Infotv.)
3) a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény (továbbiakban: Gyvt.),
4) a szociális igazgatásról és szociális ellátásokról szóló 1993. évi III. törvény (továbbiakban: Szt.),
5) a személyes gondoskodást nyújtó gyermekjóléti, gyermekvédelmi intézmények, személyek szakmai feladatairól és működésük feltételeiről szóló 15/1998. (IV. 30.) NM (továbbiakban: NMr.)
6) a személyes gondoskodást nyújtó szociális intézmények szakmai feladatairól és működésük feltételeiről szóló 1/2000. (I. 7.) SzCsM rendelet
7) a gyámhatóságok, a területi gyermekvédelmi szakszolgálatok, a gyermekjóléti szolgálatok és a személyes gondoskodást nyújtó szervek és személyek által kezelt személyes adatokról szóló 235/1997. (XII. 17.) Korm. rendelet
8) a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény,
9) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény,
10) a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény
11) szakmai szabályzók, útmutatók protokollok
12) Szociális Munka Etikai Kódexe

II. Általános rendelkezések

1. Az adatvédelmi és adatbiztonsági szabályzat célja, rendeltetése

1.1. A Szentesi Családsegítő Központ elismeri a természetes személyek személyes adataik kezelésével összefüggő védelemhez való jogot alapvető jogként, összhangban az Európai Unió Alapjogi Chartája (Charta) 8. cikkének (1) bekezdésével és az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikkének (1) bekezdésével, mely rögzíti, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.

1.2. A személyes adatok védelméhez való jog azonban nem abszolút jog, azt az arányosság elvével, a jelen szabályzat és a mindenkor hatályos jogszabályokkal összhangban, a társadalomban betöltött szerepének függvényében kell figyelembe venni, egyensúlyban más alapvető jogokkal.

1.3. A természetes személyek következetes és magas szintű védelmének biztosítása érdekében a természetes személyeknek a személyes adatok kezelésével összefüggésben fennálló jogait és szabadságait védelemben kell részesíteni, melynek megvalósítása érdekében szükséges intézményi feladatokat jelen szabályzat foglalja össze.

1.4. Jelen szabályzat célja, hogy az Intézményben kezelt adatokra megfelelő, egységes eljárást alakítson ki, valamint biztosítsa az adatok nyilvántartásának törvényes rendjét, az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését.

1.5. A szabályzat célja továbbá az adatkezelésben érintett személyek egyértelmű és részletes tájékoztatása az adatok kezeléséhez tartozó minden tényről, különösen az adatkezelés céljairól és jogalapjáról, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg a kezelt adatokat.

1.6. A szabályzat célja az is, hogy az Intézmény használatában lévő, illetve általa működtetett információ technológiai (továbbiakban IT) rendszerek védelmét, valamint az IT rendszerekkel kezelt adatok bizalmasságát, hitelességét, sérthetetlenségét, rendelkezésre állását a fenyegető veszélyekkel szemben a lehető legnagyobb mértékben biztosítsa.

1.7. A cél megvalósulása, valamint az érintettek alapvető jogainak érvényesülése érdekében az adatkezelés összes körülményéhez, így különösen céljához, továbbá az adatkezelés által fenyegető kockázatokhoz igazodó műszaki és szervezési intézkedéseket tesz, melynek keretében az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 25/A. § (3) bekezdése szerinti jelen szabályzatot alkotott, melynek integráns részét képezi az Európai Parlament és a Tanács 2016/679 rendelete (Általános Adatvédelmi rendelet) 12. cikkében foglaltaknak való megfelelés érdekében kiadott tájékoztatók.

1.8. A jelen szabályzat és adatvédelmi tájékoztató információt ad

- a Szentesi Családsegítő Központ által alkalmazott adatvédelmi és adatbiztonsági szabályokról, megtett intézkedésekről,
- az érintettnek az adatkezelés megkezdése előtt a jogairól, az adatkezelés céljáról, jogalapjáról, a kezelt adatok köréről, az adatokat megismerő személyekről, az adatok őrzésének idejéről, az érintettek jogairól, az igényérvényesítés útjáról,
- az adatvédelmi incidenskezelésről,
- a személyes adatok kezelésével kapcsolatos panasz előterjesztésének módjáról, a panaszkezelés folyamatáról, jogorvoslatról,
- az adattovábbításokról,

azaz az érintett teljes és valós képet kap a megadott személyes adatok kezelésének teljes folyamatáról a felvételtől a törlésig, míg az intézmény adatkezelési szempontú működésének alapjául szolgál.

1.9. Jelen szabályzat külön rögzíti az adatvédelmi elveket, amelyeket a Szentesi Családsegítő Központ jelen szabályzat elfogadásával is kötelezőnek ismer el magára nézve és felelősséget vállal arra, hogy tevékenysége megfelel a jelen tájékoztatóban és a hatályos jogszabályokban meghatározott jogi normáknak.

2. A belső adatvédelmi és adatbiztonsági szabályzat hatálya és módosítása

2.1. Tárgyi és időbeli hatály

2.1.1. A jelen tájékoztató hatálya Szentesi Családsegítő Központ, mint adatkezelő által végzett adatkezelési tevékenységre terjed ki a kiadás napjától kezdődően, annak visszavonásáig

2.1.2. Jelen adatkezelési szabályzat hatályon kívül helyezi Szentesi Családsegítő Központ valamennyi korábbi adatkezelési szabályzatát, belső utasítást. Adatkezelési tevékenységet az intézmény a továbbiakban jelen adatkezelési szabályzat alapján végez.

2.2. Az adatkezelő adatai

Név	**Szentesi Családsegítő Központ**
Székhely	6600 Szentes, Ady Endre u. 10.
Adószám	16684801-2-06
Telefon	+3663-561-510; +3663-561-520
Email	info@cssk-szentes.hu; igazgató: galantal@cssk-szentes.hu; CsGyK: laszlogyongyi@cssk-szentes.hu; CsGySz: levaine@cssk-szentes.hu
Telephely 1	Szentesi Családsegítő Központ **Gyermekek Átmeneti Otthona**
Cím	6600 Szentes, Munkácsy Mihály u. 3
Telefon, Email	+3663-444-500; gyao@cssk-szentes.hu
Telephely 2	Szentesi Családsegítő Központ **Családok Átmeneti Otthona**
Cím	6600 Szentes, Koszta József u. 7
Telefon, Email	+3663-444-600; csao@cssk-szentes.hu
Telephely 3	Szentesi Családsegítő Központ **Dózsa-ház Közösségi Tér**
Cím	6600 Szentes, Csongrádi út 2.
Telefon, Email	+3663-444-700; kozter@cssk-szentes.hu
Telephely 4	**Szentes Városi Üdülő - Szigliget**
Cím	Szigliget, Külsőhegyi út 66, 8264
Telefon, Email	+3687-461-451;

2.3. Személyi hatály, érintettek köre

2.3.1. A szabályzat hatálya kiterjed a Szentesi Családsegítő Központ valamennyi szervezeti egységére, valamennyi dolgozójára, aki az adatok kezeléséhez kapcsolódó feladatokat végez vagy az intézmény által kezelt adatokkal kapcsolatba kerül, továbbá, aki a feladatellátás során IT eszközzel munkát végez.

2.3.2. A szabályzat hatálya kiterjed továbbá az Intézmény IT rendszerével polgári jogi vagy más jogviszony alapján kapcsolatba kerülő természetes vagy jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre a velük kötött szerződésben rögzített mértékben, illetve titoktartási nyilatkozat alapján.

2.3.3. A szabályzat hatálya kiterjed az intézménynél folyó szakmai munka és dolgozói nyilvántartások során keletkezett minden adat kezelésére, továbbítására, feldolgozására, nyilvántartására, adatvédelmére, továbbá az Intézmény használatára vonatkozó minden informatikai eszközre, az általa használt alkalmazásokra és adatbázisokra.

2.4. A belső adatvédelmi és biztonsági szabályzat módosítása

2.4.1. A szabályzat módosítására az intézmény bármely dolgozója javaslatot tehet az intézményvezetőnek megküldött, de az adatvédelmi tisztviselőnek címzett írásbeli megkeresésben.

2.4.2. A megkeresésnek tartalmaznia kell a dolgozó nevét, aláírását, elérhetőségét, a javasolt módosítást röviden összefoglalva, továbbá a módosítás szükségességét alátámasztó indokokat.

2.4.3. A megkeresés iktatás után kiszignálásra kerül az adatvédelmi tisztviselőhöz, aki megvizsgálja a javasolt módosításokat, elkészíti ajánlását a javasolt módosítás tekintetében.

2.4.4. A megkeresés az ajánlással együtt megküldésre kerül az érintett szakmai vezetőnek, illetve az intézményvezetőnek, aki jóváhagyja a módosítás előkészítését.

2.4.5. Az adatvédelmi tisztviselő előkészíti a módosítás tervezetét és megküldi az érintett szakmai vezetőnek, az intézményvezetőnek egyeztetésre.

2.4.6. A módosítási eljárás szabályait a szakmai vezető, illetve intézményvezető megkeresése alapján indított módosítási eljárás esetében is megfelelően alkalmazni kell.

2.4.7. A módosításokat az intézmény foglalkoztatottjaival, illetve folyamatban lévő ügyek esetében az érintettekkel meg kell ismertetni.

3. Az intézmény adatkezelő szervezete

3.1. Az intézmény valamennyi dolgozója számára kötelező az adatvédelmi és adatbiztonsági szabályok, valamint a munkavégzésükre vonatkozó szakmai adatvédelmi és adatbiztonsági szabályok és előírások betartása.

3.2. Az adatvédelemmel kapcsolatos előírások, így különösen a jelen szabályzat rendelkezéseinek betartását, az adatkezelést és adatfeldolgozást végző szervezeti egység vezetője folyamatosan ellenőrzi.

3.3. Az intézményvezető jogsértés esetén, a tudomására jutást követően azonnal intézkedik a jogsértő adatkezelés megszüntetése iránt.

3.4. Az Intézményvezető az adatvédelmi és adatkezelési szabályok betartása, a törvényesség biztosítása érdekében adatvédelmi felelőst nevezhet ki, vagy olyan külső személyt, szervezetet bízhat meg, aki, amely:

- közreműködik, illetve segítséget nyújt az adatkezelésekkel kapcsolatos döntések meghozatalában, valamint az érintettek jogainak biztosításában,
- az intézményvezető felkérésére ellenőrzi a törvények és más szabályok rendelkezéseinek és az adatbiztonsági követelmények betartását, mely eredményekről írásban beszámol az intézményvezetőnek,
- kivizsgálja a hozzá érkező, neki továbbított bejelentéseket, jogosulatlan adatkezelés észlelése esetén, annak megszüntetése érdekében,
- karbantartja, aktualizálja a belső adatvédelmi és adatbiztonsági szabályzatot,
- jogosult az Intézmény valamennyi szervezeti egységénél az adatkezelésbe betekinteni,

- az egység vezetőjétől, munkatársaitól szóban, írásban felvilágosítást érhet megismert személyes adatokkal kapcsolatban titoktartás terheli,
- törvénysértés esetén ennek megszüntetésére szólítja fel az adatkezelőt, szükség esetén segítséget nyújt a törvényes állapot helyreállításához.

3.5. A szervezeti egység vezetője munkájával segíti az intézményvezető és az adatvédelmi tisztviselő munkáját, közreműködik az adatvédelmi és adatbiztonsági szabályok betartatásában. Ellenőrzi a szervezeti egységnek az adatkezelési és adatbiztonsági szabályoknak történő megfelelést.

4. Fogalom-meghatározások

4.1. *érintett*: bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy;

4.2. *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;

4.3. *személyes adat*: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;

4.4. *különleges adat:*

a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,

b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

4.5. *bűnügyi személyes adat:* a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;

4.6. *közérdekű adat:* az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

4.7. *közérdekből nyilvános adat:* a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

4.8. *hozzájárulás*: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a

rá vonatkozó személyes adat - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez;

4.9. *tiltakozás:* az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri;

4.10. *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 (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

4.11. *közös adatkezelő:* az az adatkezelő, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - az adatkezelés céljait és eszközeit egy vagy több másik adatkezelővel közösen határozza meg, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket egy vagy több másik adatkezelővel közösen hozza meg és hajtja végre vagy hajtatja végre az adatfeldolgozóval;

4.12. *adatkezelés:* az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

4.13. *adattovábbítás:* az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

4.14. *nyilvánosságra hozatal:* az adat bárki számára történő hozzáférhetővé tétele;

4.15. *adattörlés:* az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

4.16. *adatmegjelölés:* az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

4.17. *adatzárolás:* az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

4.18. *adatmegsemmisítés:* az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;

4.19. *adatfeldolgozás*: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adaton végzik;

4.20. *adatfeldolgozó:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;

4.21. *adatfelelős:* az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett*;*

4.22. *adatközlő:* az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatot honlapon közzéteszi;

4.23. *adatállomány:* az egy nyilvántartásban kezelt adatok összessége;

4.24. *harmadik személy:* olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval;

4.25. *EGT-állam:* az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez;

4.26. *harmadik ország:* minden olyan állam, amely nem EGT-állam;

4.27. *kötelező szervezeti szabályozás:* több országban, de köztük legalább egy EGT-államban is tevékenységet folytató adatkezelő vagy adatkezelők csoportja által elfogadott és a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) által jóváhagyott, az adatkezelőre vagy adatkezelők csoportjára nézve kötelező belső adatvédelmi szabályzat, amely a harmadik országba történő adattovábbítás esetén a személyes adatok védelmét az adatkezelő vagy adatkezelők csoportjának egyoldalú kötelezettségvállalása útján biztosítja;

4.28. *adatvédelmi incidens:* személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

4.29. *profilalkotás:* személyes adat bármely olyan - automatizált módon történő - kezelése, amely az érintett személyes jellemzőinek, különösen a munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelésére, elemzésére vagy előrejelzésére irányul;

4.30. *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;

4.31. *álnevesítés:* személyes adat olyan módon történő kezelése, amely - a személyes adattól elkülönítve tárolt - további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely érintettre vonatkozik, valamint műszaki és szervezési intézkedések megtételével biztosítja, hogy azt azonosított vagy azonosítható természetes személyhez ne lehessen kapcsolni.

4.32. *hatóság:* Nemzeti Adatvédelmi és Információszabadság Hatóság feladata a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése, továbbá a személyes adatok Európai Unión belüli szabad áramlásának elősegítése. Székhely: 1125 Budapest, Szilágyi Erzsébet fasor 22/C., postacím: 1530 Szentes, Pf.: 5., E-mail: ugyfelszolgalat@naih.hu, URL: http://naih.hu

5. Az adatkezelés alapelvei

5.1. Jogszerűség, tisztességes eljárás és átláthatóság elve

Személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. Az alapelv megköveteli, hogy személyes adatokat csak megfelelő jogalap birtokában kezelhet az intézmény. A tisztességesség megköveteli, hogy érintetteket az adatkezelés megkezdése előtt kellő információval lássa el az intézmény az adatkezelés teljes folyamatáról, a jogalapról, a célról, az őrzési időtartamról, az érintett jogairól, az adattovábbítás lehetőségeiről, a személyes adatok kezelésével összefüggő kockázatokról, szabályokról, garanciákról és jogokról, valamint arról, hogy hogyan gyakorolhatja az adatkezelés kapcsán megillető jogokat.

5.2. A célhoz kötöttség elve

Személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet. Az intézmény által kezelt személyes adatok esetében az adatkezelés célját táblázatos formában az adatkezelési tevékenységek nyilvántartása tartalmazza.

A személyes adatokat az intézmény nem kezeli a célokkal össze nem egyeztethető módon.

5.3. Adattakarékosság elve

Az intézmény csak a cél eléréséhez szükséges mértékben és a cél szempontjából releváns adatokat kezeli. Az intézmény tartózkodik a készletező adatgyűjtéstől, így nem kerül sor a cél eléréséhez nem szükséges adatok felvételére sem.

5.4. Pontosság elve

Az intézmény törekszik a személyes adatok pontosságára naprakészségére, melynek betartása érdekében a jelen szabályzatba foglalt intézkedéseket teszi meg.

5.5. Korlátozott tárolhatóság elve

A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az e rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.

5.6. Integritás és bizalmas jelleg elve

A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve. Az elv érvényesülése érdekében az intézmény a jelen szabályzatban foglalt rendelkezéseket alkalmazza.

5.7. Elszámoltathatóság

Az adatkezelő felelős az alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

6. Különös szabályok

6.1. Zárt adatkezelés

a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény 17§ (2a) szerint a gyermekjóléti szolgáltatást nyújtó szolgáltató és a gyámhatóság a gyermek bántalmazása, elhanyagolása miatt jelzést vagy kezdeményezést tevő intézmény, személy adatait erre irányuló külön kérelem hiányában is zártan kezeli
A jelzést, a bejelentést tartalmazó iratot a gyermek dokumentációjában külön kell kezelni, a zártan kezelt iratokat zárt borítékban kell továbbítani. A zárt iratanyagba a szülő nem tekinthet bele, az GYSZ adatlapokon a zártan kezelt iratokat nem kell feltüntetni. Az iratból kivonat készíthető, de oly módon, hogy abból a jelzést tevő személyére következtetést ne lehessen levonni (NAIH-1938-2/2013./T)

6.2. Nyilatkozat

az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 6§ (3) szerint, a 16 évét betöltött kiskorú érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos hozzájárulása nem szükséges.

6.3. A gyermek veszélyeztetettségére vonatkozó bejelentés visszavonása, az iratok visszakérése

az érintett gyermek veszélyeztetettségére vonatkozó bejelentés visszavonása esetén, az iratok nem adhatók vissza, a jelzést zártan kell kezelni, a gyermek helyzetét a visszavonás ellenére vizsgálni kell. (Adatvédelmi biztos 587/K/2006-3. számú ajánlása)

6.4. Iratbetekintés

a különélő másik szülő iratbetekintési és iratanyag-másolat készítés kérelme esetén, az iratbetekintés biztosítására a szolgálat/központ munkatársának fel kell készülni, mely során, egyeztetett időpontban kell az iratbetekintést megvalósítani.

Az adatok kiadása előtt vizsgálni kell,

- az iratbetekintés kérelem indokoltságát,
- a kérelmezővel szemben nincs-e büntető eljárás folyamatban a kiskorú vagy az őt nevelő szülővel szemben elkövetett bűncselekmény miatt,
- van-e ideiglenes távoltartó döntés vagy eljárás folyamatban a kérelmezővel szemben,
- melyek a védendő adatok.

7. Az adatkezelési tevékenységek jogszerűsége

7.1. Az intézmény adatkezelést közhatalmi adatkezelési tevékenysége körében

a) törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben, különleges adatnak vagy bűnügyi személyes adatnak nem minősülő adat esetén - helyi önkormányzat rendelete közérdeken alapuló célbóli elrendelés alapján, vagy

b) ennek hiányában az adatkezelés az adatkezelő törvényben meghatározott feladatainak ellátásához feltétlenül szükséges és az érintett a személyes adatok kezeléséhez kifejezetten hozzájárult, vagy

c) az a) pontban 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, vagy
d) az a) pontban meghatározottak hiányában a személyes adatot az érintett kifejezetten nyilvánosságra hozta és az az adatkezelés céljának megvalósulásához szükséges és azzal arányos.
e) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
f) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;

7.2. Az adatkezelési tevékenységeket az intézmény elsődlegesen jogszabályi felhatalmazás alapján végez a feladatainak ellátásához szükséges mértékben. Az adatkezelési tevékenységek nyilvántartása adatonként – táblázatos formában – tartalmazza az adott adat kezelésének jogalapját.

7.3. Ha az adatkezelés hozzájáruláson alapul, az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett a személyes adatainak kezeléséhez hozzájárult. Az igazolás megfelelő, amennyiben a hozzájárulás írásba lett foglalva és az minden ügyre külön is tartalmazza a hozzájárulást.

7.4. Az írásbeli hozzájárulás esetén a hozzájárulást a 3. számú melléklet szerinti formanyomtatványokon, vagy az intézmény által a Szervezeti és Működési Szabályzat mellékleteként használt formanyomtatványon, vagy a jogszabály alapján rendszeresített formanyomtatványon kell megadni.

7.5. Megfelelő az igazolás abban az esetben is, amennyiben az ügy körülményeiből megállapítható a hozzájárulás megadása. Megadottnak tekintjük a hozzájárulást, amennyiben az érintett beadvánnyal fordult az intézményhez.

7.6. Az adatkezelés megkezdése és a hozzájárulás megadása előtt az érintettet tájékoztatni kell a belső adatvédelmi és adatbiztonsági szabályzat VII.4.4.1. pontja szerinti tényekről és körülményekről.

7.7. A hozzájárulását az érintett bármikor visszavonhatja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás visszavonásának jogáról és menetéről az érintettet tájékoztatni kell. Az érintett bármely kérelmét, melynek tartalmából a hozzájárulás visszavonására lehet következetni hozzájárulás visszavonásának kell tekinteni. Az érintett az adatkezeléshez hozzájárulását a 4. számú melléklet szerinti formanyomtatványon is bejelentheti.

8. Az érintett jogai és gyakorlásához kapcsolódó eljárási szabályok

8.1. Az érintettet az adatkezeléséhez kapcsolódóan az alábbi jogok illetik meg:
a) Tájékoztatáshoz való jog
b) Az érintett hozzáférési joga és iratbetekintéshez való jog
c) A helyesbítéshez való jog
d) A törléshez való jog („az elfeledtetéshez való jog”)
e) Az adatkezelés korlátozásához való jog
f) A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség
g) Az adathordozhatósághoz való jog

h) A tiltakozáshoz való jog

8.2. Az intézmény minden dolgozója köteles az érintettek jogainak érvényesülése érdekében szükséges intézkedéseket elősegíteni.

9. Tájékoztatáshoz való jog

9.1. Az intézmény a személyes adatok megszerzésének időpontjában, illetve hozzájáruláson alapuló adatkezelés esetén a hozzájárulás megadása előtt az érintett rendelkezésére bocsátja a következő információk mindegyikét:

a) az adatkezelőnek a kilétét és elérhetőségeit
b) az adatvédelmi tisztviselő elérhetőségeit
c) a személyes adatok tervezett kezelésének célját, valamint az adatkezelés jogalapját
d) a személyes adatok címzettjeit, illetve a címzettek kategóriáit
e) annak ténye, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat, adattovábbítás esetén a megfelelő és alkalmas garanciák megjelölése, valamint az azok másolatának megszerzésére szolgáló módokra vagy az azok elérhetőségére való hivatkozás.
f) tájékoztatás a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól
g) tájékoztatás az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról;
h) tájékoztatást a hozzájárulás visszavonásához való jogról, amennyiben hozzájáruláson alapul az adatkezelés, illetve azon körülményről, hogy a visszavonás nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
i) a felügyeleti hatósághoz címzett panasz benyújtásának jogáról
j) tájékoztatást arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása;
k) tájékoztatás az automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

9.2. Az intézmény adatkezelési tájékoztatókat készített az általa végzett adatkezelési tevékenységek tekintetében a fenti tartalommal. Az egyes adatkezelési tájékoztatók a jelen belső adatvédelmi és adatbiztonsági szabályzat mellékleteit képezik.

10. Az érintett hozzáférési joga és iratbetekintéshez való jog

10.1. Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

a) az adatkezelés céljai;

b) az érintett személyes adatok kategóriái;
c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
d) adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
e) az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
f) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ, kivéve a gyermek veszélyeztetettségének a jelen szabályzatban megfogalmazott esetét

10.2. Az intézmény az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által – ugyanazon adatkörben - kért további másolatokért az adatkezelő az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel.

Ugyanarra az adatkörre vonatkozó első adatkérés ingyenes, egy éven belüli második adatkérés esetében 20.000.-Ft összeg kerül felszámolásra, egy éven belüli harmadik adatkérés 40.000.-Ft, minden további egy éven belüli adatkérés esetében a megelőző összeg duplázódik.

10.3. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri. Széles körben használt elektronikus formátumnak tekinti az intézmény a pdf vagy word formátumot.

10.4. Az érintett által benyújtott, a hozzáférési jogosultság érvényesítésére irányuló kérelmet annak benyújtásától számított huszonöt napon belül bírálja el az intézmény és döntéséről az érintettet írásban vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti.

10.5. A nem az arra jogosulttól érkező vagy értelmezhetetlen, pontosításra szoruló kérelem esetében a kérelmezőt hiánypótlásra kell felhívni, a hiánypótlásban pontosan meg kell jelölni a hiánypótlás kiadásának jogi indokát, valamint, hogy a kérelem mely hiányok pótlása esetén teljesíthető. A hiányok pótlására 15 napot kell biztosítani, mely egy alkalommal újabb 15 nappal meghosszabbítható. A hiányok nem teljesítése esetén a kérelmet el kell utasítani.

Nem kell hiánypótlási felhívást kiadni, amennyiben a hozzáférési jog gyakorlása iránti kérelem teljesítése a rendelkezésre álló információk alapján megtagadható, vagy korlátozható.

10.6. A hozzáférés megtagadása esetén az intézmény írásban, haladéktalanul, legkésőbb 8 napon belül tájékoztatja az érintettet
a) a hozzáférés korlátozásának vagy megtagadásának tényéről, továbbá jogi és ténybeli indokairól, ha ezeknek az érintett rendelkezésére bocsátása valamely alábbi érdek érvényesülését nem veszélyezteti (az intézmény által vagy részvételével végzett vizsgálatok vagy eljárások - így különösen a büntetőeljárás - hatékony és eredményes lefolytatásának, a bűncselekmények hatékony és eredményes megelőzésének és felderítésének, a bűncselekmények elkövetőivel szemben alkalmazott büntetések és intézkedések végrehajtásának, a közbiztonság hatékony és eredményes védelmének, az állam külső és belső biztonsága hatékony és eredményes védelmének, így különösen a honvédelem

és a nemzetbiztonság vagy harmadik személyek alapvető jogai védelmének biztosításához szükséges), valamint

b) az érintettet e törvény alapján megillető jogokról, valamint azok érvényesítésének módjáról, így különösen arról, hogy az érintett a hozzáféréshez való jogát a Hatóság közreműködésével is gyakorolhatja.

10.7. A hozzáférési jog gyakorlása iránti kérelmekre adandó választ az adatvédelmi tisztviselővel egyeztetni kell. A hozzáférési jog gyakorlásának megtagadását vagy korlátozását tartalmazó döntést kizárólag az adatvédelmi tisztviselő egyetértésével lehet meghozni.

10.8. Nem illeti meg az érintettet a hozzáférés joga, amennyiben azt jogszabály kizárja, így különösen a bántalmazás, elhanyagolás miatt jelzés vagy kezdeményezést tevő intézmény, személy adatai tekintetében.

10.9. Az intézmény azokat a személyes adatokat, melyek tekintetében az érintett nem gyakorolhatja a hozzáférési jogát zártan kezeli. A zártan kezelt adatokat az akta többi részétől és a többi személyes adattól elkülönítetten kezeli. A zártan kezelendő személyes adatok lezárt borítékban, széfben kerülnek tárolásra, melyhez kizárólag az intézményvezető, illetve az általa feljogosított személynek van hozzáférése.

10.10. A zárt borítékon feltüntetésre kerül az iktatószám és az érintett TAJ száma, mellyel az adott aktával való kapcsolata megteremthető.

10.11. Az intézmény megtagadja a szülő tájékoztatását a gyermek és az őt nevelő szülő vagy a gyermek törvényes képviselője tartózkodási helyére vonatkozóan, illetve korlátozza a szülő iratbetekintési jogát, ha

a) a szülő ellen gyermeke vagy a gyermeket nevelő másik szülő sérelmére elkövetett bűncselekmény miatt büntetőeljárás van folyamatban, annak jogerős befejezéséig,

b) a szülő ellen gyermeke vagy a gyermeket nevelő másik szülő sérelmére elkövetett külön törvényben meghatározott hozzátartozók közötti erőszak miatt alkalmazható ideiglenes megelőző távoltartó határozat vagy megelőző távoltartó határozat iránti eljárás van folyamatban, a távoltartás időtartamáig.

10.12. A gyermek szülője vagy törvényes képviselője intézmény vezetőjénél – a hozzáférési joga gyakorlása körében - kérelmezheti, hogy betekinthessen a külön jogszabály szerinti gyermekvédelmi nyilvántartásnak a gyermek vonatkozásában kitöltött adatlapjaiba, valamint a gyermekjóléti, gyermekvédelmi szolgáltatónál, intézménynél keletkezett, illetve részére megküldött, a gyermekkel kapcsolatos iratba. Az iratokról kivonat vagy másolat kérhető. A közigazgatási hatósági eljárás általános szabályairól szóló törvényben meghatározottakon túl az érintett írásbeli hozzájárulása hiányában nem lehet betekinteni a másik szülőre vonatkozó, különleges adatot tartalmazó iratba, kivéve, ha az a gyermek érdekében kezdeményezett, a gyermek védelembe vételére vagy nevelésbe vételére irányuló gyámhatósági eljárás, illetve a gyermek elhelyezésének megváltoztatására irányuló bírósági eljárás megindításához elengedhetetlenül szükséges.

10.13. Az érintett jogosult halála esetére közokiratban, vagy teljes bizonyító erejű magánokiratba foglalt nyilatkozatot tenni az adatkezelőnél a jogszabályban meghatározott jogok gyakorlására, a jogszabályban meghatározott időtartamra. Nyilatkozat hiányában a közeli hozzátartozó csak korlátozott, a jogszabályban meghatározott jogokat gyakorolhatja. A jogokat érvényesítő személy az érintett halálának tényét és idejét halotti anyakönyvi kivonattal vagy bírósági határozattal,

valamint saját személyazonosságát, közeli hozzátartozói minőségét közokirattal igazolja.

10.14. Az iratbetekintési jog gyakorlásához az intézmény a 6. számú melléklet szerinti formanyomtatványt bocsátja az érintett rendelkezésére, azonban az iratbetekintés iránti kérelem bármely formában előterjeszthető. Az iratbetekintéshez kapcsolódó adatkezelési tájékoztatót a 6/A. szám alatti melléklet tartalmazza.

10.15. Az adatkezelő az érintett hozzáférési jogával kapcsolatos intézkedésekről nyilvántartást vezet, mely tartalmazza az érintett hozzáférési jogának érvényesítését az információs önrendelkezési jogról és az információszabadságról 2011. évi CXII. törvény szerint korlátozó vagy megtagadó intézkedésének jogi és ténybeli indokait. A nyilvántartást a 15. számú melléklet tartalmazza.

11. A helyesbítéshez való jog

11.1. A személyes adatokat pontosan kell rögzíteni a belső adatvédelmi és adatbiztonsági szabályzat VII.1.4. pontjában foglalt alapelv rendelkezéseinek megfelelően.

11.2. A személyes adatot felvevő személy köteles a személyes adatot a felvétel után ellenőrizni, és a hibás adatot azonnal javítani oly módon, hogy megállapítható legyen a javítás előtti adat, a javítás időpontja, illetve a javítást végző személy.

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

11.4. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok kiegészítését.

11.5. Az érintett által benyújtott, a helyesbítési jogosultság érvényesítésére irányuló kérelmet annak benyújtásától számított huszonöt napon belül bírálja el az intézmény és döntéséről az érintettet írásban vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti.

11.6. A nem az arra jogosulttól érkező, vagy értelmezhetetlen, pontosításra szoruló kérelem esetében a kérelmezőt hiánypótlásra kell felhívni. A hiánypótlásra alkalmazni kell a jelen belső adatvédelmi és adatbiztonsági szabályzat VII.4.2.5. pontjának rendelkezéseit.

11.7. A helyesbítési jog gyakorlása iránti kérelmekre adandó választ az adatvédelmi tisztviselővel egyeztetni kell. A helyesbítési jog gyakorlásának megtagadását vagy korlátozását tartalmazó döntést kizárólag az adatvédelmi tisztviselő egyetértésével lehet meghozni.

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

12.1. Az intézmény személyes adatokat a jogszabályban, valamint az adatkezelési tevékenységek nyilvántartásában megjelölt időtartamban kezeli.

12.2. Az időtartam lejártával a személyes adatokat az intézmény törli.

12.3. 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 az alábbi indokok valamelyike fennáll:

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
b) az érintett visszavonja a 6. cikk (1) bekezdésének a) pontja vagy a 9. cikk (2) bekezdésének a) pontja értelmében az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
c) az érintett tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,
d) a személyes adatokat jogellenesen kezelték;
a) a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

12.4. Nem alkalmazandó az érintett törléshez való joga, amennyiben az adatkezelés szükséges:
b) a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;
c) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

12.5. A személyes adatok törlésére és iratok megsemmisítésére a jelen szabályzat 7. számú melléklete szerinti iratkezelési szabályzat szerint van lehetőség.

12.6. Az érintett által benyújtott, a törlési jogosultság érvényesítésére irányuló kérelmet annak benyújtásától számított huszonöt napon belül bírálja el az intézmény és döntéséről az érintettet írásban vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti.

12.7. A nem az arra jogosulttól érkező, vagy értelmezhetetlen, pontosításra szoruló kérelem esetében a kérelmezőt hiánypótlásra kell felhívni. A hiánypótlásra alkalmazni kell a jelen belső adatvédelmi és adatbiztonsági szabályzat VII.4.2.5. pontjának rendelkezéseit.

12.8. A törlési jog gyakorlása iránti kérelmekre adandó választ az adatvédelmi tisztviselővel egyeztetni kell. A törlési jog gyakorlásának megtagadását vagy korlátozását tartalmazó döntést kizárólag az adatvédelmi tisztviselő egyetértésével lehet meghozni.

13. Az adatkezelés korlátozásához való jog

13.1. Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

a) 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;
b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
c) az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
d) 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.

13.2. Az érintett által benyújtott, a korlátozási jogosultság érvényesítésére irányuló kérelmet annak benyújtásától számított huszonöt napon belül bírálja el az

intézmény és döntéséről az érintettet írásban vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti.

13.3. A nem az arra jogosulttól érkező, vagy értelmezhetetlen, pontosításra szoruló kérelem esetében a kérelmezőt hiánypótlásra kell felhívni. A hiánypótlásra alkalmazni kell a jelen belső adatvédelmi és adatbiztonsági szabályzat VII.4.2.5. pontjának rendelkezéseit.

13.4. A korlátozáshoz való jog gyakorlása iránti kérelmekre adandó választ az adatvédelmi tisztviselővel egyeztetni kell. A korlátozáshoz való jog gyakorlásának megtagadását vagy korlátozását tartalmazó döntést kizárólag az adatvédelmi tisztviselő egyetértésével lehet meghozni.

14. A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség

14.1. 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.

14.2. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.

14.3. Azt, hogy mi minősül lehetetlennek, vagy aránytalanul nagy erőfeszítésnek az adatvédelmi tisztviselő állásfoglalása alapján az intézményvezető állapítja meg.

15. Az adathordozhatósághoz való jog

15.1. Az érintett által benyújtott, az adathordozhatósághoz való jogosultság érvényesítésére irányuló kérelmet annak benyújtásától számított huszonöt napon belül bírálja el az intézmény és döntéséről az érintettet írásban vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti.

15.2. A nem az arra jogosulttól érkező, vagy értelmezhetetlen, pontosításra szoruló kérelem esetében a kérelmezőt hiánypótlásra kell felhívni. A hiánypótlásra alkalmazni kell a jelen belső adatvédelmi és adatbiztonsági szabályzat VII.4.2.5. pontjának rendelkezéseit.

15.3. Az adathordozhatósághoz való jog gyakorlása iránti kérelmekre adandó választ az adatvédelmi tisztviselővel egyeztetni kell. Az adathordozhatósághoz való jog gyakorlásának megtagadását vagy korlátozását tartalmazó döntést kizárólag az adatvédelmi tisztviselő egyetértésével lehet meghozni.

15.4. Figyelemmel arra, hogy az intézményi adatkezelés nem automatizált módon történik, így nem áll fenn jogszabályi kötelezettsége az adathordozhatósághoz kapcsolódó jog teljesítéséhez, így az erre irányuló kérelmet az intézmény csak kivételesen indokolt esetben, a költségek megtérítése után, egyedi mérlegeléssel teljesítheti.

15.5. Az adathordozhatósághoz kapcsolódó költségekről az intézmény, a kérelem teljesítése előtt tájékoztatást küld. A költségek minimum összege, 1.000.-Ft/személyes adat, de maximum 100.000.-Ft.

16. A tiltakozáshoz való jog

16.1. Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak kezelése ellen, amennyiben az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához, vagy az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

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

16.3. A tiltakozáshoz való jogról az érintettnek legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni a figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

16.4. Az érintett által benyújtott, a tiltakozáshoz való jogosultság érvényesítésére irányuló kérelmet annak benyújtásától számított huszonöt napon belül bírálja el az intézmény és döntéséről az érintettet írásban vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti.

16.5. A nem az arra jogosulttól érkező, vagy értelmezhetetlen, pontosításra szoruló kérelem esetében a kérelmezőt hiánypótlásra kell felhívni.

16.6. A tiltakozáshoz való jog gyakorlása iránti kérelmekre adandó választ az adatvédelmi tisztviselővel egyeztetni kell. A tiltakozáshoz való jog gyakorlásának megtagadását vagy korlátozását tartalmazó döntést kizárólag az adatvédelmi tisztviselő egyetértésével lehet meghozni.

17. Kapcsolódó szabályok

Az adatvédelmi és adatbiztonsági szabályokat az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni,

a) Szervezeti és Működési Szabályzat,
b) Iratkezelési szabályzat
c) Szakmai Program

18. Az adatok kezelésének rendje

18.1. Személyes adat akkor kezelhető – mind a munkatársak, mind a szolgáltatást igénybe vevők körében - ha az érintett hozzájárul, vagy azt törvény, vagy törvény felhatalmazása alapján helyi önkormányzati rendelet –közérdeken alapuló célból- elrendeli.

18.2. Különleges adat akkor kezelhető, ha

a) az érintett írásban hozzájárul
b) nemzetközi egyezményen alapul, az Alaptörvényben biztosított alapvető jog érvényesítéséért, továbbá nemzetbiztonsági vagy bűnmegelőzés, vagy bűnüldözés érdekében történik
c) ha azt törvény elrendeli.

18.3. Személyes adat kezelhető akkor is, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése, az adatkezelőre vonatkozó jogi kötelezettség teljesítése, valamint, az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdekek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

18.4. A személyes adatok védelméhez fűződő jogot és az érintett személyiségi jogait az adatkezeléshez fűződő más érdekek nem sérthetik.

18.5. A kezelt személyes adatoknak meg kell felelniük az alábbi követelményeknek:

a) felvételük és kezelésük tisztességes és törvényes,

b) pontosak, teljesek,

c) tárolásuk módja alkalmas arra, hogy az érintett személyiségi jogai ne sérüljenek.

III. Közalkalmazottakra vonatkozó adatkezelés

Az Intézményben személyi irat minden adathordozó, amely a közalkalmazotti jogviszony létesítésekor, fennállása alatt, megszűnésekor, illetve azt követően keletkezik, és a közalkalmazott személyével összefüggésben adatot, megállapítást tartalmaz.

1. Személyi iratok köre

a) a személyi anyag iratai,

b) a közalkalmazotti jogviszonnyal kapcsolatos egyéb iratok,

c) a közalkalmazott közalkalmazotti jogviszonnyal összefüggő egyéb jogviszonyokkal kapcsolatos iratai (adóbevallás, fizetési letiltás stb.),

d) a közalkalmazott saját kérelmére kiállított vagy átadott iratok.

2. Jogosultságok, felelősségi szabályok:

2.1. Az intézményvezető jogosult az intézmény közalkalmazottjának személyi nyilvántartásába teljes körűen betekinteni.

2.2. A személyügyi és bérgazdálkodási feladatokat ellátó közalkalmazott a munkavégzéshez szükséges mértékű adatkezelési, betekintési, adatrögzítési, másolatkészítési, üzemeltetési jogosultsága és adatvédelmi kötelezettsége van az Intézmény személyi állománya adataira vonatkozóan. Adathelyesbítés csak az intézményvezető tudtával és beleegyezésével történhet.

2.3. Az intézményvezetőnek, helyettesének és a személyügyi, bérgazdálkodási feladatokat ellátó munkatársnak, a bérszámfejtéshez nélkülözhetetlen adatok vonatkozásában adatvédelmi, kötelezettsége van.

2.4. A közalkalmazott kizárólag saját nyilvántartott adatait illetően jogosult betekintésre, helyesbítés, másolat kérésére, illetve megismerésére és felelős azért, hogy az általa szolgáltatott adatok hitelesek, pontosak, teljesek és aktuálisak legyenek.

3. Általános feladatok és eljárási szabályok

3.1. A közalkalmazotti nyilvántartásban, a személyi anyagban, a személyi iratokban nyilvántartott adatokkal kapcsolatban minden ezen szabályzat szerint információhoz jutó személyt adatvédelmi kötelezettség terhel. Felelős a tudomására jutott adat rendeltetésének megfelelő felhasználásáért, valamint azért, hogy ezen szabályzat szerint illetéktelen személy birtokába védett adat ne kerülhessen.

3.2. A személyügyi és bérgazdálkodási feladatokat ellátó közalkalmazott az általa kezelt közalkalmazotti jogviszonnyal összefüggő iratra adatot, megállapítást csak közokirat, a közalkalmazott írásbeli nyilatkozata, a munkáltatói jogkör gyakorlójának írásbeli rendelkezése, bíróság vagy más hatóság döntése, jogszabályi rendelkezés alapján tehet és köteles kezdeményezni a vezetőjénél a megítélése szerint a valóságnak már nem megfelelő adat helyesbítését, törlését.

3.3. Személyi iratot tárolni csak a személyügyi és bérgazdálkodási feladatot ellátó dolgozó hivatali helyiségében, zárral ellátott irattárolóban, a munkavégzés befejezése után zárt hivatali helyiségben lehet.

3.4. A személyügyi és bérgazdálkodási feladatott ellátó dolgozó, mind a személyes adatok, iratok, mind az egyéb személyes információk megtartásáért felel, azokat csak törvényes feltételek megléte esetén továbbítja.

3.5. A munkavállalótól csak olyan adat közlése kérhető, amely személyiségi jogát nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges.

3.6. A munkaviszony létesítésekor a munkavállaló átadja a munkaszerződés megkötéséhez, illetve a munkáltató társadalombiztosítási bejelentési kötelezettsége teljesítése érdekében szükséges személyes adatait tartalmazó dokumentumokat, igazolványokat, melyeken található adatokról a Szentesi Családsegítő Központ munkatársa adatfelvételi lapot vesz fel.

3.7. Az igazolványokról másolat nem készül.

3.8. A személyes adatok és az adatfelvételi lap a személyi nyilvántartásban kerülnek rögzítésre.

3.9. A hozzájáruláson alapuló adatkezelés esetén a munkavállaló írásbeli hozzájárulását be kell szerezni. A hozzájárulás szövegét a 8. számú melléklet tartalmazza.

3.10. A foglalkoztatottaknak a melléklet szerinti nyilatkozatot kell aláírniuk a tájékoztatás megtörténtének igazolása érdekében.

3.11. A központosított illetményszámfejtés biztosítja az intézménynél foglalkoztatott közalkalmazottak, munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban állók személyi juttatásainak (illetmények és a jogviszony alapján járó egyéb juttatások), egészségbiztosítási ellátásainak (táppénz, GYED, terhességi gyermekágyi segély, baleseti táppénz), illetve a munkáltatókat terhelő közterheknek elszámolását.

3.12. A központi illetményszámfejtés a Magyar Államkincstár által biztosított, fejlesztett és működtetett számítógépes programon (a továbbiakban: illetményszámfejtő program) keresztül valósul meg.

3.13. Az intézmény a Magyar Államkincstár felé dokumentumokat elsődlegesen elektronikusan küld meg. Eredeti – foglalkoztatottnak címzett, vagy a rendelkezése alatt álló - iratnak a Magyar Államkincstár felé történő megküldése csak a

foglalkoztatott írásbeli hozzájárulása alapján és a Magyar Államkincstár előzetes írásbeli kérése alapján van lehetőség.

3.14. A munkavállalók részére az intézmény igazolványt bocsát a rendelkezésére, melyet a munkavállaló köteles intézkedése előtt az érintettnek bemutatni. Az igazolvány tartalmazza a munkavállaló nevét, az igazolvány azonosító számát, valamint az intézmény nevét, székhelyét, a kiállító aláírását és a hivatalos bélyegzőlenyomatát.

4. A számítógépen vezetett közalkalmazotti nyilvántartás fizikai védelmének szabályai

4.1. A személyügyi adatkezelést végző helyiségben az ott dolgozókon kívül csak az intézményvezető, ill. helyettese, a szakmai vezető, vagy a saját ügyében eljáró közalkalmazott tartózkodhat, az új felvételre vagy az ellenőrzésre jogosultak léphetnek be.

4.2. A számítástechnikai eszközökhöz való hozzáférési jogosultság biztosítását az adatkezelőnek neki kiadott azonosítási jelszóval kell lehetővé tenni.

4.3. A jelszót úgy kell kialakítani, hogy saját jelszavát az adatkezelőn kívül csak a vezetője, vagy az arra felhatalmazott személy ismerhesse meg.

4.4. A személyügyi adatkezelést ellátó munkahelyet csak a számítógép kikapcsolt, vagy jelszóval védett állapotában hagyhatja el a kezelője.

4.5. A személyügyi és bérgazdálkodási feladatokat ellátó dolgozó jogosult és köteles személyügyi adatokat szolgáltatni a Magyar Államkincstár, mint az intézménnyel külön kötött megállapodás szerint a bérgazdálkodással, bérszámfejtéssel megbízott szerv felé.

5. Az üzemeltetés biztonsági szabálya

A közalkalmazotti nyilvántartás számítástechnikai eszközeit üzemeltető személy megváltozásával egyidejűleg vagy szükség szerint a jelszót is meg kell változtatni. A számítástechnikai rendszer bármely eleme csak az intézményvezető, akadályoztatása esetén a helyettese, vagy felhatalmazott személy tudtával, engedélyével változtatható meg.

6. A személyi iratok kezelésének legfontosabb technikai szabályai

6.1. Személyi iratra csak olyan adat, megállapítás kerülhet, amely alapja: közokirat, vagy a közalkalmazott nyilatkozata, a munkáltatói jogkör gyakorlójának írásbeli rendelkezése, bíróság vagy hatóság döntése, illetve jogszabályi rendelkezés.

6.2. Személyi anyagot a közalkalmazotti jogviszony megszűnésétől számított 50 évig központi irattárban kell megőrizni.

IV. Az ügyfelek adatainak kezeléséhez kapcsolódó szabályok

1. Általános szabályok

1.1. Személyes adatot csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet kezelni. Az adatkezelés minden szakaszában meg kell felelni e célnak, az adatok felvételének és kezelésének törvényesnek kell lenni.

1.2. Az ügyfelek személyes iratanyagáért (a benne kinyomtatott adatlapok, levelezések, szakértői vélemények, jelzések, panaszok, az arra adott válaszok, nyilatkozatok, kérvények eredeti vagy másolt példányokért) velük közvetlen kapcsolatban álló esetfelelős, esetvivő (családsegítő, esetmenedzser, tanácsadók) felel. Az iratok ügyfélhez és a vele kapcsolatban álló szakemberhez rendeltek. Az egyéni belépési kóddal rendelkező munkatárs az ügyfélhez rendelt számítógépes információkat saját mappában tárolja, rendszeresen saját gépre menti. Adatot, információt csak az ügyfél engedélyével, tudtával, vagy a törvényekben meghatározott céllal, meghatározott szerv képviselőjének továbbít.

1.3. A szociális asszisztensek a számítógépen tárolt ügyfélnyilvántartásért, annak tárolásáért felelősséggel tartoznak. Utasításra adatszűréseket végeznek, adatlapok szerint aktualizálják a nyilvántartott adatokat. Engedély, törvényes indokolás hiányában adatot nem törölhetnek, nem változtathatnak meg, nem adhatják ki.

1.4. A szakmai vezetők kötelesek az adatkezeléseket úgy megtervezni és végrehajtani, hogy a szükséges törvények és az adatkezelésre vonatkozó más jogszabályok alkalmazása során biztosítsa az érintettek személyes adatainak biztonságát, magánszférájának védelmét.

1.5. Az adatokat megfelelő intézkedésekkel védeni kell, különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, törlés, megsemmisítés, vagy véletlen megsemmisülés, sérülés ellen. Az adatkezelést és adatvédelmet szolgáló intézkedések során tekintettel kell lenni a mindenkori technika fejlettségére, az intézményi adottságokra, több lehetséges adatkezelési megoldás közül azt kell választani, ami a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.

1.6. Az ügyfelekre vonatkozó nyilvántartások biztonságos megőrzéséről, a feltételek biztosításáról az intézményvezetőnek kell gondoskodnia.

1.7. Az intézményben kezelt adatok céljai különösen

1.7.1. a szociális és egyéb szolgáltatást igénybe vevők jogosultságának megállapítása, a szociális és egyéb szolgáltatások igénybe vevőivel végzett szakmai munka,

1.7.2. az intézményben folyó szakmai munka során szükségessé váló intézkedések, szakmai intervenciók, lépések megvalósítása,

1.7.3. szakmai vizsgálat, elemzés és fejlesztés tervezése, szervezése, költségvetési tervezés,

1.7.4. az Intézmény hatósági vagy törvényességi ellenőrzését, szakmai felügyeletét végző szervek munkájának elősegítése,

1.7.5. az Intézmény dolgozóinak adatkezelése.

1.8. Nyilvántartásból adat, csak az adatigénylésre jogosult szervnek, személynek adható ki. A szociális és személyazonosító adatok kezelése során biztosítani kell az adatok biztonságát véletlen vagy szándékos megsemmisítéssel, megsemmisüléssel, megváltoztatásával, nyilvánosságra kerülésével szemben.

1.9. A számítógépen vezetett elektronikus nyilvántartást minden hónapban legalább egyszer külön adathordozóra is le kell menteni, melyet elzárt helyiségben kell tárolni.

2. A Család- és Gyermekjóléti Szolgálat és Központ kötelező adminisztrációja és nyilvántartása

Az ügyfelekre vonatkozó adatokat, dokumentumokban rögzített nyilvántartásokat a Szociális törvény, a Gyermekvédelmi törvény, azok végrehajtási rendeletei, valamint az ágazatra vonatkozó miniszteri és kormányrendeletek, és a hivatalos szabályozó dokumentumok határozzák meg. A nyilvántartott dokumentumok és adatok a kötelező adminisztráció részei, mint:

2.1. Kapcsolatfelvétel:

- Tájékoztatási nyilatkozat
- Ügyfélnyilvántartásba történő bevezetés

2.2. Információszolgáltatás/egyszeri ügyintézés:

- Tájékoztatásról szóló nyilatkozat
- Ügyfélnyilvántartásba történő bevezetés
- KENYSZI egyszerűsített adattartalommal

2.3. Az együttműködési megállapodás megkötése utáni dokumentáció:

- Esetnapló A)-B) 1.2. részének kitöltése
- Veszélyeztetett gyermek esetén Esetnapló betétlap, GYSZ-2,
- Hatósági intézkedés kezdeményezésének lehetősége felmerül és nem volt Esetnapló betétlap: T-lap, GYSZ-1 és GYSZ-3
- Járási központ speciális szolgáltatásainak bevonásakor GYSZ-1 adatlap
- Eset lezárását megelőzően esetkonferencia (emlékeztető), Esetnaplóban és KENYSZI-ben lezárás

2.4. Hatósági intézkedés kezdeményezése:

- Ha nem volt előzmény: T-lap, GYSZ-1, GYSZ-2, GYSZ-3
- Ha volt előzmény, de nem volt veszélyeztetettség: akkor Esetnapló, T-lap, GYSZ-1, GYSZ-2, GYSZ-3, GYSZ-4
- Ha volt előzmény, és volt veszélyeztetettség, akkor Esetnapló, Esetnapló betétlap, GYSZ-1, GYSZ-2, GYSZ-3, GYSZ-4

2.5. A gyermekvédelmi gondoskodás intézkedései:

- Ideiglenes hatályú elhelyezés :
  - ha nem volt előzmény: T-lap, GYSZ-1, GYSZ-2;
  - ha már volt szociális segítő munka, de nem volt veszélyeztetettség akkor Esetnapló, T-lap, GYSZ1, GYSZ-2, GYSZ-3, GYSZ-4;
  - ha már volt szociális segítő munka és volt veszélyeztetettség, akkor Esetnapló,
  - Esetnapló betétlap, GYSZ-1, GYSZ-2, GYSZ-3, GYSZ-4
- Családbafogadás:
  - ha nem volt előzmény: T-lap, GYSZ-1, GYSZ-2;

- ha már volt szociális segítő munka, de nem volt veszélyeztetettség akkor Esetnapló, T-lap, GYSZ-1, GYSZ-2, GYSZ-3, GYSZ-4;
- ha már volt szociális segítő munka és volt veszélyeztetettség, akkor Esetnapló,
- Esetnapló betétlap, GYSZ-1, GYSZ-2, GYSZ-3, GYSZ-4
- A gyermek harmadik személynél történő elhelyezése: Esetnapló, Esetnapló betétlap, GYSZ-1, GYSZ-2, GYSZ-3

2.6. A család- és gyermekjóléti szolgáltatás egyéb tevékenységeinek adminisztrációja:

- Halmozottan hátrányos helyzet megállapítása: tájékoztatásról szóló nyilatkozat, ügyfélnyilvántartásba történő bevezetés, KENYSZI, a gyámhatóságokról, valamint a gyermekvédelmi és gyámügyi eljárásról szóló149/1997 (IX.10.) kormányrendelet 3/a melléklete-környezettanulmány.
- Gyermekétkeztetés: ügyfélnyilvántartásba történő bevezetés, a személyes gondoskodást nyújtó gyermekjóléti alapellátások és gyermekvédelmi szakellátások térítési díjáról és az igénylésükhöz felhasználható bizonyítékokról szóló 328/2011 (XII.29.)Korm. rendelet

2.7. Az észlelő és jelzőrendszeri tanácsadó kötelező adminisztrációja:

- Az összegyűjtött a települések észlelő- és jelzőrendszeri felelősei által készített intézkedési terveiből statisztikát készít.
- Az összegyűjtött jelzésekből és az azokhoz kötődő intézkedésekből legalább egy alkalommal évente értékelést készít.

3. A Családok és a Gyermekek Átmeneti Otthonainak kötelező adminisztrációja és nyilvántartása

Az ügyfelekre vonatkozó adatokat, dokumentumokban rögzített nyilvántartásokat a Szociális törvény, a Gyermekvédelmi törvény, azok végrehajtási rendeletei, valamint az ágazatra vonatkozó miniszteri és kormányrendeletek, és a hivatalos szabályozó dokumentumok határozzák meg. A nyilvántartott dokumentumok és adatok a kötelező adminisztráció részei, mint:

3.1. Kapcsolatfelvétel:

- Tájékoztatási nyilatkozat
- Ügyfélnyilvántartásba történő bevezetés
- Megállapodás
- KENYSZI egyszerűsített adattartalommal

3.2. Az együttműködési megállapodás megkötése utáni dokumentáció:

- Törzslap
- IX. sz adatlap,
- Jövedelem ig. 5 sz. mell.
- ÁTG-2
- ÁTG-3
- ÁTG-4

3.3. A család- és gyermekjóléti szolgáltatás egyéb tevékenységeinek adminisztrációja:

- Halmozottan hátrányos helyzet megállapítása: tájékoztatásról szóló nyilatkozat, ügyfélnyilvántartásba történő bevezetés, KENYSZI, a gyámhatóságokról, valamint a gyermekvédelmi és gyámügyi eljárásról szóló149/1997 (IX.10.) kormányrendelet 3/a melléklete-környezettanulmány.
- Gyermekétkeztetés: ügyfélnyilvántartásba történő bevezetés, a személyes gondoskodást nyújtó gyermekjóléti alapellátások és gyermekvédelmi szakellátások térítési díjáról és az igénylésükhöz felhasználható bizonyítékokról szóló 328/2011 (XII.29.)Korm. rendelet
- Kliensnyilvántartás
- Ellátási napokról szóló nyilvántartás
- Térítési díj nyilvántartás
- Ügyeleti napló

4. A Dózsa-ház Közösségi Tér kötelező adminisztrációja és nyilvántartása

Az igénybevevőkre vonatkozó adatokat és dokumentumokban rögzített nyilvántartásokat a helyiségfoglalásokhoz, táborokban, programokon való részvételhez, valamint a szolgáltatások forgalmi adatainak rögzítése céljából gyűjt és kezel az intézmény.
kapcsolódóan

Az online, személyes (papír alapú), vagy telefonos foglalás esetén az intézmény az alábbi adatok rendelkezésre bocsátását kéri/kérheti a vendégektől: megszólítás, vezetéknév, keresztnév, cím (település, irányítószám,), e-mail cím, telefonszám.

Terembérleti szerződés megkötése esetén kötelezően megadandó adatok: családi név, keresztnév, születési hely és idő, személyi igazolvány szám, lakcím, foglalás időtartama, adószám, aláírás.

5. A Szentes Városi Üdülő – Szigliget adminisztrációja és nyilvántartása

Szobafoglaláshoz, táborokban, tábori programokon való részvételéhez kapcsolódóan

Az online, személyes (papír alapú), vagy telefonos szobafoglalás esetén az Üdülőtábor az alábbi adatok rendelkezésre bocsátását kéri/kérheti a vendégektől: megszólítás, vezetéknév, keresztnév, cím (település, irányítószám, ország), e-mail cím, telefonszám, a fizetés módja (készpénz, bankkártya, Széchenyi Pihenőkártya).

A bejelentőlapon kötelezően megadandó adatok: családi név, keresztnév, születési hely és idő, állampolgárság (önkéntes hozzájárulás alapján, statisztikai célból), személyi igazolvány szám, lakcím, érkezés dátuma, elutazás dátuma, nyilatkozat az IFA mentességről, aláírás.

Tájékoztatjuk vendégeinket, hogy a harmadik országbeli állampolgárokról az alábbi adatok kezelése jogszabályi előírás: a természetes személyazonosító adatokon kívül, az úti okmány (útlevél) azonosító adat, az országba történt beutazás napja, aláírás.

Ezen adatok megadása a szállodai szolgáltatás igénybevételének az elengedhetetlen feltétele.

A vendégnévsoron kötelezően megadandó adatok: név, nemzetiség, születési idő, lakcím, érkezés ideje, távozás ideje, aláírás. Ezen túlmenően a csoportvezető telefonszáma.

Az Üdülőtábor az általa üzemeltetett honlap (www.szigligeti.udulo.szentes.hu) látogatásakor sem a felhasználó IP címét, sem más adatot nem rögzít.

Az Üdülőtábor a felhasználó böngészése közben a számítógépen kizárólag a szolgáltatások fenntartása és fejlesztése illetve statisztikai célokra ún. sütit helyezhet el. Ezeket a felhasználó a saját számítógépén törölni tudja, vagy a böngészőjében eleve megtilthatja alkalmazásukat.

Az Üdülőtábor által üzemeltetett weboldal html kódja webanalitikai mérések céljából független, külső szerverről érkező és külső szerverre mutató hivatkozásokat tartalmazhat. A webanalitikai szolgáltató személyes adatokat nem, csak a böngészéssel kapcsolatos, az egyének beazonosítására alkalmatlan adatokat kezel.

AZ ÜDÜLŐTÁBOR EGYÉB ADATKEZELÉSEI című fejezetben rögzített adatkezelései során az ott meghatározott adatköröket kezeli az Üdülőtábor.

V. Az informatikai rendszer védelme

1. Általános szabályok

1.1. A Szentesi Családsegítő Központ a munkatársak részére számítógépet (beleértve lap top, táblagép, notebook, ipad, pendrive stb.) és okos telefont tart fenn.

1.2. A foglalkoztatott rendelkezésére bocsátott eszközök személyes célra nem használhatóak. A felhasználók az Intézményben lévő internetet csak a munkájukhoz szükséges mértékben használhatják, a munkához nem tartozó internetes tartalmak letöltése tilos,

1.3. elektronikus levelezés során az Intézmény érdekeit figyelembe véve kell eljárni, a levelezési normák betartása mellett, hivatalos ügyben levél csak a ……@cssk-szentes.hu e-mail címről küldhető

1.4. Az eszközök ellenőrzésére, a rajta lévő személyes adatok lementésére és tárolására az intézmény képviseletében az intézményvezető és az informatikus együttesen előre jelzett ellenőrzési időszakban, tetszőleges időpontban – a foglalkoztatott jelenléte biztosításának lehetőségével - jogosult. Az ellenőrzés célja a foglalkoztatotti kötelezettségek teljesítésének ellenőrzése.

1.5. A foglalkoztatottnak az adatok törlésére nyitva álló ideje 2 munkanap. A foglalkoztatott az engedély nélkül tárolt személyes adatainak a törlését úgy köteles végrehajtani, hogy az intézmény által kezelt adatok ne sérüljenek. Az intézmény informatikai karbantartását végző munkatárs segítsége igénybe vehető a törlés elvégzéséhez. A kötelezettség elmulasztása esetén a személyes adat az eszközökről törlésre kerül.

1.6. Nem kerülnek törlésre a személyes adatok, illetve nem munkakörbe tartozó tevékenység adatai, amennyiben az, az intézmény érdekeinek megóvása érdekében, munkajogi jogkövetkezmények alkalmazása céljából elengedhetetlenül szükségesek. Az intézményt az eljárást az elévülési időn belül megindítja.

2. Hálózati azonosítás, hozzáférés

2.1. Windows hálózati hozzáférés:

2.1.1. az Intézmény által használt hálózati rendszerben az azonosítás olyan hozzáférés felhasználásával történik, melynek részei a felhasználó név és a jelszó, melyek együttesen érvényesek,

2.1.2. a felhasználó nevet és jelszót a rendszergazda hozza létre az intézményvezető utasítására.

2.1.3. belépési jelszó megváltoztatására az intézményvezető felhatalmazása alapján az informatikus jogosult. A jelszavakat 3 havonta kötelező megváltoztatni.

2.2. Alkalmazásszintű bejelentkezés:

Ha egy alkalmazás futtatásához vagy annak adatainak eléréséhez felhasználói azonosításra van szükség és az alkalmazás önálló felhasználó-kezeléssel rendelkezik, akkor alkalmazásszintű bejelentkezésre van szükség.

2.3. A hozzáférés felhasználási feltételei:

2.3.1. A személyre szabott jelszót a felhasználó köteles titokban tartani, azt másnak átadni, leírni vagy egyéb formában rögzíteni tilos,

2.3.2. az intézmény hálózatában, alkalmazásaiban használt jelszavak internetes hálózatban való alkalmazása nem javasolt,

2.3.3. a felhasználó felelősséggel tartozik a személyre szóló hozzáférésért,

2.3.4. a kitudódott jelszó illetéktelen felhasználásából eredő kár és felelősség a hozzáférés tulajdonosát terheli,

2.3.5. a hozzáférés jelszavait a felhasználó személyének változásakor azzal egyidejűleg meg kell változtatni,

2.3.6. amennyiben egy számítógépet többen használnak, a felhasználóváltás funkcióval ki, illetve be kell lépni,

2.3.7. amennyiben többen használnak egy számítógépet minden az adott számítógéphez rendelt felhasználó felelős az adatok védelméért.

2.4. A hozzáférés korlátozása:

2.4.1. A biztonsági előírások és az Intézmény érdekei megkövetelik, hogy visszaélések vagy azok gyanúja esetén a felhasználó rendszerhez, alkalmazáshoz való hozzáférését korlátozzák, amelyről az intézményvezető gondoskodik,

2.4.2. a korlátozás a következő esetekben indokolt: hozzáférés jogosulatlan használatakor, visszaélés, károkozás esetén, a foglalkoztatási jogviszony megszűnése esetén, a felhasználó vagy felettese indokolt kérése alapján,

2.4.3. a korlátozás az intézményvezető engedélyével oldható fel.

2.5. Felelősség:

2.5.1. A hozzáférés felhasználási feltételeit, vagy jelen Szabályzat valamely rendelkezéseit ismételten megszegő felhasználót az intézményvezető felelősségre vonhatja,

2.5.2. jelen Szabályzatba ütköző bármely magatartást tanúsító, valamint szándékos vagy elvárható gondosságot elmulasztó tevékenységgel kárt okozó az előidézett vagyoni és nem vagyoni kárért felelősséggel tartozik.

3. Az informatikai rendszer védelme

3.1. A védelem elemei és eszközei:

3.1.1. Környezeti infrastruktúra, hardver elemek, adathordozók, szoftver elemek, dokumentumok, adatok, a rendszerelemekkel kapcsolatban álló személyek.

3.1.2. A védelmi intézkedések kiterjednek, a rendszer elemeinek elhelyezésére szolgáló helyiségekre, az alkalmazott hardver eszközökre és azok működési biztonságára, az informatikai eszközök üzemeltetésre vonatkozó okmányokra és dokumentációkra, az adatokra és adathordozókra a megsemmisülésükig, illetve a törlésre szánt adatok felhasználásáig, az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszerszoftverek tartalmi és logikai egységére, előírásszerű felhasználhatóságára, reprodukálhatóságára,

3.1.3. a személyhez fűződő és vagyoni értékű jogokra.

3.2. Fizikai védelem:

3.2.1. Informatikai rendszerek (kivéve a kliensek számára biztosított számítógép-használat, valamint a recepció érintett számítógépei) zárható irodai helyiségekben tárolható,

3.2.2. a monitorokat úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelenek ne láthassák,

3.2.3. az adatkezelés során az adatkezelésre használt számítástechnikai és manuális eszközöket védeni kell az illetéktelen hozzáférés, megismerés, lemásolás, megváltoztatás, törlés vagy az adathordozó eltulajdonításától.

3.2.4. a számítógépes infrastruktúrát védendő az Intézményt központi riasztóval kell ellátni, mely kapcsolódik a Zuglói Közbiztonsági non-profit Kft (továbbiakban: ZKNP) központi jelző rendszeréhez, amely bármely behatolás kísérletének jelzése esetén a helyszínre vonul, és az eseménynek megfelelően intézkedik,

3.2.5. az épületbe meghatározott személyek csak a személyesen kiadott belépési kóddal léphetnek be, amelyet a kód, dátum és időpont szerint rögzítésre kerül,

3.2.6. az épületben csak nyitvatartási időben lehet tartózkodni, kivéve, olyan szakmai esemény, rendezvény esetén, amelyről a szakmai vezetők, az intézményvezető, tudomással bír, és a szolgáltatás szükséges eseménye,

3.2.7. nyitvatartási időn túl az intézmény irodáiba, számítógépeket tartalmazó helyiségeibe indokolatlanul tartózkodni tilos, illetéktelen nem léphet be,

3.2.8. nyitvatartási időben az intézmény számítógépeket tartalmazó helyiségeiben ügyfél nem tartózkodhat.

3.3. Hardver védelem:

3.3.1. A berendezések üzemeltetése csak hibátlan állapotban és rendeltetésnek megfelelően történhet,

3.3.2. a szükséges karbantartási és szervizelési munkák a költségvetésben biztosított feltételek, és a szerződésben megállapított normák szerint végezhetők el,

3.3.3. a számítástechnikai eszközöket javításra vagy más célból átadni csak elismervény ellenében lehet, az átadott eszközön található adatok védelméről az eszközt használó személy, a fenntartó által kezelt központi számítógép beszerzés, selejtezés esetén, a fenntartó által kijelölt átvevő gondoskodik,

3.3.4. a számítástechnikai rendszer vagy bármely eleme csak az intézményvezető felhatalmazásával változtatható meg, minden eszköz cseréjének idejét dokumentálni kell.

3.4. Szoftver és program védelem:

3.4.1. Az Intézményben csak hivatalosan beszerzett, írásbeli igazolásokkal ellátott szoftvereket lehet használni,

3.4.2. a beszerzett és használatban lévő szoftverek védelme az Intézmény valamennyi felhasználójának kötelessége,

3.4.3. az intézményben használt alkalmazásokat, adatokat, külső, illetéktelen személyekkel megismertetni, lemásolni, átadni, tilos,

3.4.4. a szoftver alkalmazása során, minden eltérésről értesíteni kell a rendszergazdát, a szoftvert üzemeltető cég megbízottját, az intézményvezetőt,

3.4.5. az intézményi számítógépekre idegen programokat, a rendszerre veszélyt jelentő adatokat, alkalmazásokat, internetes tartalmakat (zenét, filmet stb.) letölteni tilos,

3.4.6. a rendszergazda biztosítja, hogy a rendszerszoftver naprakész állapotban legyen, és a segédprogramok, programkönyvtárak hozzáférhetők legyenek,

3.4.7. a rendszerszoftver módosítását csak a rendszergazda végezheti el, a változtatásokról nyilvántartást kell vezetnie,

3.4.8. a számítógépekre bármilyen program csak a rendszergazda és az intézményvezető engedélyével telepíthető fel.

3.5. Mentés, fájlok védelme:

3.5.1. A munka során létrehozott általános (Word, Excel stb.) dokumentumok mentése az

3.5.2. azt létrehozó felhasználók feladata,

3.5.3. a felhasználók számítógépén létrehozott adatok, dokumentumok biztonsági mentést

3.5.4. a felhasználónak kell készítenie, az archiválásban a rendszergazda nyújt segítséget, a vásárolt szoftverekről biztonsági másolatot kell készíteni.

3.5.5. A számítógépek működési biztonsága:

3.5.6. Célszerű szünetmentes áramforrást használni, amely megvédi a berendezéseket az

3.5.7. áramingadozástól, az áramkimaradás esetén az adatvesztéstől,

3.5.8. a hálózati vezetékeket mindennemű sérüléstől óvni kell, a hálózat megbontását csak a rendszergazda végezheti el.

3.6. Vírusvédelem:

3.6.1. Az intézmény számítógépeinek, adathordozóinak vírusvédelméről folyamatosan gondoskodni kell, a rendszergazda feladata az időszakos ellenőrzés, és szükség esetén a beavatkozás,

3.6.2. amennyiben a felhasználó vírusra utaló jelenséget tapasztal, köteles jelezni a rendszergazdának, az intézményvezetőnek,

3.6.3. nem irtható vírus esetén a rendszergazda köteles a vírusvédelmi szoftver ügyfélszolgálatához fordulni, és a lehető legrövidebb időn belül a kártékony adatállomány eltávolítására megoldást találni.

3.7. Kárelhárítás:

Vészhelyzet esetén (elemi csapás, közüzemi szolgáltatásra visszavezethető, vagy emberi mulasztás miatt kialakuló súlyos zavarok) esetén bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell végrehajtani:

a) a még használható anyagot le kell menteni,
b) biztonsági mentésekből, háttértárakról a megsérült adatokat vissza kell állítani,
c) károkozás ellen védett helyiségben és gépen kell a műveleteket elvégezni.

4. Cookie-k alkalmazása és Facebook profil fenntartása

4.1. Az intézmény a honlapot meglátogató felhasználó számítógépén adatcsomagot (ún. „cookie"-t) nem helyez el.

4.2. Az intézmény hivatalos facebook profilt tarthat fenn, amelyen „like”-oló, illetve „követő” felhasználók lehetővé teszik, hogy a saját oldalukon közzétett adatokat a szolgáltató megismerje. A szolgáltató a megismert adatokat nem gyűjti, azokról nem vezet nyilvántartást és nem is továbbítja.

4.3. Az intézmény a facebook profilt az ügyfelek gyors és közvetlen tájékoztatására használja, konkrét ügyre vonatkozó, személyes adatot tartalmazó üzenetváltásra nem kerül sor.

4.4. Az intézmény hivatalos facebook profilt az intézmény hivatalos e-mail címével kell regisztrálni, az oldalhoz hozzáférést biztosító jelszót és felhasználónevet az intézményvezető őrzi.

5. IQtató iktatási program használata

5.1. Az intézmény az IQtató iktatási programot alkalmazza, mely moduláris felépítésű, terhelhető komplex iktató program és ügyviteli rendszer. Legfőbb funkciói: érkeztetés, iktatás tetszőleges iktatószám képzéssel, fájlok csatolása, dossziézás, ügyintézői feljegyzések kezelése, elektronikus eseménykezelés határidőkkel, felelősökkel, likviditás menedzsment támogatása, archiválás, irattárazás.

5.2. Az elektronikus keresés lehetővé teszi, hogy akár adattöredék esetén is (névrészlet, fél telefonszám, egy szótöredék stb.) a program pillanatok alatt megtalálja a keresett iratot, nevet, céget, telefonszámot.

5.3. Az iktatóprogram jelszóval védett, a programhoz hozzáféréssel az intézményvezető, a helyettes, és az asszisztensek rendelkeznek.

6. Elektronikus megfigyelőrendszer alkalmazásához, képfelvételek készítéséhez kapcsolódó szabályok

6.1. A megfigyelő kamerás rendszerek útján rögzített és kezelt felvételek személyes adatnak minősülnek.

6.1.1. A megfigyelőrendszer alkalmazásának célja az emberi élet, a testi épség, a személyi szabadság védelme, a vagyonvédelem. Az elhelyezett kamerák látószöge, a célhoz kötöttség elvének megfelelően csak az Intézmény használatban lévő területein helyezhető el.

6.1.2. Az alkalmazott kamerák látószögébe főbejárat, a recepció, a kapcsolatügyeleti bejárat, a szerverszoba helyezkedik el, mint olyan helyiségek, amelyeknél a korábbi tapasztalatok alapján (támadás, túszejtés, garázdaság, engedélynélküli tartózkodás) fokozott védelem szükséges.

6.1.3. A ZKNP kezelésébe és karbantartásába tartoznak a kihelyezett kamerák, a kamerák által közvetített képfelvételek törlése, tárolása, az általuk kihelyezett, jelszóval védett adattárolón történik, amelyhez csak a ZKNP megbízottjának van hozzáférése.

6.1.4. Bármely beavatkozás, mint a képfelvételek megtekintése, a képfelvételek tárolása csak indokolt esetben (pld. bűncselekmény gyanúja, hatósági, bírósági határozat), csak az Intézményvezető és a szakmai vezető engedélyével történhet.

6.1.5. A képfelvételek megtekintése, visszanézése csak az intézményvezető, a szakmai vezető, és indokolt esetben az érintett munkavállaló jelenlétében történhet.

6.1.6. Ügyfél sértetti minőségben elsősorban a bűncselekmény felderítésére határkörrel rendelkező szervhez kell fordulnia, és a nevezett szervek képfelvétel jogszerű kikérésén keresztül férhet hozzá, tekinthet be a felvételek azon tartományához, amely a bizonyításhoz szükséges.

6.1.7. Ügyfélre irányuló bűncselekmény gyanúja esetén, a cselekmény felderítése miatt, vagy akinek a joga vagy jogos érdeke bizonyíthatóan fennáll az Intézményvezetőtől kérhetik az adott intervallumban keletkezett képfelvételek 30 vagy 60 napig való tárolását, amelyet külön adathordozón, biztonsági zárral ellátott helyen kell a jogszerű felhasználásig tárolni.

6.1.8. Főszabályként a kamerák által készített felvételek a rögzítéstől számított 3 munkanapig tárolhatók, majd törlésre kerülnek.

6.1.9. Bíróság vagy más hatóság megkeresésére a rögzített kép-, hang-, valamint kép- és hangfelvételt, valamint más személyes adatot a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni. Amennyiben megkeresésre attól számított harminc napon belül, hogy a megsemmisítés mellőzését kérték, nem kerül sor, a rögzített képfelvételt meg kell semmisíteni, illetve törölni kell, kivéve, ha arra indokolt körülmény miatt a tárolás határideje még nem járt le.

6.2. Képfelvételek készítése, nyilvánosságra hozatala:

6.2.1. Az Infotv. szerint egy ember arca, képmása személyes adatnak minősül, képfelvétel készítése, valamint az adaton elvégzett bármely művelet pedig adatkezelésnek minősül, amelyhez külön törvényi felhatalmazás hiányában, az érintett hozzájárulása szükséges.

6.2.2. Kiskorú személyek esetében, 16 éves kor előtt, minden esetben szükség van a törvényes képviselő előzetes vagy utólagos jóváhagyására, ellenkező esetben az adatkezeléshez adott hozzájárulás semmisnek tekinthető, és az adatkezelés jogellenes. 16 évet betöltött kiskorú önállóan nyilatkozhat a személyes adatainak felhasználásról.

6.2.3. A hozzájárulás az érintettől származó kifejezett nyilatkozat, amely alapvetően megadható írásban, szóban vagy ráutaló magatartással. A hozzájárulásnak önkéntesnek, határozottnak és megfelelő tájékoztatáson alapulónak kell lennie, e három követelménynek egyidejűleg kell fennállnia.

6.2.4. Írásbeli hozzájárulás csak különleges, szenzitív adatokat illetően kötelező.

6.2.5. A főszabály, hogy bármely képfelvétel készítése esetén az érintettek hozzájárulását, kiskorú esetén a szülő, gondozó engedélyét kell kérni.

6.2.6. A képfelvételhez kért hozzájárulás nem jelent egyben felhatalmazást a fényképek nyilvánosságra hozatalára is, az ahhoz való hozzájárult külön kell kérni.

6.2.7. Olyan rendezvényeken készült képfelvételek, amelyek tömegrendezvénynek minősülnek, és az ábrázolás módja nem egyedi (a rendezvény az Intézmény átláthatóságát szolgálja, jellemzőit mutatja) nyilvános rendezvényen készült tömegfelvételnek minősül, amely közzétételéhez nem feltétlenül szükséges az érintettek hozzájárulását beszerezni.

6.2.8. Tömegfelvételnek nem minősülő képfelvételek, azok közzétételének szándéka esetén, az érintettek, kiskorú szüleinek, gondozójának hozzájárulását kell kérni.

6.2.9. A törvényes feltételek megléte mellett, a képfelvétel készítése, közzététele kapcsán mindenképpen mérlegelni kell, hogy a kiskorú jelen és jövőbeli érdekeit nem sérti-e a képfelvétel készítése, közzététele, s csak e mérlegelés után ajánlatos a képfelvétellel kapcsolatos lépéseket megtenni.

VI. Az adatvédelmi incidens és kezelése

1. Az adatvédelmi incidens észlelése

1.1. Az a munkavállaló, aki az intézmény által kezelt vagy feldolgozott személyes adatokkal kapcsolatban adatvédelmi incidenst, azaz személyes adat jogellenes kezelését vagy feldolgozását, így különösen jogosulatlan hozzáférést, megváltoztatást, továbbítást, nyilvánosságra hozatalt, törlést vagy megsemmisítést, valamint véletlen megsemmisülést és sérülést észlel, azt köteles az észleléstől számított 60 percen belül a közvetlen vezetője útján haladéktalanul bejelenteni, megadva a nevét, az incidens tárgyát, valamint azt, hogy az incidens informatikai rendszert érint-e. A bejelentő további olyan információkat is megadhat, amelyeket az incidens beazonosítása, megvizsgálása szempontjából lényegesnek ítél.

1.2. Amennyiben az adatvédelmi incidens informatikai rendszert érintően következett be, akkor az intézményvezető tájékoztatja az informatikai rendszert felügyelő személyt.

1.3. Az intézményvezető - informatikai rendszert érintő incidens esetén az informatikai rendszert felügyelő személlyel együttműködve – a bejelentést megvizsgálja, a bejelentőtől adatszolgáltatást kér, amelyet a bejelentő köteles haladéktalanul, de legkésőbb 2 munkanapon belül teljesíteni.

1.4. Az adatszolgáltatásnak tartalmaznia kell

a) az incidens bekövetkezésének időpontját és helyét,

b) az incidens leírását, körülményeit, hatásait

c) az incidens során kompromittálódott adatok körét, számosságát,

d) a kompromittálódott adatokkal érintett személyek körét

e) az incidens elhárítása érdekében tett intézkedések leírását,

f) a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását

1.5. Az adatvédelmi tisztviselő javaslatai alapján az intézményvezető az incidens jellegétől függő intézkedéseket megteszi az adatvédelmi incidens negatív következményeinek elhárítása és a hasonló incidensek megelőzése érdekében.

2. Az adatvédelmi incidens bejelentése

2.1. Az adatvédelmi incidenst az intézményvezető indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órán belül, hogy az adatvédelmi incidens az adatkezelő tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak (Az Adatvédelmi Incidensbejelentő rendszer elérhetősége: https://naih.hu/adatvedelmi-incidensbejelentorendszer.html), kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal (ide értve az alacsony kockázatot is) a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

2.2. A bejelentésben legalább:

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

b) közölni kell a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

d) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

2.3. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. Az érintett tájékoztatásában fel kell tüntetni mindazokat az adatokat, melyekről a felügyeleti hatóság tájékoztatva lett.

3. Az adatvédelmi incidens kockázatosságának, súlyosságának megállapítása

A kockázatosság megállapításához az intézmény az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) módszertani útmutatójában közzétett ajánlást követi, azonban azt nem kizárólagosan alkalmazza, az adott eset összes körülményéhez igazítottan az intézmény további, a jelen szabályzatban nem nevesített értékelési szempontokat is figyelembe vehet.

3.1. Az értékelés főbb körülményei:

Data Processing Context (DPC):	A megsérült adatok fajtáinak vizsgálata
Ease of Identification (EI):	Az érintett azonosíthatóságának foka
Circumstances of breach (CB):	A jogsértés körülményeinek leírása, kiterjesztve a szándékosság vizsgálatára, a biztonság elvesztésére

A DPC lényege, hogy egy adott adatkészlet kritikusságát egy adott feldolgozási kontextusban értékeli.

Az EI a DPC korrekciós tényezője. Az adatfeldolgozás általános kritikussága az EI értékétől függően csökkenhet, azaz minél alacsonyabb a pontszáma, annál alacsonyabb lesz az összpontszám. Az EI és a DPC kombinációja adja meg az adatvédelmi incidens súlyosságának (SE) kezdeti pontszámát.

A CB számszerűsíti a jogsértés konkrét körülményeit, amelyek jelen lehetnek egy adott helyzetben.

Az adott adatvédelmi incidens súlyossága az alábbi formula alapján állapítható meg:

SE = DPC x EI + CB

A végeredmény az alábbi négy tartományba osztható:

SE<2	alacsony kockázat	Az érintettekre vagy nincs hatással, vagy legfeljebb néhány kellemetlenséggel találkozhatnak, amelyek minden probléma nélkül leküzdhetők (az információk újbóli bevitele stb.).
2≤SE<3	közepes kockázat	Az egyének jelentős nehézségeket tapasztalhatnak, amelyeket képesek lesznek leküzdeni (többletköltségek, szolgáltatásokhoz való hozzáférés megtagadása, félelem, megértés hiánya, stressz stb.).
3≤SE<4	magas kockázat	Az egyének jelentős következményekkel is szembesülhetnek (feketelistázás, vagyoni kár, munkahely elvesztése, egészségromlás stb.).
4≤ SE	nagyon magas kockázat	Az egyének jelentős vagy akár visszafordíthatatlan következményekkel is szembesülhetnek, amelyeket nem lehet, vagy számottevő nehézség árán lehet leküzdeni (pénzügyi nehézségek, például jelentős adósság vagy munkaképtelenség, hosszú távú pszichés vagy fizikai betegségek, halál stb.).

3.2. A DPC pontszámának meghatározása:

1. lépés

Meg kell határozni az adatvédelmi incidenssel érintett adatok körét, melyet az alábbi négy kategóriába kell illeszteni és meg kell határozni az előzetes alap DPC pontszámot kapunk.

Az adatok négy kategóriába sorolandóak: egyszerű, viselkedési, pénzügyi és különleges adatok.

2. lépés

Meghatározni azon tényezők előfordulását, amelyek növelhetik vagy csökkenthetik az alap pontszámot (pl. adatmennyiség, az ellenőrök vagy az egyének sajátosságai, az adatok pontatlansága, a nyilvános hozzáférhetőség (a jogsértés előtt), az adatok jellege).

Amennyiben előfordulnak ilyen tényezők, ennek megfelelően növelni / csökkenteni kell az alap pontszámot az alábbi táblázatok segítségével.

Egyszerű adatok	életrajzi adatok, elérhetőségek, teljes név, adatok az oktatásról, a családi életről, a szakmai tapasztalatról	Pontszám
	Előzetes alapérték: ha a jogsértés "egyszerű adatokat" tartalmaz, és az adatkezelő nem ismer semmilyen súlyosbító tényezőt.	1
	Amikor az adatok lehetővé teszik a profilalkotást, vagy az egyén szociális / pénzügyi helyzetére vonatkozó feltevéseket.	2
	Amikor az adatok feltételezhetővé teszik az egyén egészségi állapotát, szexuális preferenciáit, politikai vagy vallási meggyőződését	3
	Amikor az egyén bizonyos jellemzői (például sérülékeny csoportok, kiskorúak) miatt az információ fontos lehet személyes biztonságuk vagy fizikai / pszichológiai állapotuk szempontjából.	4

Viselkedési adatok	Hely, forgalmi adatok, személyes preferenciákkal és szokásokkal kapcsolatos adatok	Pontszám
	Előzetes alapérték: Amikor a jogsértés "viselkedési adatokat" érint és az adatkezelő nem ismer súlyosító vagy enyhítő tényezőket	2
	Amikor az adathalmaz jellege nem nyújt lényeges betekintést az egyén viselkedési információihoz, vagy az adatok könnyen gyűjthetők (a jogsértéstől függetlenül) nyilvánosan elérhető forrásokon keresztül (például a webes keresésekből származó információk kombinációja)	1
	Amikor a viselkedési adatok mennyisége és / vagy a főbb jellemzői olyanok, hogy az egyén profilja létrehozható, részletes információkkal szolgálva mindennapi életéről és szokásairól.	3
	Amikor a különleges adatokon alapuló profil létrehozható	4

Pénzügyi adatok	Bármilyen típusú pénzügyi adatok (például jövedelem, pénzügyi tranzakciók adatok, bankszámlakivonatok, befektetések, hitelkártyák, számlák stb.). Tartalmazza a pénzügyi információkhoz kapcsolódó szociális jóléti adatokat.	Pontszám
	Előzetes alapérték: Amikor a jogsértés "pénzügyi adatokat" érint és az adatkezelő nem ismer súlyosító vagy enyhítő	3

	tényezőket.	
	Amikor az adathalmaz jellege nem nyújt lényeges betekintést az egyén pénzügyi információiba (pl. az a tény, hogy egy személy egy bizonyos bank ügyfele, további részletek nélkül)	1
	Amikor az adott adatkészlet tartalmaz néhány pénzügyi információt, de még mindig nem nyújt jelentős betekintést az egyén pénzügyi helyzetébe (például egyszerű bankszámlaszámok további részletek nélkül)	2
	Amikor az adott adatkészlet természete és / vagy mennyisége miatt teljes körű pénzügyi (például hitelkártya) információkkal szolgálnak, amelyek lehetővé tehetik a csalást vagy részletes társadalmi / pénzügyi profil létrehozását	4

Különleges adatok	Bármilyen típusú különleges személyes adatok	Pontszám
	Előzetes alapérték: Amikor a jogsértés "különleges személyes adatokat" érint és az adatkezelő nem ismer súlyosító vagy enyhítő tényezőket.	4
	Amikor az adatkészlet természete nem nyújt lényeges betekintést az egyén viselkedési információihoz, vagy az adatok könnyen gyűjthetők (a jogsértéstől függetlenül) nyilvánosan elérhető forrásokon keresztül (például a webes keresésekből származó információk kombinációja)	1
	Amikor az adatok jellege általános feltételezésekhez vezethet	2
	Amikor az adatok jellege az érzékeny információkra vonatkozó feltételezésekhez vezethet	3

Amennyiben az adatvédelmi incidenssel érintett adatok egynél több kategóriába tartoznak, a fenti lépéseket minden egyes kategóriára alkalmazni kell. Ezekben az esetekben a legmagasabb pontszámot kell figyelembe venni az SE meghatározásához.

Az adatvédelmi tisztviselő a DPC alap pontszámot a fentiektől eltérítheti, az új pontszámot magyarázattal kell alátámasztani, amely leírja a jogsértés egyedi körülményeit és azok hatását.

3.3. Az EI pontszám meghatározása

Az érintett azonosíthatóságának fokát négy csoportba oszthatjuk

Csoport	Pontszám	Leírás
Elhanyagolható azonosíthatóság	0,25	Amikor nincs más információ az egyénről, vagy nem lehet további információkat találni
Korlátozott azonosíthatóság	0,5	Amikor további adat szükséges az egyén beazonosításához
Jelentős azonosíthatóság	0,75	Amikor az azonosítás további személyazonosító adatokat tár fel az egyénről
Teljes azonosíthatóság	1	Amikor az egyén kétséget kizáróan beazonosítható

Az adatvédelmi tisztviselő az EI pontszámot a fentiektől eltérítheti, az új pontszámot magyarázattal kell alátámasztani, amely leírja a jogsértés sajátos körülményeit és azok hatását.

3.4. A CB pontszám meghatározása

A CB pontszám meghatározásakor a biztonság sérülését (titoktartás, integritás, elérhetőség) és rosszhiszemű szándékosságot vesszük figyelembe, melyek kiegészítik a DPC és az EI-t az alábbiak szerint

3.4.1. Titoktartás sérülése: A titoktartás sérülése akkor következik be, amikor az információkat olyan felek érik el, akik nem jogosultak az adathoz hozzáférni. A titoktartás sérülésének mértéke a közzététel terjedelmétől, azaz az adathoz jogszerűen hozzáférők számától függ.

+ 0	Nyilvános adatok
+ 0,25	Az érintett, az intézményvezető és foglalkoztatottak által elérhető adat (pl. a feladatok teljesítéséhez kapcsolódó adatok)
+ 0,5	Intézményvezető által elérhető adat (pl. jelszavak)

3.4.2. Integritás sérülése: Az integritás sérülése akkor történik meg, amikor az eredeti információ megváltozik, és az adatok helyettesítése hátrányos lehet az egyén számára. A legsúlyosabb helyzet akkor fordul elő, amikor jelentős a kockázata annak, hogy a megváltozott adatokat olyan módon használják fel, amely károsíthatja az egyént.

+ 0	Adat megváltozása illegális tevékenység azonosítása nélkül
+ 0,25	A megváltoztatott adat visszaállítható
+ 0,5	A megváltoztatott adat nem visszaállítható

3.4.3. A rendelkezésre állás hiánya: A rendelkezésre állás hiánya akkor következik be, amikor az eredeti adat nem érhető el akkor, amikor szükség lenne rá. Ez lehet átmeneti (a hozzáférés helyreállítható idővel) vagy végleges (az adatokat nem lehet visszaállítani).

+ 0	Minden nehézség nélkül visszaállítható
+ 0,25	Átmenetileg nem hozzáférhető
+ 0,5	Véglegesen nem hozzáférhető

3.4.4. Rosszhiszemű szándékosság: Ez az elem megvizsgálja a jogsértés okát, annak emberi, technikai jellegét, annak szándékos vagy gondatlan voltát. A nem rosszhiszemű jogsértések magukban foglalják a véletlen sérülést, a nem megfelelő ártalmatlanítást, az emberi hibákat és a szoftveres hibákat vagy a hibás konfigurálást. A rosszindulatú jogsértések magukban foglalják az érintettek károsítását célzó lopás és hackelés eseteit.

+ 0,5	A rosszhiszemű szándékosság megállapítható

3.5. Adatvédelmi incidensek nyilvántartása

Az adatvédelmi incidensről az adatvédelmi tisztviselő a melléklet szerinti adattartalommal nyilvántartást vezet. A nyilvántartásba történő bejegyzésről az adatvédelmi tisztviselő értesítést küld az intézményvezetőnek.

VII. Adatbiztonság

Az adatbiztonsági fejezet tartalmazza a biztonsági intézkedéseket annak érdekében, hogy a kommunikációs, információs és más elektronikus és analóg rendszerekben tárolt, feldolgozott és átvitt adatok védelme biztosítva legyen a bizalmasság, sértetlenség és rendelkezésre állás elvesztésével szemben, függetlenül az események szándékos vagy véletlen voltától.

1. Az adatbiztonság alapelvei

1.1. Bizalmasság elve

Az adatok bizalmasságának megvédése, annak garanciája, hogy az adatokhoz jogosulatlanul vagy illetéktelenül nem juthatnak hozzá.

1.2. Sértetlenség elve

Az adatok sértetlensége (integritása) azt jelenti, hogy azokat csak az arra jogosultak változtathatják meg.

1.3. Rendelkezésre állás elve

Annak a biztosítása, hogy az adatok mindig elérhetőek legyenek, jogtalanul ne semmisítsék meg, ne töröljék azokat.

2. Az adatbiztonsági ellenőrzés

2.1. Az intézmény az általa kezelt személyes adatok biztonságának megteremtéséhez szükség szerint, de évente legalább egy alkalommal adatbiztonsági ellenőrzést hajt végre, melynek keretében az adatok biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságát kell tesztelni, felmérni, értékelni.

2.2. Az adatbiztonsági ellenőrzést az adatvédelmi tisztviselő vezeti. Az ellenőrzésről jegyzőkönyv felvételére kerül sor. A jegyzőkönyvmintát a 16. számú melléklet tartalmazza. A jegyzőkönyvet az ellenőrzés során jelen lévő személyek aláírásukkal látják el. A jegyzőkönyv alapján az adatvédelmi tisztviselő értékelést és intézkedési tervet készíttet, melyet átad az intézményvezetőnek.

3. Az adatbiztonsági ellenőrzés folyamata:

a. A védelmi igény feltárása: ki kell választani az intézmény lényeges adatkezeléssel érintett rendszereit, amelyeket az intézmény védeni akar.
b. Fenyegetettség-elemzés: azoknak a fenyegető tényezőknek a feltárása, amelyek az előbbi adatokra, alkalmazásokra veszélyesek lehetnek.
c. Kockázatelemzés: a fenyegető tényezők hatását kell megvizsgálni az informatikai rendszerre, meghatározni a lehetséges károk bekövetkezésének gyakoriságát és a kárértékeket.
d. Kockázatkezelés: a megfelelő intézkedések kiválasztása és értékelése a károk csökkentésére.

3.1. A védelmi igény feltárása

3.1.1. Az intézményi adatkezelés védelme három összetevőjű, áll fizikai védelemből, eljárásvédelemből és informatikai védelemből.

3.1.2. A fizikai védelem a helyiségek, objektumok védelméből, valamint a papír alapú és más hagyományos dokumentumok védelméből áll.

3.1.3. Az eljárásvédelem az adatvédelmi és adatbiztonsági szabályok meghatározása, betartása és betartásának ellenőrzését, az intézményi dolgozók tudatosságának fejlesztését foglalja magában.

3.1.4. Az informatikai védelem a hardver és szoftvervédelemből áll.

3.2. Fenyegetettség-elemzés

3.2.1. Azoknak a fenyegető tényezőknek a feltárása, amelyek a védendő adatokra, alkalmazásokra veszélyesek lehetnek. Az adatbiztonsági ellenőrzési jegyzőkönyvben a fenyegető tényezőket táblázatos formában rögzíteni kell.

3.2.2. Az adatbiztonságot veszélyeztető főbb kockázati elemek: A külső fenyegető tényezők:

a) természeti katasztrófa;
b) külső személy által elkövetett erőszakos cselekmény;
c) közműellátási zavarok;
d) külső személy tartózkodása az objektumban;
e) védelmi berendezések technikai hibája, vészhelyzet (pl. rövidzárlat, tűz, csőtörés).

3.2.3. A hardvereszközök fenyegetettsége:

a) műszaki jellegű hibák, rendellenességek;
b) káros környezeti hatás (feszültségingadozás, szennyeződés, elektromágneses sugárzás, elektrosztatikus feltöltődés);
c) a berendezések kezelésével, karbantartásával kapcsolatos hibák;
d) perifériákhoz való illetéktelen hozzáférés;
e) a berendezések manipulálása, rongálása, lopás;
f) az eszköz elhelyezésére szolgáló helyiség vagy munkahely helytelen kiválasztása.

3.2.4. Az adathordozók veszélyeztetettsége:

a) gyártási hiba;
b) károsodás nem szabályszerű tárolás vagy kezelés miatt;
c) ismeretlen vagy kétes eredetű adathordozó alkalmazása;
d) kontroll nélküli hozzáférés az adathordozókhoz, másolás;
e) saját adathordozó ellenőrzés nélküli alkalmazása szolgálati vagy magáncélra (vírusveszély, illegális másolás).

3.2.5. Az iratokhoz, informatikai dokumentációkhoz kapcsolódó kockázati elemek:

a) a rendszerdokumentáció teljes vagy részleges hiánya;
b) az iratok követhető rendszerezettségének hiánya;
c) az aktualitás hiánya;
d) jogosulatlan, hibás, ismeretlen eredetű változtatás;
e) kontroll nélküli hozzáférés, sokszorosítás.

3.2.6. A szoftverekhez kapcsolódó veszélyforrások:

a) nem jogtiszta, ismeretlen szoftver alkalmazása;
b) szoftverhiba;
c) jogosulatlan hozzáférés, másolás lehetősége;
d) szoftver ellenőrizetlen bevitele az informatikai rendszerbe;
e) vírusveszély;
f) szándékos vagy gondatlan kezelési, karbantartási hiba;
g) a szoftver sérülése, károsodása hardverhiba miatt;
h) dokumentációk hiánya, sérülése.

3.2.7. Az alkalmazói tevékenységgel, adatokkal összefüggő kockázati elemek:

a) adatvesztés, károsodás hardver-vagy szoftverhiba miatt;
b) teljes vagy részleges adatvesztés hibás adathordozó miatt;
c) a jogosult adatkezelő által szándékosan vagy tévedésből végzett adattörlés, módosítás;
d) jogosulatlan adatkezelő által végzett másolás, törlés, módosítás;
e) hibás adatkezelés ismerethiány miatt;
f) kezelési előírások be nem tartása, oktatás hiánya.

3.2.8. Fenyegető tényezők a kommunikáció területén:

a) jogosulatlanok bejutása a hálózatba nem ellenőrizhető csatlakozás révén;
b) hálózati hardverek és szoftverek szándékos vagy gondatlan manipulálása;
c) adatforgalom lehallgatása;
d) váratlan forgalmazási akadályok, az átvitelt zavaró befolyások;
e) üzenetvesztés, üzenet megváltoztatása;
f) az adatátviteli eszközök sérülése, károsodása.

3.2.9. Személyhez fűződő veszélyforrások:

a) hibás adatkezelés ismerethiány vagy fáradtság, figyelmetlenség miatt;
b) az adatkezelésre vonatkozó előírások figyelmen kívül hagyása hiányos „biztonságtudat” miatt, a fenyegetettség lebecsülése;
c) szándékosan hibás adatkezelés belső késztetés vagy külső ráhatás következményeként;
d) jogosulatlan hozzáférés;
e) az ellenőrzés hiánya

3.3. Kockázatelemzés

3.3.1. A 3.1. és a 3.2. pontokban meghatározott tényezők összevetése és a tudomány mindenkori állásának megfelelő előfordulásának meghatározása.

3.3.2. Az előfordulási lehetőségét a valószínűsége szerint 4 csoportba osztjuk.

a) nem fordulhat elő rendes ügymenetben (pl. háború, államcsőd)
b) kismértékű előfordulási lehetőség (pl. áramszünet, viharkár)
c) reális előfordulási lehetőség (pl. betörés, vírusfertőzés)
d) minden bizonnyal be fog következni (pl. téves adatfelvétel)

3.3.3. Az adatbiztonság ellenőrzési jegyzőkönyvben meghatározott fenyegető tényezőket értékelni kell a 3.2.2. pont szerinti besorolás szerint. A kockázat értékelésére külső szakember igénybe vehető, az informatikai szempontú kockázatok értékelését az intézmény informatikusa végzi.

3.4. Kockázatkezelés

Meg kell határozni mindazokat a lehetséges intézkedéseket, melyekkel a kockázat minimálisra csökkenthető. Az intézkedések végrehajtására határidőt kell megjelölni.

Az intézményvezető intézkedik a szükséges intézkedések végrehajtásának megtervezése és kivitelezése iránt.

4. Adatbiztonsági előírások és eljárási szabályok

4.1. Beléptetés és elektronikus megfigyelési rendszer

4.1.1. Az intézmény és telephelyeire történő beléptetés megszervezése az intézményvezető, telephelyvezető feladata. Alkalmazható elektronikus megfigyelési rendszer, illetve az épületbe belépő személyek nevének, személyi igazolványszámának rögzítésével. A beléptetéshez kapcsolódó adatkezelési tájékoztatót a melléklet tartalmazza.

4.1.2. Az intézmény elektronikus megfigyelési rendszert működtethet. A kamerák látószögei a célterületre irányulhatnak csak, így kizárólag saját tulajdont vagy használatban lévő területet figyel meg. A kihelyezett kamerák helyét és a megfigyelt terület leírását a melléklet szerinti tartalommal kerül felvételre.

4.1.3. Az intézmény nem rendelkezhet olyan kamerával, amely kizárólag egy munkavállalót vagy ügyfelet és az általa végzett tevékenységet figyeli meg, vagy aminek célja a munkavállaló vagy ügyfél viselkedésének befolyásolása.

4.1.4. Az intézmény nem végezhet megfigyelést olyan helyiségekben, ahol ez az emberi méltóságot sértheti, illetve olyan helyiségben sem, ahol a munkavállaló a munkaközi szünetét tölti.

4.1.5. Az érintettek az intézmény területére történő belépéssel elismerik és tudomásul veszik a kamerás megfigyelés tényét. A megfigyelő rendszer létéről és működéséről a kötelezettségének megfelelve az intézmény figyelemfelhívó jelzést helyez el arról, hogy az adott területen elektronikus megfigyelőrendszert alkalmaz. A figyelemfelhívó jelzés mellett a melléklet szerinti adatvédelmi tájékoztatót is ki kell helyezni.

4.1.6. Az, akinek jogát vagy jogos érdekét a képfelvétel rögzítése érinti, a képfelvétel rögzítésétől számított három munkanapon belül jogának vagy jogos érdekének igazolásával kérheti, hogy az adatot az Intézmény ne semmisítse meg, illetve ne törölje.

4.1.7. Az emberi életet, testi épséget, vagyont sértő körülményt a munkavállalók a munkáltatói jogkör gyakorlója felé, az ügyfelek bármelyik munkavállaló felé jelzik szóban vagy írásban. A szóbeli jelzés esetén azonnali jegyzőkönyv felvételére kerül sor. Az írásbeli jelzés vagy a jegyzőkönyv a felvételt követően azonnal eljuttatásra kerül az intézményvezetőhöz. Az intézményvezető az emberi életet, testi épséget, vagyont sértő körülmény időpontja alapján beazonosítja és intézkedik a tevékenység és a felvétel biztonságos adathordozóra történő lementése iránt és írásbeli visszajelzést küld a körülményt jelzőnek a mentés megtörténtéről.

4.1.8. Az intézményvezető a 4.1.7. pont szerinti feladatkörét delegálhatja telephelyvezető vagy más munkavállaló, vagy az intézménnyel adatfeldolgozói szerződést kötő harmadik személy részére.

4.1.9. Bíróság vagy más hatóság megkeresésére a rögzített képfelvételt, valamint más személyes adatot a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni.

4.1.10. Amennyiben a megkeresésre - attól számított harminc napon belül-, hogy a megsemmisítés mellőzését kérték, nem kerül sor, a rögzített képfelvételt, valamint más személyes adatot meg kell semmisíteni, illetve törölni kell.

4.1.11. A tájékoztatás és a rögzítés kérése ingyenes.

4.1.12. Az adatok tárolására a kameraszerveren kerül sor.

4.2. Iratok tárolása, helyiségek őrzése

4.2.1. A személyes adatokat tartalmazó iratokat csak kizárólag erre szolgáló helyiségben lehet tárolni. A helyiség ajtaját biztonsági ráccsal vagy biztonsági ajtóval, vagy kulccsal zárható ajtóval kell ellátni, az ügyfél tértől jól elkülönített adminisztratív zónát kell kialakítani az iratok eseti átadására, ügyintézése céljából.

4.2.2. Ügyfél nem tartózkodhat olyan helyiségben, ahol a nem rá vonatkozó személyes adatok vannak, csak abban az esetben, amennyiben a nem rá vonatkozó személyes adatok kulccsal elzárt szekrényben vannak elhelyezve és ahhoz az ügyfél kulcs nélkül nem fér hozzá, nem lát rá.

4.2.3. Az iratok tárolására szolgáló helyiségben csak az intézményvezető által kijelölt személyek tartózkodhatnak. Ezen személyekről az intézményvezető listát vezet a melléklet szerinti tartalommal, melyből az adott helyiségre vonatkozóan elkészített kivonatolt névjegyzékét a helyiség ajtajára ki kell függeszteni. Az adott helyiségben önállóan tartózkodó személyek kötelesek a rendelkezést betartatni. A rendelkezés megsértése adatvédelmi incidenst keletkeztet.

4.2.4. A személyi adatok kezelésére szolgáló helyiségben takarítást, karbantartást vagy egyéb munkálatokat végezni csak az ott dolgozó munkatárs jelenlétében lehet amennyiben az adatok zárható szekrényben történő tárolása nem biztosított.

4.2.5. A személyes adatokat tartalmazó iratok munkaidő alatt őrizetlenül nem maradhatnak. A kezeléssel megbízott munkatárs helyiségből való eltávozása esetén az iratok elzárásával vagy az iroda bezárásával köteles az illetéktelen hozzáférést megakadályozni.

4.2.6. Az iratok elzárását lehetővé tevő szekrények és irodák kulcsairól listát kell vezetni a melléklet szerinti tartalommal.

4.2.7. Az intézmény a kimenő postai küldemények esetében a kettős címkontrollt alkalmazza. A küldeményt összeállító dolgozó jól láthatóan megadja a postázási címet, a boríték címzését és a borítékba helyezést végző dolgozó köteles leellenőrizni a küldemény borítékba helyezését és a címzést.

4.3. Informatikai biztonsági előírások

4.3.1. A személyes adatot tartalmazó szervert el kell zárni, az eszközöket működtető szoftvereket védeni kell az illetéktelen telepítések ellen. A szervereket úgy kell elhelyezni, hogy azok egy esetleges tűz esetén se sérüljenek, a szervert tároló szobában elektronikus megfigyelési rendszert kell alkalmazni.

4.3.2. A szervert és az informatikai rendszerek ellenőrzését és karbantartását meg kell szervezni, szünetmentes áramforrást kell biztosítani, érintésvédelmi és villámvédelmi szabályzatot kell létrehozni.

4.3.3. Az adatok mentése történhet automatikusan vagy nem automatikusan. Törekedni kell az automatikus mentés megszervezésére. A nem automatikus biztonsági mentést hetente el kell végezni, melyről teljesítési igazolást kell felvenni. A teljesítési igazolásban rögzíteni kell a mentést végző személy nevét, aláírását, a mentés idejét és a mentés során tapasztalt körülményeket. A teljesítési igazolást a melléklet tartalmazza. A teljesítési igazolást át kell adni a mentés után haladéktalanul az intézményvezetőnek, aki azt őrizni köteles.

4.3.4. A személyes adatokhoz az adatkezelési tevékenységek nyilvántartása szerinti rögzített személyek férhetnek hozzá, a munkaköri leírásokban történő külön rögzítés mellett.

4.3.5. Az informatikai rendszereket jelszóval kell védeni. A jelszavakat tartalmazó adattáblát a melléklet szerinti tartalommal kell elkészíteni. A jelszavak megváltoztatására csak az intézményvezető jogosult. A jelszavakat az adott felhasználó harmadik személynek nem adhatja ki.

4.3.6. Hálózati tűzfalak, hálózati forgalom szűrése és korlátozása, hálózaton terjedő vírusok és kémprogramok ellen védelmet kell kialakítani.

4.3.7. Számítógépes programok letöltésére csak az intézményvezető, illetve az informatikai rendszereket ellenőrző személy jogosult.

4.3.8. Az intézményi eszközöket idegen adathordozókhoz (pl. pendrive) csatlakoztatni tilos.

4.4. Oktatás

4.4.1. Az adatvédelemmel, adatbiztonsággal kapcsolatos jogokról és kötelezettségekről oktatást, előadást kell a foglalkoztatottak részére szervezni szükség szerint, de évente legalább egy alkalommal.

4.4.2. Minden újonnan belépő munkavállaló részére az oktatást meg kell szervezni.

4.4.3. A foglalkoztatott az oktatás megtörténtét aláírásával igazolja. A foglalkoztatotti nyilatkozat a személyi nyilvántartás része.

4.4.4. A jelen szabályzat melléklete tartalmazza az oktatás megtörténtének igazolására alkalmazandó nyomtatványt.

4.4.5. Az oktatás anyagát az adatvédelmi tisztviselő állítja össze.

4.4.6. Az oktatás megszervezésében az intézményvezető segítséget nyújt az adatvédelmi tisztviselőnek.

4.4.7. Az oktatás megtartását követően a tudásszint felmérésére ellenőrző teszt alkalmazható.

A Szentesi Családsegítő Központ Adatvédelmi Szabályzata 2020. március 01-től hatályos.

Szentes, 2020. február 26.

…….

Gál Antal

igazgató

VIII. MELLÉKLETEK

1. számú melléklet – Adatkezelési tájékoztató

1. Bevezetés

A **Szentesi Családsegítő Központ** működése során, az ellátásokat igénybevevő személyek adatait kezeli abból a célból, hogy részükre megfelelő szolgáltatást nyújthasson.
A szolgáltató teljes mértékben meg kíván felelni a személyes adatok kezelésére vonatkozó jogszabályi előírásoknak, különösen az Európai Parlament és a Tanács (EU) 2016/679 rendeletében foglaltaknak.
Ez az adatkezelési tájékoztató a természetes személyek személyes adatai védelméről és az adatok szabad áramlásáról az Európai Parlament és a Tanács (EU) 2016/679 rendelete alapján készült, figyelemmel a 2011. évi CXII. törvény tartalmára, amely az információs önrendelkezési jogról és az információszabadságról szól.

2. Szolgáltató, adatkezelő megnevezés, elérhetősége

Név	**Szentesi Családsegítő Központ**
Székhely	6600 Szentes, Ady Endre u. 10.
Adószám	16684801-2-06
Telefon	+3663-561-510; +3663-561-520
Email	info@cssk-szentes.hu; igazgató: galantal@cssk-szentes.hu; CsGyK: laszlogyongyi@cssk-szentes.hu; CsGySz: levaine@cssk-szentes.hu
Telephely 1	Szentesi Családsegítő Központ **Gyermekek Átmeneti Otthona**
Cím	6600 Szentes, Munkácsy Mihály u. 3
Telefon, Email	+3663-444-500; gyao@cssk-szentes.hu
Telephely 2	Szentesi Családsegítő Központ **Családok Átmeneti Otthona**
Cím	6600 Szentes, Koszta József u. 7
Telefon, Email	+3663-444-600; csao@cssk-szentes.hu
Telephely 3	Szentesi Családsegítő Központ **Dózsa-ház Közösségi Tér**
Cím	6600 Szentes, Csongrádi út 2.
Telefon, Email	+3663-444-700; kozter@cssk-szentes.hu
Telephely 4	**Szentes Városi Üdülő - Szigliget**
Cím	Szigliget, Külsőhegyi út 66, 8264
Telefon, Email	+3687-461-451;

3. Fogalom-meghatározások

- a **GDPR** (General Data Protection Regulation) az Európai Unió új Adatvédelmi Rendelete;
- **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;

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

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

- **személyes adat**: azonosított vagy azonosítható természetes személyre (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;

- **Egészségügyi adat:** egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

- **Közérdekű adat:** az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

- **Közérdekből nyilvános adat:** a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

- **érintett**: bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy.

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

- **Adatfeldolgozás**: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik.

- **Adattovábbítás**: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

- **Hozzájárulás**: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez.

- **Harmadik személy:** olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel vagy az adatkezelővel.
- **Célhoz kötött adatkezelés:** meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető személyes adat kezelése. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. Az adatkezelés során biztosítani kell, hogy az adat pontos, teljes és – ha az adatkezelés céljára tekintettel szükséges – naprakész legyen, va lamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.
- **Tiltakozás**: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.
- **címzett**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;
- **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;

4. Az adatkezelés irányelvei

Az adatkezelő kijelenti, hogy az adatkezelési tájékoztatóban foglaltak szerint végzi a személyes adatok kezelését és betartja a vonatkozó jogszabályok előírásait, különös figyelemmel az alábbiakra:

A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.

A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet.

A személyes adatok kezelésének célja megfelelő és releváns legyen, és csak a szükséges mértékű lehet.

A személyes adatoknak pontosnak és naprakésznek kell lenniük. A pontatlan személyes adatokat haladéktalanul törölni kell.

A személyes adatok tárolásának olyan formában kell történnie, hogy az érintettek azonosítását csak szükséges ideig tegye lehetővé. A személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, ha a tárolás közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történik.

A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell.

5. Az érintettek jogai

Az érintett jogai röviden (az érintett személy az, akinek a személyes adatait az Adatkezelő kezeli):

- a Szentesi Családsegítő Központtól tájékoztatást kapjon a személyes adatainak kezeléséről, tájékoztatási jog,
- kérelmezheti a rá vonatkozó személyes adatokhoz való hozzáférést,
- kérelmezheti azok helyesbítését,
- kérelmezheti azok törlését: az adatok törlésének kérelmezése, illetve ez alapján az adatok törlése nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
- kérelmezheti a GDPR 18. cikkében foglalt feltételek fennállása esetén a személyes adatok kezelésének korlátozását (tehát azt, hogy az Adatkezelő az adatokat ne törölje, vagy ne semmisítse meg bíróság vagy hatóság megkereséséig, de legfeljebb harminc napig, s ezen túlmenően más céllal az adatot ne kezelje),
- tiltakozhat a személyes adatok kezelése ellen: személyes adatai kezelésének, illetve az adatok megőrzésének időtartamát az adatkörök tekintetében minden esetben az irányadó törvényi szabályok tartalmazzák,
- megilleti a felügyeleti hatósághoz címzett panasz benyújtásának joga a jelen tájékoztató „Jogorvoslati lehetőségek" címében foglaltak szerint.

6. Az adatkezelés jogalapja

Személyes adat akkor kezelhető:

1. az érintett hozzájárulásával, vagy
2. azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli:
   - -1997. évi XXXI. törvény a gyermekek védelméről és a gyámügyi igazgatásról,
   - 15/1998. (IV. 30.) NM rendelet a személyes gondoskodást nyújtó gyermekjóléti, gyermekvédelmi intézmények, valamint személyek szakmai feladatairól és működésük feltételeiről,
   - 235/1997. (XII. 17.) Korm. rendelet a gyámhatóságok, a területi gyermekvédelmi szakszolgálatok, a gyermekjóléti szolgálatok és a személyes gondoskodást nyújtó szervek és személyek által kezelt személyes adatokról.
3. az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése .

a) az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy

b) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll. Ha az érintett cselekvőképtelensége folytán vagy más elháríthatatlan okból nem képes hozzájárulását megadni, akkor a saját vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi

épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges mértékben a hozzájárulás akadályainak fennállása alatt az érintett személyes adatai kezelhetőek. A 16. életévét betöltött kiskorú érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása nem szükséges.

7. Adatkezelés

7.1. Az adatok felhasználása körében a döntéseket az adatkezelő vezetője (intézményvezető), illetve az ő felhatalmazása alapján a szakmai egység vezető vagy az ügyintéző hozza meg.

7.2. Az adatkezelés során az érintettek adatai kerülnek feldolgozásra.

7.3. Az adatkezelő által kezelt személyes adatok köre (adattípusok):

Azonosító adatok:

a) Természetes azonosítók (pl.: név, születés helye és ideje, anyja neve, lakcímadatok – általában többet kell alkalmazni egyszerre az azonosításhoz)
b) Mesterséges azonosítók (matematikai eljárással generált kódok, pl.: szig. szám, adóazonosító szám, TAJ szám, stb. – egy is elég az azonosításhoz)

Leíró adatok:

- Érintett különböző jellemzőit, tulajdonságait, viszonyait fejezik ki.

Különleges adatok:

a) a faji eredetre,
b) a nemzeti, és etnikai kisebbséghez tartozásra,
c) a politikai véleményre vagy pártállásra,
d) a vallásos vagy más világnézeti meggyőződésre,
e) az érdekképviseleti szervezeti tagságra,
f) a szexuális életre vonatkozó adat,
g) az egészségi állapotra,
h) a kóros szenvedélyre vonatkozó adat, és
i) a bűnügyi személyes adat

7.4. Az adatkezelés célja: közfeladat ellátása.

A Szentesi Családsegítő Központ jogszabályban meghatározott feladat- és hatáskörei keretében jár el: család- és gyermekjóléti szolgálatot illetve család- és gyermekjóléti központot, gyermekek átmeneti gondozását, tanyagondnoki szolgálatot, közösségi teret, valamint üdülőtábort működtet, a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. tv. és a szociális igazgatásról és szociális ellátásokról szóló 1993. évi III. tv. alapján.

7.5. A személyes adatok szolgáltatása jogszabályon alapul vagy szerződés kötésének az előfeltétele.

7.6. Az adatkezelő által kezelt személyes adatok címzettjei elsősorban a jogszabályban meghatározott személyek és hivatalos szervek.

8. Egyéb

A Szentesi Családsegítő Központ munkatársai az adatvédelemmel kapcsolatos feladatai körében:

a) amunkájuk során kötelesek gondoskodni arról, hogy jogosulatlan személyek ne tekinthessenek be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhet ő, megváltoztatható, megsemmisíthető;

b) a nap folyamán úgy hagyhatják el az olyan helyi séget, ahol adatkezelés vagy adatfeldolgozás folyik, hogy a rábízott adathordozókat elzárják, vagy az irodát bezárják .

9. A képmáshoz, és hangfelvételhez való jog

Képmás vagy hangfelvétel elkészítéséhez és felhasználásához az érintett személy hozzájárulása szükséges.

Nincs szükség az érintett hozzájárulására a felvétel elkészítéséhez és az elkészített felvétel felhasználásához tömegfelvétel és nyilvános közéleti szereplésről készült felvétel esetén. A Szentesi Családsegítő Központ rendezvényein kép- és hangfelvétel készülhet az eseményről, melyen szolgáltatást igénybevevő is szerepelhet. Ezen kép- és hangfelvételeket a Szentesi Családsegítő Központ további ellenszolgáltatás nélkül felhasználhatja, sokszorosíthatja, közzéteheti.

10. Különös szabályok

10.1. Az 1997. évi XXXI. törvény 134. § (1) bekezdése alapján a gyermekek védelmét biztosító feladat- és hatáskört gyakorló állami és nem állami szerv (a továbbiakban: adatkezelő szerv) az e törvényben szabályozott feladatai ellátásához a 135-136. § -ban felsorolt adatkörben, az ott meghatározott célok teljesüléséhez elengedhetetlenül szükséges személyes adatokat kezelheti.

10.2. A GDPR 8. cikk (1) bekezdése alapján a 16. életévét betöltött kiskorú érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása nem szükséges, a 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte.

10.3. **Zárt adatkezelés**: a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény 17§ (2a) szerint a gyermekjóléti szolgáltatást nyújtó szolgáltató és a gyámhatóság a gyermek bántalmazása, elhanyagolása miatt jelzést vagy kezdeményezést tevő intézmény, személy adatait erre irányuló külön kérelem hiányában is zártan kezeli. A jelzést, a bejelentést tartalmazó iratot a gyermek dokumentációjában külön kell kezelni, a zártan kezelt iratokat zárt borítékban kell továbbítani. A zárt iratanyagba a szülő nem tekinthet bele, a „Gyermekeink védelmében” adatlapokon a zártan kezelt iratokat nem kell feltüntetni.

10.4. **Az iratból kivonat készíthető,** de oly módon, hogy abból a jelzést tevő személyére következtetést ne lehessen levonni (NAIH-1938-2/2013./T).

10.5. **A gyermek veszélyeztetettségére vonatkozó bejelentés visszavonása, az iratok visszakérése:** az érintett gyermek veszélyeztetettségére vonatkozó bejelentés visszavonása esetén, az iratok nem adhatók vissza, a jelzést zártan kell kezelni, a

gyermek helyzetét a visszavonás ellenére vizsgálni kell. (Adatvédelmi biztos 587/K/2006 -3. számú ajánlása)

10.6. Iratba betekintés, kivonat, másolat kiadása: az 1997. évi XXXI. törvény 136/A.§ (1) bekezdése alapján a gyermek szülője vagy törvényes képviselője a szolgáltató (intézmény) vezetőjénél kérelmezheti, hogy betekinthessen a külön jogszabály szerinti gyermekvédelmi nyilvántartásnak a gyermek vonatkozásában kitöltött adatlapjaiba, valamint - a (2) bekezdésben foglalt kivétellel - a gyermekjóléti, gyermekvédelmi szolgáltatónál, intézménynél keletkezett, illetve részére megküldött, a gyermekkel kapcsolatos iratba. Az iratokról kivonat vagy másolat kérhető.

10.7. Az Ákr. -ben meghatározottakon túl az érintett írásbeli hozzájárulása hiányában nem lehet betekinteni a másik szülőre vonatkozó, különleges adatot tartalmazó iratba, kivéve, ha az a gyermek érdekében kezdeményezett, a gyermek védelembe vételére vagy nevelésbe vételére irányuló gyámhatósági eljárás, illetve a gyermek elhelyezésének megváltoztatására irányuló bírósági eljárás megindításához elengedhetetlenül szükséges.

10.8. A gyámhatóság és a személyes gondoskodást nyújtó gyermekjóléti, gyermekvédelmi szolgáltató tevékenységet végző szervezet alkalmazottja és vezetője, a gyermek és az őt nevelő szülő vagy a gyermek törvényes képviselője tartózkodási helyére vonatkozóan megtagadhatja a szülő tájékoztatását, illetve korlátozhatja a szülő iratbetekintési jogát, ha

10.9. a szülő a gyermeke vagy a gyermeket nevelő másik szülő sérelmére elkövetett bűncselekmény miatt büntetőeljárás hatálya alatt áll,

10.10. a szülő ellen gyermeke vagy a gyermeket nevelő másik szülő sérelmére elkövetett külön törvényben meghatározott hozzátartozók közötti erőszak miatt alkalmazható ideiglenes megelőző távoltartó határozat vagy megelőző távoltartó határozat iránti eljárás van folyamatban, a távoltartás időtartamáig.

11. Az adatkezelés alapjául szolgáló jogszabályok

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.
- A köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény.
- A közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet.
- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.
- 2003. évi C. törvény az elektronikus hírközlésről.

12. Jogorvoslati lehetőségek

A személyes adatai kezelésével kapcsolatos panaszával kérjük, keresse az intézményt.

Az Intézmény a panaszát kivizsgálja, és tájékoztatja a vizsgálat eredményéről és az általa megtett intézkedésekről.

Amennyiben az Ön megítélése szerint személyes adatainak kezelése sérti a vonatkozó jogszabályokat, jogosult az adatvédelmi felügyeleti hatóságnál panaszt tenni vagy bírósághoz fordulni. Az adatvédelmi perek elbírálása a törvényszék hatáskörébe tartozik. A per – az érintett választása szerint – az érintett lakóhelye vagy tartózkodási helye szerinti törvényszék előtt is.

A felügyeleti hatósági feladatokat Magyarországon a Nemzeti Adatvédelmi és Információbiztonság Hatóság (NAIH) látja el. A NAIH felé bejelentéssel élhet minden állampolgár személyes adatai kezelésével kapcsolatosan.

Amennyiben az Ön megítélése szerint a jogszerű állapot nem állítható helyre, értesítse erről a hatóságot az alábbi elérhetőségeken:

Nemzeti Adatvédelmi és Információszabadság Hatóság
Postacím: 1530 Budapest, Pf.: 5.
Cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
Telefon: +36 (1) 391-1400
Fax: +36 (1) 391-1410
E-mail: ugyfelszolgalat@naih.hu
URL https://naih.hu
koordináták: É 47°30'56''; K 18°59'57''

2. számú melléklet – Nyilatkozat adatkezelési tájékoztatás megtörténtéről és adatkezelési tájékoztató megismeréséről

Alulírott az alábbiakban nyilatkozom, hogy a Szentesi Családsegítő Központ munkatársa tájékoztatott a(z) …….. tevékenységhez kapcsolódó adatkezelésről, az adatkezelési tájékoztatót, az adatkezelési tevékenységek nyilvántartását megismertem, így tisztában vagyok azzal, hogy ki, milyen jogalapból, milyen célból, milyen időtartamig kezeli az adataimat.

Tudomásul veszem, hogy a szolgáltatás önkéntes igénybevétele esetén a közölt személyes és egyéb adataimat az adatkezelő **Szentesi Családsegítő Központ** munkatársa megismeri, a vonatkozó nyilvántartásba rögzíti, a szolgáltatás igénybevételéhez kapcsolódó célból kezeli és jogszabályban meghatározott ideig tárolja. Tudomásul veszem, hogy adataimat (kiskorú adatait) az adatkezelő kizárólag a szolgáltatás igénybevételének elősegítése céljából más adatkezelő(k) felé továbbítja, az adattovábbítás címzettjeiről és a várható adatkezelési időről a munkatárs számomra előzetes tájékoztatást adott.

Kötelező igénybevétel esetén tudomásul veszem, hogy adataimat az adatkezelő jogszabály erejénél fogva, kötelezően kezeli és továbbítja.

Tudomásul veszem, hogy adataim kezelésével kapcsolatban – ha azt jogszabály nem korlátozza, vagy ki nem zárja – a következő jogok illetnek meg: tájékoztatás kéréshez való jog, iratbetekintés joga, helyesbítéshez való jog, törléshez való jog, zároláshoz (adatkezelés korlátozásához) való jog, tiltakozáshoz való jog, adathordozhatósághoz való jog, hozzájárulás visszavonásának joga, jogorvoslathoz való jog.

Tudomásul veszem, hogy az adatkezelési tevékenységek nyilvántartása, az adatkezelési tájékoztató, az adatvédelmi tisztviselő elérhetőségei jól látható helyen kifüggesztésre kerültek és ügyfélfogadási időben hozzáférhető, ügyfélfogadási időn kívül az intézmény honlapján elérhető.

Az ellátást igénybevevő (vagy törvényes képviselője) panaszával elsődlegesen **az intézmény vezető**jéhez fordulhat. Amennyiben az intézmény vezetője a panasz írásos benyújtásától számított 15 napon belül nem vizsgálja ki a panaszt, vagy a panasztevő nem ért egyet az intézkedéssel úgy az igénylő a **fenntartó**hoz fordulhat.

Amennyiben az ellátást igénybevevő megítélése szerint személyes adatainak kezelése sérti a vonatkozó jogszabályokat, jogosult az adatvédelmi felügyeleti hatóságnál panaszt tenni vagy bírósághoz fordulni.

Magyarországon az adatvédelmi felügyeleti hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság (1125 Budapest, Szilágyi Erzsébet fasor 22/C) ugyfelszolgalat@naih.hu.

Az adatvédelmi perek elbírálása a törvényszék hatáskörébe tartozik. A per – az érintett választása szerint – az érintett lakóhelye vagy tartózkodási helye szerinti törvényszék előtt is megindítható.

Tudomásul veszem, hogy köteles vagyok

- a jogszabályok alapján vezetett intézményi nyilvántartásokhoz adatokat szolgáltatni - társadalombiztosítási igazolványt, lakcímet igazoló hatósági igazolványt, személyazonosító igazolványt – kérésre bemutatni.
- bejelenteni a jogosultsági feltételekben, valamint a személyazonosító adatokban beállott változást

Dátum: Szentes, ……év……hó……..napon

…… ……

Igénybevevő/Szülő/Törvényes képviselő Gyermek/fiatal

Az adatkezelési tájékoztató szerinti és a hozzájárulásomon alapuló adattovábbításhoz hozzájárulok.

Dátum: Szentes, ……év……hó……..napon

…… ……

Igénybevevő/Szülő/Törvényes képviselő Gyermek/fiatal

3. számú melléklet – Foglalkoztatott adatkezelési hozzájárulása

Alulírott

Név: ……..

Születési név: ……..

Születési hely: ……..

Születési idő: ……..

Anyja neve: ……..

Lakcím: ……..

jelen nyilatkozat aláírásával hozzájárulok ahhoz, hogy a …….. kapcsolatos személyes adatomat a Szentesi Családsegítő Központ kezelje az adatkezelési tájékoztatóban megjelölt célból, határidőig, az adatkezelési tájékoztatóban megjelölt adattovábbítás lehetőségével és megismerhetőséggel.

Kijelentem, hogy az intézmény adatkezelési tájékoztatóját megismertem, a jelen hozzájárulásomat az adatkezelési tájékoztató elolvasása és értelmezése után, önkéntesen adtam meg, külön kijelentem, tudomással bírok arról, hogy hozzájárulásomat bármikor – jogkövetkezmények alkalmazása nélkül - visszavonhatom.

Keltezés helye, ideje:

……
[Név, aláírás]

4. számú melléklet – Adatkezelési hozzájárulás

Név: ……..

Születési név: ……..

Születési hely: ……..

Születési idő: ……..

Anyja neve: ……..

Lakcím: ……..

jelen nyilatkozat aláírásával hozzájárulok ahhoz, hogy a személyes adataimat az intézmény kezelje a …… üggyel kapcsolatosan az adatkezelési tájékoztatóban és az adatkezelési tevékenységek nyilvántartásában megjelölt célból, határidőig, a megjelölt adattovábbítás lehetőségével és megismerhetőséggel.

Kijelentem, hogy az intézmény adatkezelési tájékoztatóját és az adatkezelési tevékenységek nyilvántartásának elérhetőségét megismertem, a jelen hozzájárulásomat az adatkezelési tájékoztató elolvasása és értelmezése után, önkéntesen adtam meg, külön kijelentem, tudomással bírok arról, hogy hozzájárulásomat bármikor – jogkövetkezmények alkalmazása nélkül - visszavonhatom.

Keltezés helye, ideje:

……

[Név, aláírás]

5. számú melléklet- Hozzájárulás az ellátottakról készített fénykép és videofelvétel készítéséhez kapcsolódó adatkezelési tevékenységhez

Alulírott

Név: …….

Születési név: …….

Születési hely: …….

Születési idő: …….

Anyja neve: …….

Lakcím: …….

☐ hozzájárulok ahhoz, hogy a Szentesi Családsegítő Központ részéről az intézményben tartózkodásom ideje alatt rólam fénykép - vagy videofelvétel készüljön és ezen felvételek az intézmény honlapján, az intézmény épületében közzétételre kerüljenek az intézményi élet, szervezett program bemutatása okán.

☐ nem járulok hozzá ahhoz, hogy a Szentesi Családsegítő Központ részéről az intézményben tartózkodásom ideje alatt rólam fénykép - vagy videofelvétel készüljön és ezen felvételek az intézmény honlapján, az intézmény épületében közzétételre kerüljenek az intézményi élet, szervezett program bemutatása okán.

☐ hozzájárulok ahhoz, hogy a Szentesi Családsegítő Központ részéről az intézményben tartózkodásom ideje alatt rólam fénykép - vagy videofelvétel készüljön és ezen felvételek az oktatás kiegészítéseként szakmai dokumentációban, szakvizsgán, továbbképzésen vagy szakmai publikáció során felhasználásra kerüljenek.

☐ nem járulok hozzá ahhoz, hogy a Szentesi Családsegítő Központ részéről az intézményben tartózkodásom ideje alatt rólam fénykép - vagy videofelvétel készüljön és ezen felvételek az oktatás kiegészítéseként szakmai dokumentációban, szakvizsgán, továbbképzésen vagy szakmai publikáció során felhasználásra kerüljenek.

☐ hozzájárulok ahhoz, hogy a Szentesi Családsegítő Központ részéről az intézményben tartózkodásom ideje alatt rólam a sajtó és média munkatársai fénykép - vagy videofelvételeket készítsenek és ezen felvételeket a bölcsődei élet bemutatása okán megjelentessék.

☐ nem járulok hozzá ahhoz, hogy a Szentesi Családsegítő Központ részéről az intézményben tartózkodásom ideje alatt rólam a sajtó és média munkatársai fénykép - vagy videofelvételeket készítsenek és ezen felvételeket a bölcsődei élet bemutatása okán megjelentessék.

Kijelentem, hogy a fenti hozzájárulásom megadása előtt *„Az ellátottakról készített fénykép és videofelvétel készítéséhez kapcsolódó adatkezelési tevékenységekkel összefüggő adatkezelési tájékoztató”*-t megismertem, így tudomásom van az adatkezelő és az adatvédelmi tisztviselő személyéről, elérhetőségeiről, az adatkezelés jogalapjáról és céljáról, az adatkezelés időtartamáról, az adatkezeléshez kapcsolódó jogaimról, így a hozzájárulás visszavonásának jogáról is, továbbá a jogorvoslati lehetőségekről.

Tudomásom van arról, hogy a Szentesi Családsegítő Központ az adatkezelési tevékenységeiről nyilvántartást vezet, mely adatkezelési tevékenységek nyilvántartása az ellátottakról készített fénykép és videofelvétel készítéséhez kapcsolódó adatkezelési tevékenységekkel összefüggő adatkezelési tájékoztatóval együtt elérhető elektronikusan az Intézmény honlapján, illetve papír alapon az egyes részlegeknél.

Keltezés helye, ideje:

……

(aláírás)

6. számú melléklet – Adatkezeléshez hozzájárulás visszavonása formanyomtatvány

Név: ……..

Születési név: ……..

Születési hely: ……..

Születési idő: ……..

Anyja neve: ……..

Lakcím: ……..

jelen nyilatkozat aláírásával visszavonom a …… napon ……..ügyben személyes adataim tekintetében megadott adatkezelési hozzájárulásomat.

Keltezés helye, ideje:

……

[Név, aláírás]

7. számú melléklet- adatvédelmi incidensek nyilvántartása

I. Az adatkezelő adatai és elérhetőségei

Név:	**Szentesi Családsegítő Központ**
Cím:	6600 Szentes, Ady Endre u. 10
Telefon:	06-63/561-521
Email:	info@cssk-szentes.hu
Weboldal:	
Adatvédelmi tisztviselő neve:	
Adatvédelmi tisztviselő elérhetősége:	
Adatvédelmi tisztviselő ügyfélfogadása:	Előzetes egyeztetés alapján

II. Az adatvédelmi incidensek adattartalma

1. Bekövetkezés időpontja
2. Érintett személyes adatok köre
3. Az érintettek köre és száma
4. A bekövetkezés körülményei
5. Az adatvédelmi incidens hatásai
6. Az adatvédelmi incidens elhárítására megtett/tervezett intézkedések, hátrányos következmények enyhítését célzó intézkedések
7. Egyéb adatok
8. Kockázatelemzés időpontja eredménye
9. NAIH bejelentés időpontja és ahhoz kapcsolódó körülmények
10. NAIH vizsgálat ügyszáma, ügyintéző neve

III. Adatvédelmi incidens bejelentő formanyomtatvány

A Hatóság kérdései	**A kitöltő válaszai**
0. Adatvédelmi incidens jelentése	
Bejelentés típusa	☐ teljes bejelentés ☐ szakaszos bejelentés ☐ bejelentés módosítása
A korábban bejelentett incidens azonosítója	
A korábbi bejelentés időpontja	

1. A bejelentő adatai

1.1 Kapcsolati

A bejelentő adatkezelő cégjegyzékszáma		
A bejelentő adatkezelő adószáma (magánszemély bejelentése esetén nem kell)		
Szervezet száma		
A bejelentő adatkezelő elnevezése		
Az incidenssel érintett igazgatási/szervezeti egység megnevezése és elérhetőségei		
A bejelentő adatkezelő címe és egyéb elérhetőségei		
A bejelentő természetes személy neve és beosztása		
A bejelentő természetes személy elérhetőségei		
Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és beosztása		
Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó email elérhetősége		
Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó telefonszáma		
Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó levelezési címe		
Az adatkezelő az alábbiak közül melyik szektorba tartozik		Adminisztratív és szolgáltatást támogató tevékenység
		Bányászat, kőfejtés
		Büntetés-végrehajtás
		Bűnüldözés
		Egészségügy, szociális ellátás
		Egyéb közhatalmi tevékenység
		Építőipar
		Helyi önkormányzati igazgatás
		Honvédelem

		Információ, kommunikáció, hírközlés
		Ingatlanügyletek
		Kereskedelem
		Könnyűipar, feldolgozóipar
		Közlekedés, közlekedésbiztonság
		Központi közigazgatás
		Közrend és közbiztonság védelem
		Média
		Mezőgazdaság, erdőgazdálkodás, halászat
		Munkaügy
		Művészet, szórakoztatás
		Nehézipar, gépgyártás
		Nemzetbiztonság
		Oktatás, kutatás
		Pénzügyi, biztosítási tevékenység
		Rendvédelem
		Szakmai, tudományos, műszaki tevékenység
		Szálláshely-szolgáltatás, vendéglátás
		Szállítás, raktározás
		Személy- és vagyonvédelem
		Társadalmi szervezetek által végzett tevékenység
		Társadalombiztosítás
		Villamosenergia-, gáz-, gőzellátás, légkondicionálás
		Vízellátás, szennyvíz gyűjtése, kezelése, hulladékgazdálkodás, szennyeződésmentesítés
		Egyéb

1.2 Az adatkezelőn kívüli felek részvétele az adatvédelmi incidenssel érintett szolgáltatásban	
Az adatkezelőn kívül részt vesz-e más személy/szervezet az adatvédelmi incidenssel érintett adatkezelés folyamatában?	Igen/Nem
Az adatkezelőn kívüli fél megnevezése és minősége	

2. Időpontok	
Adatvédelmi incidens időpontja	
Adatvédelmi incidens kezdő időpontja	
Adatvédelmi incidens záró időpontja	

Az adatvédelmi incidens továbbra is fennáll	Igen/Nem
Az incidensről való tudomásszerzés időpontja	
Az incidens észlelésének módja	
Az adatfeldolgozó általi értesítés időpontja	
A késedelmes tájékoztatás indokai	
Egyéb megjegyzések az incidens időpontját érintően	

3. Az adatvédelmi incidensről

Bizalmas jelleg	Sérült/Nem sérült	
Integritás	Sérült/Nem sérült	
Rendelkezésre állás	Sérült/Nem sérült	
Adatvédelmi incidens jellege (több válasz is elfogadható)		adathalászat
		elektronikus hulladék (a személyes adatok rajta maradnak az elavult eszközön)
		eszköz elvesztése vagy ellopása
		informatikai rendszer feltörése (hackelés)
		levél elvesztése vagy jogosulatlan felnyitása
		papír alapú dokumentum elvesztése, ellopása, vagy olyan helyen hagyása, amely nem minősül biztonságosnak
		papír alapú dokumentum nem megfelelő módon történő megsemmisítése
		rosszindulatú számítógépes programok pl. Zsarolóprogram
		személyes adatok jogosulatlan megismerése
		személyes adatok jogosulatlan szóbeli közlése
		személyes adatok nagy nyilvánosság előtti jogellenes közzététele
		személyes adatok téves címzett részére történő elküldése
		egyéb
Egyéb megjegyzés az adatvédelmi incidens részletes leírásához		

Adatvédelmi incidens okai (több válasz is elfogadható)		külső, rosszhiszemű cselekmény
		külső, rosszhiszeműnek nem minősülő cselekmény
		szervezeten belüli, rosszhiszemű cselekmény
		szervezeten belüli, rosszhiszeműnek nem minősülő cselekmény
		egyéb
Adatvédelmi incidens egyéb okainak leírása		

4. Az adatvédelmi incidenssel érintett személyes adatok	
4.1 Személyes adatok	
Személyazonossághoz kapcsolódó adatok	Érintett/Nem érintett
Személyi szám	Érintett/Nem érintett
Elérhetőségi adatok	Érintett/Nem érintett
Azonosító adatok	Érintett/Nem érintett
Gazdasági, pénzügyi adatok	Érintett/Nem érintett
Képfelvétel	Érintett/Nem érintett
Hangfelvétel	Érintett/Nem érintett
Hivatalos okmányok	Érintett/Nem érintett
Helymeghatározó adatok	Érintett/Nem érintett
Biometrikus adatok	Érintett/Nem érintett
Büntetett előélettel, bűncselekményekkel vagy büntetéssel, intézkedéssel kapcsolatos adatok	Érintett/Nem érintett

4.2 Különleges adatok	
Faji eredetre, nemzetiséghez tartozásra vonatkozó adatok	Érintett/Nem érintett
Politikai véleményre vonatkozó adatok	Érintett/Nem érintett
Vallásos vagy más világnézeti meggyőződésre vonatkozó adatok	Érintett/Nem érintett
Érdek-képviseleti szervezeti tagságra vonatkozó adatok	Érintett/Nem érintett

Szexuális életre vonatkozó adatok	Érintett/Nem érintett
Egészségügyi adatok	Érintett/Nem érintett
Genetikai adatok	Érintett/Nem érintett
Még nem ismert	Érintett/Nem érintett
Egyéb	Érintett/Nem érintett
Az egyéb személyes adatok leírása	
Az adatvédelmi incidenssel érintett személyes adatok becsült száma	

5. Az érintettek	
Alkalmazottak	Érintett/Nem érintett
Felhasználók	Érintett/Nem érintett
Feliratkozók	Érintett/Nem érintett
Diákok	Érintett/Nem érintett
Katonai állomány tagjai	Érintett/Nem érintett
Ügyfelek (jelenlegi és potenciális)	Érintett/Nem érintett
Páciensek	Érintett/Nem érintett
Kiskorúak	Érintett/Nem érintett
Kiszolgáltatott személyek	Érintett/Nem érintett
Hatósági eljárás vagy intézkedés alá vont, vagy azok által érintett személyek	Érintett/Nem érintett
Még nem ismert	Érintett/Nem érintett
Egyéb	Érintett/Nem érintett
Az egyéb leírása	
Az incidenssel érintett adatalanyok részletes leírása	
Az adatvédelmi incidenssel érintettek becsült száma	

6. Az incidens ELŐTT alkalmazott intézkedések	
Az adatvédelmi incidens előtt alkalmazott intézkedések leírása	

7. Következmények	
7.1 Bizalmas jelleg sérülése	
Szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult	Igen/Nem
Az adat összekapcsolhatóvá vált az érintett egyéb adatával	Igen/Nem
Az adatot más célokból történő, tisztességtelen módon történő kezelése lehetséges	Igen/Nem
Egyéb	Igen/Nem
Az egyéb bizalmas jelleget érintő következmény leírása	

7.2 Intergritás sérülése	
Az adat módosíthatóvá vált annak ellenére, hogy archivált elavult adat volt	Igen/Nem
Az adatot valószínűsíthetően módosították egyébként pontos adatokra, és azokat eltérő célokra használhatták	Igen/Nem
Egyéb	Igen/Nem
Az egyéb integritást érintő következmény leírása	

7.3 Rendelkezésre állás sérülése	
Az érintettek számára történő kritikus szolgáltatásnyújtás képességének elvesztése	Igen/Nem
Az érintettek számára történő kritikus szolgáltatásnyújtás képességének módosulása	Igen/Nem
Egyéb	Igen/Nem
Az egyéb rendelkezésre állást érintő következmény leírása	

7.4 Az érintetteket ért fizikai, anyagi vagy nem vagyoni károk, vagy egyéb jelentős következmények		
Az incidens valószínűsíthető hatásai az érintettekre (több válasz is elfogadható)		álnevesítés engedély nélküli feloldása
		érintett jogainak korlátozása
		hátrányos megkülönböztetés
		jó hírnév sérelme
		pénzügyi veszteség
		szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése
		személyazonosság-lopás
		személyazonossággal való visszaélés
		személyes adatok feletti rendelkezés elvesztése
		egyéb
Az egyéb valószínűsíthető hatások leírása		
A valószínűsíthető következmények súlyossága		elhanyagolható
		korlátozott
		jelentős
		maximális

8. Megtett intézkedések		
8.1 Érintettek tájékoztatása		
Érintettek tájékoztatása		a, Az érintetteket tájékoztatta
		b, Az érintettek tájékoztatását tervezi
		c, Az érintettek tájékoztatását NEM tervezi
		d, Nem tudja

Tájékoztatás időpontja („a” válasz esetén)		
Tájékoztatás tervezett időpontja („b” válasz esetén)		
A tájékoztatás tervezett időpontja még nincs eldöntve („b” válasz esetén		El van döntve/Nincs eldöntve
Tájékoztatás hiányának indokai („c” válasz esetén)		I, Az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen olyan intézkedéseket, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat
		II, 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
		III, Az érintettek egyenkénti tájékoztatása aránytalan erőfeszítést tenne szükségessé az adatkezelő számára
Intézkedések leírása, amelyek alapján az érintettek tájékoztatására nem került sor („c” válasz esetén)		
Tájékoztatott érintettek száma („a” válasz esetén)		
Az érintett tájékoztatásának formája („a” válasz esetén)		
Az érintetteknek szóló tájékoztatás tartalma („a” válasz esetén)		
Nyilvánosan közzétett információk, vagy hasonló intézkedés („c” illetve „III” válasz esetén)		

8.2 Az adatvédelmi incidens orvoslására tett intézkedések	
Az adatkezelő által az adatvédelmi incidens orvoslására tett intézkedések	

8.3 Egyéb bejelentések	
A vezető hatóságnak bejelentett határokon átnyúló adatvédelmi incidens	Igen/Nem

Az EU felügyeleti hatóságok listája, amelyeket az adatvédelmi incidens érinthet (több válasz is elfogadható)		Ausztria
		Belgium
		Bulgária
		Ciprus
		Csehország
		Dánia
		Egyesült Királyság
		Észtország
		Finnország
		Franciaország
		Görögország
		Hollandia
		Horvátország
		Írország
		Izland
		Lengyelország
		Lettország
		Liechtenstein
		Litvánia
		Luxemburg
		Magyarország
		Málta
		Németország
		Norvégia
		Olaszország
		Portugália
		Románia
		Spanyolország
		Svájc
		Svédország
		Szlovákia
		Szlovénia
Az adatkezelő bejelentette-e, vagy be fogja-e jelenteni az adatvédelmi incidenst közvetlenül más tagállam felügyeleti hatóságának?		
Az EU felügyeleti hatóságok listája, amelyeknek az adatkezelő közvetlenül bejelentette-e, vagy be fogja-e jelenteni az adatvédelmi incidenst (több válasz is elfogadható)		Ausztria
		Belgium
		Bulgária
		Ciprus
		Csehország
		Dánia
		Egyesült Királyság
		Észtország
		Finnország

		Franciaország
		Görögország
		Hollandia
		Horvátország
		Írország
		Izland
		Lengyelország
		Lettország
		Liechtenstein
		Litvánia
		Luxemburg
		Magyarország
		Málta
		Németország
		Norvégia
		Olaszország
		Portugália
		Románia
		Spanyolország
		Svájc
		Svédország
		Szlovákia
		Szlovénia
Bejelentette-, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst másik EGT-tagállam olyan adatkezelőjének, amely részére az incidenssel érintett adatokat korábban továbbította, vagy amely adatkezelő az incidenssel érintett adatokat részére átadta?		Igen/Nem
Azon más EGT-tagállami adatkezelő megnevezése és elérhetőségei, amelynek az incidenst bejelentette vagy be fogja jelenteni.		
Bejelentette-e, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst EU-n kívüli adatvédelmi hatóságnak?		Igen/Nem
Az EU-n kívüli felügyeleti hatóságok listája, amelyeknek az adatvédelmi incidenst bejelentette, vagy be fogja jelenteni az adatkezelő		
Bejelentette-, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst egyéb EU-s hatóságnak egyéb jogszabály alapján fennálló kötelezettség alapján? (NIS Irányelv, eIDAS Rendelet)?		Igen/Nem
Egyéb EU hatóságok listája, amelyeknek az adatvédelmi incidenst bejelentette vagy be fogja jelenteni az adatkezelő.		

8. számú melléklet - Az érintett hozzáférési jogával kapcsolatos intézkedések nyilvántartása

I. Az adatkezelő adatai és elérhetőségei

Név: **Szentesi Családsegítő Központ**
Cím: 6600 Szentes, Ady Endre u. 10
Telefon: 06-63/561-521
Email: info@cssk-szentes.hu
Weboldal:
Adatvédelmi tisztviselő neve:
Adatvédelmi tisztviselő elérhetősége:
Adatvédelmi tisztviselő ügyfélfogadása: Előzetes egyeztetés alapján

II. A hozzáférési jog gyakorlásához kapcsolódó adatok

A hozzáférési jogát gyakorló érintett neve	A hozzáférési jogát gyakorló érintett elérhetőségei	Adatok, melyre vonatkozóan az érintett a hozzáférési jogát gyakorolja	Az érintett hozzáférési jogát korlátozó vagy megtagadó intézkedésének jogi indokai	Az érintett hozzáférési jogát korlátozó vagy megtagadó intézkedésének ténybeli indokai

9. számú melléklet – Adatbiztonsági ellenőrzésről készített jegyzőkönyv

Felvétel ideje:
Felvétel helye:
Jelen vannak:

Az adatvédelmi tisztviselő köszönti a megjelenteket és megnyitja az egyeztetést.

Védendő területek:

Helyiségek, objektumok védelme							
Kockázati tényezők	**Előfordulási lehetőségek[1]**				**Eddigi védelem leírása**	**A kockázat csökkentésére tett javaslat**	**Határidő**
	Nem fordulhat elő	**Kismértékű előfordulási lehetőség**	**Reális előfordulási lehetőség**	**Minden bizonnyal előfordul**			
természeti katasztrófa							
külső személy által elkövetett erőszakos cselekmény							
közműellátási zavarok							
külső személy tartózkodása az épületben							
védelmi berendezések technikai hibája, vészhelyzet (pl. rövidzárlat, tűz, csőtörés)							

A papír alapú és más hagyományos dokumentumok védelme							
Kockázati tényezők	**Előfordulási lehetőségek[2]**				**Eddigi védelem leírása**	**A kockázat csökkentésére tett javaslat**	**Határidő**
	Nem fordulhat elő	**Kismértékű előfordulási lehetőség**	**Reális előfordulási lehetőség**	**Minden bizonnyal előfordul**			
hibás adatkezelés ismerethiány vagy fáradtság, figyelmetlenség miatt							
jogosulatlan hozzáférés							
az adatkezelésre vonatkozó előírások figyelmen kívül hagyása hiányos„biztonságtudat” miatt, a fenyegetettség lebecsülése							
károsodás nem szabályszerű tárolás vagy kezelés miatt							
kontroll nélküli hozzáférés az adathordozókhoz, másolás							
elhelyezésére szolgáló helyiség vagy munkahely helytelen kiválasztása.							

[1] X-et kell tenni abba a négyzetbe, melynek legnagyobb a valószínűsége
[2] X-et kell tenni abba a négyzetbe, melynek legnagyobb a valószínűsége

eltulajdonítás elleni védelmet, vagyonvédelem							
fizikai sérülések							
az aktualitás hiánya							
jogosulatlan, hibás, ismeretlen eredetű változtatás							
kontroll nélküli hozzáférés, sokszorosítás							

Hardver és szoftvervédelem							
Kockázati tényezők	**Előfordulási lehetőségek[3]**				**Eddigi védelem leírása**	**A kockázat csökkentésére tett javaslat**	**Határidő**
	Nem fordulhat elő	**Kismértékű előfordulási lehetőség**	**Reális előfordulási lehetőség**	**Minden bizonnyal előfordul**			
műszaki jellegű hibák, rendellenességek							
káros környezeti hatás (feszültségingadozás, szennyeződés, elektromágneses sugárzás, elektrosztatikus feltöltődés);							
a berendezések kezelésével, karbantartásával kapcsolatos hibák							
illetéktelen hozzáférés							
a berendezések manipulálása, rongálása, lopás							
az eszköz elhelyezésére szolgáló helyiség vagy munkahely helytelen kiválasztása							
károsodás nem szabályszerű tárolás vagy kezelés miatt							
ismeretlen vagy kétes eredetű adathordozó alkalmazása							
kontroll nélküli hozzáférés az adathordozókhoz, másolás							
saját adathordozó ellenőrzés nélküli alkalmazása szolgálati vagy magáncélra							
az aktualitás hiánya							
jogosulatlan, hibás, ismeretlen eredetű változtatás							
kontroll nélküli hozzáférés, sokszorosítás							
nem jogtiszta, ismeretlen szoftver alkalmazása							
szoftverhiba							
jogosulatlan hozzáférés, másolás lehetősége							
szoftver ellenőrizetlen bevitele az informatikai rendszerbe							
vírusveszély							
szándékos vagy gondatlan kezelési, karbantartási hiba							
a szoftver sérülése, károsodása hardverhiba miatt							
adatvesztés, károsodás hardver- vagy szoftverhiba miatt							

[3] X-et kell tenni abba a négyzetbe, melynek legnagyobb a valószínűsége

teljes vagy részleges adatvesztés hibás adathordozó miatt							
a jogosult adatkezelő által szándékosan vagy tévedésből végzett adattörlés, módosítás							
jogosulatlan adatkezelő által végzett másolás, törlés, módosítás							
hibás adatkezelés ismerethiány miatt							
kezelési előírások, oktatás hiánya							
jogosulatlanok bejutása a hálózatba nem ellenőrizhető csatlakozás révén							
hálózati hardverek és szoftverek szándékos vagy gondatlan manipulálása							
adatforgalom lehallgatása							
váratlan forgalmazási akadályok, az átvitelt zavaró befolyások							
az adatátviteli eszközök sérülése, károsodása							

Megjegyzések:
……
……
……
……
……
……

Aláírások:

…….. …….
intézményvezető adatvédelmi tisztviselő

…….
informatikus

10. számú melléklet – Elhelyezett kamerák és megfigyelt területek leírása

Sorszám	Kamera helye	Megfigyelt terület	Adattárolás helye

12. számú melléklet – Kulcs-nyilvántartás

Sorszám	Kulccsal zárható helyiség, vagy szekrény megjelölése	Kulcsok darabszáma	Kulccsal rendelkezők neve

13. számú melléklet – Nem automatikus adatmentésről felvett teljesítési igazolás

A mentést végezte:…….
A mentés elvégzésének időpontja:…….
A mentést végző aláírása:……
A mentés során tapasztaltak leírása:
……
……
……

Egy példányt a mai napon átvettem:

(Keltezés helye, ideje)

……..
intézményvezető

14. számú melléklet – Az informatikai rendszerek jelszavait tartalmazó adattábla minta

Informatikai berendezés megjelölése	Informatikai berendezés helye	Informatikai berendezése dolgozó munkavállaló megjelölése	Informatikai berendezés jelszava	Informatikai berendezés jelszóadásának ideje

15. számú melléklet – Adatvédelmi, adatbiztonsági oktatási napló

Szervezeti egység megnevezése: .....……..
Munkahely megnevezése: .....
Oktatás időpontja: …..... év .....hó .....nap
Oktatás jellege: - ismétlődő - pótoktatás - rendkívüli **-***
Oktatott dolgozók létszáma: ..... fő
Az oktatás javasolt tematikája:

1. Az Európai Unió Általános Adatvédelmi Rendeletének ismertetése
2. Az adatvédelem szükségessége, veszélyforrások áttekintése
3. A Szentesi Családsegítő Központ által végzett adatkezelési tevékenységek ismertetése (jogalap, cél, időtartam)
4. Az érintettek jogai
5. A munkavállalók kötelezettsége az adatkezeléssel, adatvédelemmel, adatbiztonsággal összefüggésben
6. Az elmúlt időszak tanulságos eseteinek az ismertetése
7. Az elkövetkező időszak feladataihoz kapcsolódó adatvédelmi és biztonsági kérdések, betartandó magatartási szabályok, intézkedések ismertetése.

Egyéb oktatott téma:
.....……
.....
.....
.....
.....
.....
……...
……...

Oktató neve: .....…..……. beosztása: .....…….
aláírása: .....…..
* a megfelelő szöveg aláhúzandó

JELENLÉTI IV

Az elhangzottakat tudomásul vettük és magunkra nézve kötelezőnek ismerjük el

Sor-szám	**Oktatásban részesülők**		
	neve	**beosztása, munkakör**	**aláírása (hiányzás oka)**
1.			
2.			
3.			
4.			