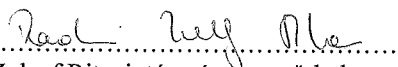


A Boldog Gizella Alapítvány Gizella Otthon

Belső adatvédelmi és adatbiztonsági szabályzata

a természetes személyek személyes adatainak kezelésével összefüggő védelme érdekében

Készítette: dr. Anda Péter adatvédelmi tisztviselő
Jóváhagyta: Radnai-Zulauf Rita intézményvezető-helyettes
Kiadás napja: 2026. 04. 01.


Radnai-Zulauf Rita intézményvezető-helyettes

Fenntartói tudomásul vétel kelte: 2026.04.15.

BOLDOG GIZELLA
ALAPÍTVÁNY
2051 Biatorbágy, Boldog Gizella u. 1.
Adószám: 18690125-1-13

TARTALOM

I. Az adatkezelő adatai	6
II. A belső adatvédelmi és adatbiztonsági szabályzat rendeltetése	7
III. Jogszabályi háttér, alkalmazandó jog.....	8
IV. A belső adatvédelmi és adatbiztonsági szabályzat hatálya és módosítása	9
<i>Tárgyi és időbeli hatály:</i>	9
<i>Személyi hatály, érintettek köre:</i>	9
<i>A belső adatvédelmi és biztonsági szabályzat módosítása</i>	9
V. Fogalom-meghatározások	10
VI. Az intézmény adatkezelő szervezete.....	13
1. Az intézményvezető	13
2. Az adatvédelmi tisztviselő	13
Az adatvédelmi tisztviselővé kinevezés feltételei:	14
Az adatvédelmi tisztviselő feladatai	14
Az adatvédelmi tisztviselő jogállása	14
Az adatvédelmi tisztviselő titoktartási kötelezettsége	15
3. A szervezeti egység vezetője.....	15
4. Az intézmény fenntartója.....	Hiba! A könyvjelző nem létezik.
5. Az adatkezelő irányítása alatt adatkezelést végző foglalkoztatottak.....	15
6. Adatfeldolgozók	16
VII. Az intézmény által végzett adatkezelés	17
1. Az adatkezelés alapelvei	17
2. Új adatkezelés bevezetésével összefüggő eljárásrend és a Hatásvizsgálat	17
3. Az adatkezelési tevékenységek nyilvántartása	19
4. Az adatkezelési tevékenységek jogszerűsége	19
5. Az érintett jogai és gyakorlásához kapcsolódó eljárási szabályok	20
5.1. Tájékoztatáshoz való jog.....	20
5.2. Az érintett hozzáférési joga és iratbetekintéshez való jog.....	22
5.3. A helyesbítéshez való jog.....	23

5.4. A törléshez való jog („az elfeledtetéshez való jog”)	23
5.5. Az adatkezelés korlátozásához való jog	24
5.6. A személyes adatok helyesbitéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség	25
5.7. Az adathordozhatósághoz való jog	25
5.8. A tiltakozáshoz való jog	25
6. Az intézménnyel foglalkoztatási jogviszonyban álló természetes személyek adatainak kezelése	27
6.1. Általános szabályok	27
6.2. Mobiltelefon használatához kapcsolódó adatkezelési tevékenység	27
6.3. Az e-mail cím használatához kapcsolódó adatkezelési tevékenység	27
6.4. A számítógépek használatához kapcsolódó adatkezelési tevékenység	28
6.5. Az intézményhez munkára jelentkezők személyes adataihoz kapcsolódó adatkezelési tevékenység	28
6.6. Az intézménnyel jogviszonyban álló természetes személyek alkalmassági vizsgálataival kapcsolatos adatok kezelése	29
6.7. Az intézménnyel foglalkoztatási jogviszonyban álló természetes személyek fényképeinek kezelése	30
6.8. Szociális alap-, mester-, és szakképzésben résztvevő hallgatók fogadása /terepgyakorlat biztosítása/	30
7. Cookie-k alkalmazása és Közösségi oldalon profil fenntartása	30
8. Szocio.NET szoftver alkalmazása	30
9. Csalseg.net.hu program alkalmazása	Hiba! A könyvjelző nem létezik.
10. IQtató iktatási program használata	Hiba! A könyvjelző nem létezik.
11. Számítógép megosztott adattartalma	31
12. Az intézményi tevékenységgel kapcsolatos adatkezelési előírások	31
13. Céghatár működtetéséhez kapcsolódó adatkezelési rendelkezések	32
14. Adományozás	32
15. Egészségügyi szolgáltatásokhoz kapcsolódó kiegészítő adatkezelési szabályok	32
16. Adattovábbítás	33
16. 1. Magyar Államkincstár felé történő adattovábbítás	33
17. Gyermekünk védelmében elnevezésű informatikai rendszer	Hiba! A könyvjelző nem létezik.
18. Esetmegbeszélésen és esetkonferencián készített hangfelvétel	Hiba! A könyvjelző nem létezik.
VIII. Az adatvédelmi incidens és kezelése	34

1. AZ ADATVÉDELMI INCIDENS KEZELÉSÉNEK FOLYAMATÁBRÁJA	34
2. Az adatvédelmi incidens észlelése.....	35
2. Az adatvédelmi incidens bejelentése	35
3. Az adatvédelmi incidens kockázatosságának, súlyosságának megállapítása	36
3.1. Az értékelés főbb körülményei:.....	36
3.2. A DPC pontszámának meghatározása:	37
3.3. Az EI pontszám meghatározása.....	38
3.4. A CB pontszám meghatározása.....	38
4. Adatvédelmi incidensek nyilvántartása.....	39
IX. Adatbiztonság	40
1. Az adatbiztonság alapelvei	40
2. Az adatbiztonsági ellenőrzés.....	40
2.1. A védelmi igény feltárása.....	40
2.2. Fenyegtettség-elemzés.....	40
2.3. Kockázatelemzés	42
2.4. Kockázatkezelés	42
3. Adatbiztonsági előírások és eljárási szabályok	42
3.1. Beléptetés és elektronikus megfigyelési rendszer	42
3.2. Iratok tárolása, helyiségek őrzése.....	43
3.3. Informatikai biztonsági előírások	44
3.4. Oktatás.....	44
Mellékletek	45
1. számú melléklet – A belső adatvédelmi és adatbiztonsági szabályzat megismerésének a jegyzéke.....	45
2. számú melléklet - Ellenőrzési nyomvonal.....	46
3. számú melléklet – Az adatkezelési tevékenységek nyilvántartása	50
4. számú melléklet- adatvédelmi incidensek nyilvántartása minta	50
5. számú Adatbiztonsági ellenőrzésről készített jegyzőkönyv	50
6. számú melléklet – Adatkezelési hozzájárulás	54
7. számú melléklet – Hozzájárulás a személyes adatoknak a szociális alap-, mester-, és szakképzésben résztvevő hallgatók.....	55

8. számú melléklet – Adatkezeléshez hozzájárulás visszavonása formanyomtatvány	56
9. számú melléklet – Nyilatkozat adatkezelési tájékoztatás megtörténtéről és adatkezelési tájékoztató megismeréséről	57
10. számú melléklet – Formanyomtatvány iratbetekintési jog, személyes adatokhoz való hozzáférési jog gyakorlásához	Hiba! A könyvjelző nem létezik.
11. számú melléklet Iratbetekintés engedélyezését megelőző iratellenőrzési ív.....	Hiba! A könyvjelző nem létezik.
12. számú melléklet – Foglalkoztatott adatkezelési hozzájárulása	59
13. számú melléklet – foglalkoztatotti Nyilatkozat adatkezelési tájékoztató megismeréséről.....	59
14. számú melléklet - Értesítés sikertelen pályázatról.....	60
15. számú melléklet - Kérelem pályázat őrzéséhez	61
16. számú melléklet – Elhelyezett kamerák és megfigyelt területek leírása	62
17. számú melléklet – Kulcs-nyilvántartás.....	62
18. számú melléklet – Adott helyiségben önállóan tartózkodható személyek listája	63
19. számú melléklet – Az informatikai rendszerek jelszavait tartalmazó adattábla minta.....	64
20. számú melléklet – Adatvédelmi, adatbiztonsági oktatási napló.....	65
21. számú melléklet – Nem automatikus adatmentésről felvett teljesítési igazolás.....	66
22. számú melléklet – Megbízólevél.....	Hiba! A könyvjelző nem létezik.
23. számú melléklet – Igazolás gyógyszerek átvételére történő felhatalmazásról.....	67
24. számú melléklet – Igazolás orvosi iratok átvételére történő felhatalmazásról	68
25. számú melléklet – adatkezelési tájékoztatók	71
26. számú melléklet – személyes adat törlésére jegyzőkönyv, adathordozó megsemmisítéséről jegyzőkönyv	69

I. AZ ADATKEZELŐ ADATAI

Az adatkezelő adatai és elérhetőségei

Név:	Boldog Gizella Alapítvány (továbbiakban Intézmény)
Cím:	2051 Biatorbágy, Boldog Gizella utca 1.
Telefon:	+36 23 530 550+36 23 530-550
Email:	info@gizella.hu
Weboldal:	www.gizella.hu
Adatvédelmi tisztviselő neve:	dr. Anda Péter
Adatvédelmi tisztviselő elérhetősége:	dr.anda.peter@gmail.com , 06702762663
Adatvédelmi tisztviselő ügyfélfogadása:	Előzetes egyeztetés alapján

II. A BELSŐ ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT RENDELTETÉSE

1. Az intézmény 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.
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.
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.
4. A jelen szabályzat célja tehát a természetes személyek személyes adatainak következetes és magas szintű védelmének és az adatkezelés jogszerűségének biztosítása, továbbá az érintetteknek tájékoztatás megadása a beépített és alapértelmezett adatvédelem követelményeinek figyelembevételével.
5. 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 jelen szabályzatot alkotta meg és melynek integráns részét képezi az Európai Parlament és a Tanács 2016/679 rendelete (Általános Adatvédelmi rendelet) 12. cikkében foglaltaknak való megfelelés érdekében kiadott adatkezelési tájékoztatók.
6. A jelen szabályzat és az adatkezelési tájékoztatók információt adnak
 - az intézmény által alkalmazott adatvédelmi és adatbiztonsági szabályokról, megtett intézkedésekről,
 - az érintettek 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 adatkezeléssel összefüggő működésének alapjául szolgál.

7. Jelen szabályzat külön rögzíti az adatvédelmi elveket, amelyeket az intézmény 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.

III. JOGSZABÁLYI HÁTTER, ALKALMAZANDÓ JOG

A belső adatvédelmi és adatbiztonsági szabályzat rendelkezéseinek alapjául különösen az alábbi jogszabályok szolgálták:

- a. a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló az Európai Parlament és a Tanács 2016/679 rendelete (Általános adatvédelmi rendelet)
- b. az információs önrendelkezési jogról és az információ szabadságról szóló 2011. évi CXII. törvényben (továbbiakban: Infotv.)
- c. a szociális igazgatásról és szociális ellátásokról szóló 1993. évi III. törvény (továbbiakban: Szt.),
- d. az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény
- e. a személyes gondoskodást nyújtó szociális intézmények szakmai feladatairól és működésük feltételeiről szóló 1/2000. (I. 7.) SzCsM rendelet
- f. a személyes gondoskodást végző személyek adatainak működési nyilvántartásáról szóló 8/2000. (VIII. 4.) SzCsM rendelet
- g. a személyes gondoskodást nyújtó szociális ellátások térítési díjáról szóló 29/1993. (II. 17.) Korm. rendelet
- h. szakmai protokollok
- i. az otthoni szakápolási tevékenységről szóló 20/1996. (VII. 26.) NM rendelet
- j. az egészségügyi szolgáltatások nyújtásához szükséges szakmai minimumfeltételekről szóló 60/2003. (X. 20.) ESzCsM rendelet

IV. A BELSŐ ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT HATÁLYA ÉS MÓDOSÍTÁSA

TÁRGYI ÉS IDŐBELI HATÁLY:

1. A jelen tájékoztató hatálya az intézmény, mint adatkezelő által végzett adatkezelési tevékenységre terjed ki a kiadás napjától kezdődően, annak visszavonásáig.
2. Jelen adatkezelési szabályzat hatályon kívül helyezi az adatkezelő valamennyi korábbi adatkezelési szabályzatát, belső utasítást. Adatkezelési tevékenységet a társaság a továbbiakban jelen adatkezelési szabályzat alapján végez.

SZEMÉLYI HATÁLY, ÉRINTETTEK KÖRE:

- a. az intézménnyel foglalkoztatási jogviszonyban álló természetes személyek
- b. az intézmény természetes személy ügyfelei, szolgáltatást igénybe vevők
- c. az intézménnyel kapcsolatba kerülő természetes személyek.

A BELSŐ ADATVÉDELMI ÉS BIZTONSÁGI SZABÁLYZAT MÓDOSÍTÁSA

1. A szabályzat módosítására az intézmény bármely dolgozója javaslatot tehet az intézményvezetőnek megküldött, de az adatvédelmi tisztviselőnek címzett írásbeli megkeresésben.
2. A megkeresésnek tartalmaznia kell a dolgozó nevét, aláírását, elérhetőségét, a javasolt módosítást röviden összefoglalva, továbbá a módosítás szükségességét alátámasztó indokokat.
3. A megkeresés iktatás után kiszignálásra kerül az adatvédelmi tisztviselőhöz, aki megvizsgálja a javasolt módosításokat, elkészíti ajánlását a javasolt módosítás tekintetében.
4. A megkeresés az ajánlással együtt megküldésre kerül az érintett szakmai vezetőnek, illetve az intézményvezetőnek, aki jóváhagyja a módosítás előkészítését.
5. Az adatvédelmi tisztviselő előkészíti a módosítás tervezetét és megküldi az érintett szakmai vezetőnek, az intézményvezetőnek egyeztetésre.
6. A módosítási eljárás szabályait a szakmai vezető, illetve intézményvezető megkeresése alapján indított módosítási eljárás esetében is megfelelően alkalmazni kell.
7. Az intézmény honlapján a módosítás előtti és utáni változatokat is közzé kell tenni a hatályba lépés és a hatályon kívül helyezés időpontjának megjelölése mellett.
8. A módosításokat az intézmény foglalkoztatottjaival, illetve folyamatban lévő ügyek esetében az érintettekkel meg kell ismertetni.

A belső adatvédelmi és adatbiztonsági szabályzat alkalmazásában:

1. **érintett:** bármely információ alapján azonosított vagy azonosítható természetes személy;
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 a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;
3. **személyes adat:** az érintettre vonatkozó bármely információ;
4. **különleges adat:** a személyes adatok különleges kategóriába tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok,

genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered;

biometrikus adat: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat;

egészségügyi adat: egy természetes személy testi vagy szellemi 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;

5. **hozzájárulás:** az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez;
6. **adatkezelő:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;
9. **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 hajtja végre az adatfeldolgozóval;
7. **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, iriszkép) rögzítése;
8. **adatkezelési tevékenység:** az intézményi feladatok, és az intézmény által kifejtett tevékenységek, mely során adatkezelés valósul meg;
9. **adatkezelési tevékenységek nyilvántartása:** adatkezelő a felelősségébe tartozóan végzett adatkezelési tevékenységeiről vezetett nyilvántartás (jelen szabályzat 3. számú melléklete);

10. **adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
10. **közvetett adattovábbítás:** személyes adatnak valamely harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbítása útján valamely más harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítása;
11. **nemzetközi szervezet:** a nemzetközi közjog hatálya alá tartozó szervezet és annak alárendelt szervei, továbbá olyan egyéb szerv, amelyet két vagy több állam közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre;
11. **nyilvánosságra hozatal:** az adat bárki számára történő hozzáférhetővé tétele;
12. **adattörlés:** az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
13. **adatkezelés korlátozása:** a tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölése útján;
14. **adatmegsemmisítés:** az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;
15. **adatfeldolgozás:** az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége;
16. **adatfeldolgozó:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel - az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel;
17. **adatállomány:** az egy nyilvántartásban kezelt adatok összessége;
18. **harmadik személy:** olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek;
19. **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;
20. **harmadik ország:** minden olyan állam, amely nem EGT-állam;
21. **adattvédelmi incidens:** az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi;
22. **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;
23. **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;
24. **átláthatóság:** személyes adat olyan módon történő kezelése, amely - a személyes adattól elkülönítve tárolt - további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely

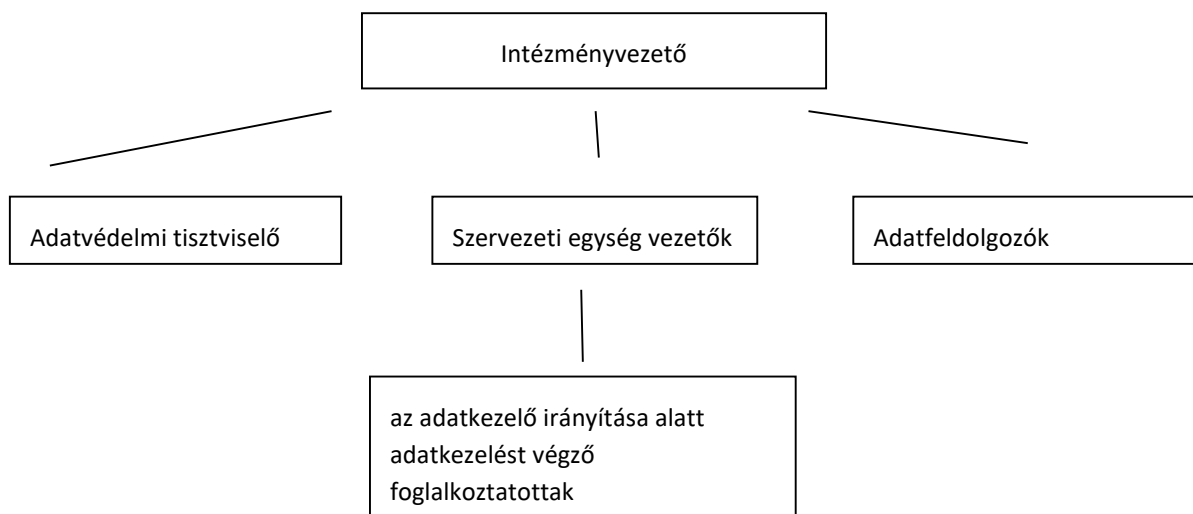
érintettre vonatkozik, valamint műszaki és szervezési intézkedések megtételével biztosítja, hogy azt azonosított vagy azonosítható természetes személyhez ne lehessen kapcsolni.

25. **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: 1055 Budapest, Falk Miksa utca 9-11, postacím: 1363 Budapest, Pf.: 9., E-mail: ugyfelszolgalat@naih.hu, URL: <http://naih.hu>
26. **adatvédelmi tisztviselők konferenciája:** a Hatóság és az adatvédelmi tisztviselők rendszeres szakmai kapcsolattartását szolgálja, célja a személyes adatok védelmére és a közérdekű adatok megismerésére vonatkozó jogszabályok alkalmazása során az egységes joggyakorlat kialakítása. A konferenciát a Hatóság elnöke szükség szerint, de évente legalább egyszer hívja össze, és meghatározza napirendjét.



VI. AZ INTÉZMÉNY ADATKEZELŐ SZERVEZETE

1. Az intézmény valamennyi foglalkoztatottja számára kötelező az adatvédelmi és adatbiztonsági szabályok, valamint a munkavégzésükre vonatkozó szakmai adatvédelmi és adatbiztonsági szabályok és előírások betartása.
2. Az intézmény adatkezelő szervezetének felépítése:
 - intézményvezető
 - adatvédelmi tisztviselő
 - szervezeti egység vezető
 - az adatkezelő irányítása alatt adatkezelést végző foglalkoztatottak
 - adatfeldolgozók



1. AZ INTÉZMÉNYVEZETŐ

1. Az intézmény törvényes képviselője, vezető állású munkavállaló. Jogviszonyának keltezését és megszűnését jogszabály szabályozza. Az intézmény szervezeti egységeinek összehangolt irányítását végzi.
2. A belső adatvédelmi és adatbiztonsági szabályzatot az intézményvezető hagyja jóvá.
3. Az intézményvezető feladata és felelőssége, hogy az adatkezelő olyan megfelelő technikai és szervezési intézkedéseket – például árnevesítést – hajtson végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az Általános adatvédelmi rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése. Az adatkezelő a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során az adatkezelés folyamatába szabályoznia kell az intézményben foglalkoztatottak, valamint az intézményi ellátást igénybe vevő ellátottak adatvédelmével, adatbiztonságával kapcsolatos feladatokat.
4. Az intézményvezetőnek feladata, hogy folyamatosan ellenőrizze, figyelemmel kíséresse, hogy az intézményben történő adatkezelés megfelel-e a jogszabályokban, valamint a belső dokumentumokban meghatározott szabályoknak.
5. Az intézményvezető adatvédelmi tisztviselőt jelöl ki.

2. AZ ADATVÉDELMI TISZTVISELŐ

1. Az intézmény a személyes adatok kezelésére vonatkozó jogi előírások teljesítésének és az érintettek jogai érvényesülésének elősegítése érdekében adatvédelmi tisztviselőt alkalmaz.

2. Az adatvédelmi tisztviselő neve és elérhetősége megtalálható a jelen szabályzat I. pontjában az adatkezelő adatainál.
3. Az adatvédelmi tisztviselő nevét és elérhetőségét közzé kell tenni:
 - az intézmény székhelyén és telephelyén jól látható módon
 - az intézmény honlapján
 - az adatkezelési tájékoztatókban
 - az adatkezelési tevékenységek nyilvántartásában
 - az adatvédelmi incidensek nyilvántartásában
 - az érintett hozzáférési jogával kapcsolatos intézkedések nyilvántartásában

AZ ADATVÉDELMI TISZTVISELŐVÉ KINEVEZÉS FELTÉTELEI:

4. Adatvédelmi tisztviselőnek az jelölhető ki, aki a személyes adatok védelmére vonatkozó jogi előírások és jogalkalmazási gyakorlat megfelelő szintű ismeretével rendelkezik és alkalmas a jogszabályban és a jelen szabályzatban meghatározott feladatok ellátására.
 - Jogi és jogalkalmazási gyakorlat megfelelő szintű ismerettel rendelkezik az a személy, aki jogász végzettséggel rendelkezik, illetve a TÜV Rheinland InterCert által igazolt adatvédelmi tisztviselő vizsgakövetelményei alapján sikeres vizsgát tett.
 - A jogszabályban meghatározott feladatok ellátására való alkalmasságot az intézményvezető felvételi elbeszélgetésen állapítja meg.

AZ ADATVÉDELMI TISZTVISELŐ FELADATAI

5. Az adatvédelmi tisztviselő elősegíti az adatkezelő, illetve az adatfeldolgozó - a személyes adatok kezelésére vonatkozó jogi előírásokban meghatározott - kötelezettségeinek teljesítését, így különösen:
 - a. a személyes adatok kezelésére vonatkozó jogi előírásokról naprakész tájékoztatást nyújt és azok érvényesítésének módjaival kapcsolatban tanácsot ad az intézmény, mint adatkezelő és az általa foglalkoztatott, az adatkezelési műveleteket végző személyek részére;
 - b. folyamatosan figyelemmel kíséri és ellenőrzi a személyes adatok kezelésére vonatkozó jogi előírások, így különösen a jogszabályok és belső adatvédelmi és adatbiztonsági szabályzat érvényesülését, ennek keretei között az egyes adatkezelési műveletekhez kapcsolódó egyértelmű feladat-meghatározás, az adatkezelési műveletekben közreműködő foglalkoztatottak adatvédelmi ismereteinek bővítése és tudatosságnövelése, valamint a rendszeres időközönként lefolytatandó vizsgálatok megvalósulását;
 - c. elősegíti az érintettet megillető jogok gyakorlását, így különösen kivizsgálja az érintettek panaszait és kezdeményezi az adatkezelőnél, illetve az adatfeldolgozónál a panasz orvoslásához szükséges intézkedések megtételét,
 - d. szakmai tanácsadással elősegíti és figyelemmel kíséri az adatvédelmi hatásvizsgálat lefolytatását,
 - e. együttműködik az adatkezelés jogszerűségével kapcsolatos eljárások lefolytatására jogosult szervekkel és személyekkel, így különösen kapcsolatot tart a Hatósággal az előzetes konzultáció és a Hatóság által lefolytatott eljárások elősegítése érdekében,
 - f. közreműködik a belső adatvédelmi és adatbiztonsági szabályzat megalkotásában
 - g. az érintettek a személyes adataik kezeléséhez és a személyes adatok kezeléséhez kapcsolódó jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak, melynek keretében köteles megvizsgálni a kérelem tárgyát és a szükséges intézkedést megtenni.
 - h. részt vesz a Hatóság által szervezett adatvédelmi tisztviselők konferenciáján.

AZ ADATVÉDELMI TISZTVISELŐ JOGÁLLÁSA

6. Az intézmény adatvédelmi tisztviselője szolgáltatási szerződés alapján, megbízási jogviszony keretében látja el tevékenységét.
7. A megbízási jogviszony határozatlan időtartamra jön létre.

8. A jogviszony megszüntethető bármelyik fél által a másik fél súlyos szerződés szegése esetén azonnali hatállyal, míg legalább 30 nap, maximum 90 nap felmondási idő alkalmazásával felmondással. A felmondási idő mértékét a felek a szolgáltatási szerződésben állapítják meg.
9. Az adatvédelmi tisztviselő a tevékenységének ellátásáért megbízási díjra jogosult, melynek mértékét a szolgáltatási szerződés tartalmazza. A díj meghatározásánál figyelemmel kell lenni az intézmény költségvetésére, az érintettek és a foglalkoztatottak számára, a rendelkezésre állás időtartamára.
10. Az adatvédelmi tisztviselő egyidejűleg több adatkezelő, illetve adatfeldolgozó tekintetében is elláthatja az adatvédelmi tisztviselő jogszabályban meghatározott feladatait, ha az feladatainak szakszerű és hatékony ellátását nem veszélyezteti. Az adatvédelmi tisztviselő szóban tájékoztatja az intézményvezetőt arról, hogy mely más adatkezelőnél vagy adatfeldolgozónál lát el adatvédelmi tisztviselői feladatokat.
11. Az intézmény biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.
12. Az intézmény támogatja az adatvédelmi tisztviselőt a feladatai ellátásában, biztosítja számára azokat az forrásokat, amelyek a feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek.
13. Az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől nem fogadhat el. Az intézmény az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül az intézményvezetőnek tartozik felelősséggel.
14. Az adatvédelmi tisztviselő az intézményben más feladatokat is elláthat.

AZ ADATVÉDELMI TISZTVISELŐ TITOKTARTÁSI KÖTELEZETTSÉGE

1. Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.
2. Az adatvédelmi tisztviselő jogviszonyának fennállása alatt és annak megszűnését követően is titokként megőrzi a tevékenységével, annak ellátásával kapcsolatban tudomására jutott személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy körülményt, amelyet az intézmény nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni.

3. A SZERVEZETI EGYSÉG VEZETŐJE

1. A szervezeti egység vezetője munkájával segíti az intézményvezető és az adatvédelmi tisztviselő munkáját, közreműködik az adatvédelmi és adatbiztonsági szabályok betartásában.
2. Ellenőrzi a szervezeti egységnek az adatkezelési és adatbiztonsági szabályoknak történő megfelelést.
3. A szervezeti egység vezetője az általa vezetett terület jogszabályváltozásairól beszámol az adatvédelmi tisztviselőnek és az adatvédelmi tisztviselővel közösen értékeli a jogszabályváltozás hatását az intézményi adatkezelésre és kezdeményezi az új adatkezelésre vonatkozó eljárás megindítását.

4. AZ ADATKEZELŐ IRÁNYÍTÁSA ALATT ADATKEZELÉST VÉGZŐ FOGLALKOZTATOTTAK

1. Az adatkezelő irányítása alatt adatkezelést végző foglalkoztatottak munkájukkal segítik a szakmai vezetők és az adatvédelmi tisztviselő munkáját, közreműködnek az adatvédelmi és adatbiztonsági szabályok betartásában.
2. A munkavégzését érintő terület jogszabályváltozásairól beszámol az adatvédelmi tisztviselőnek és a szakmai vezetőnek és közösen értékeli a jogszabályváltozás hatását az intézményi adatkezelésre és kezdeményezi az új adatkezelésre vonatkozó eljárás megindítását.

3. Az adatkezelő irányítása alatt adatkezelést végző foglalkoztatottak munkaköri leírásában vagy szerződésben fel kell tüntetni:
„A foglalkoztatott feladata a Belső adatvédelmi és adatbiztonsági szabályzatban, az adatkezelési tevékenységek nyilvántartásában és az intézmény adatvédelem és adatbiztonsággal összefüggő valamennyi belső szabályzatban, utasításban, valamint jogszabályi rendelkezésben foglalt rendelkezés betartása, valamint az adatvédelmi tisztviselő felé jelezni, amennyiben tevékenysége személyes adatok kezelését érintő változással jár.”

6. ADATFELDOLGOZÓK

1. Az intézmény, mint adatkezelő a nevében adatkezelést végző adatfeldolgozókat vehet igénybe az adatkezelése során.
2. Az adatfeldolgozókkal adatfeldolgozási megállapodást kell kötni, melyben
 - a. kijelenti, hogy betartja az Európai Unió és Magyarország területén hatályos adatvédelmi és adatbiztonsági szabályokat, vele szemben nincs folyamatban semmilyen eljárás adatvédelmi szabályok megsértése miatt, amennyiben ezen tárgykörben eljárás indul, abban az esetben 5 munkanapon belül tájékoztatja az adatkezelőt
 - b. kötelezettséget vállal arra, hogy az intézmény és az érintett természetes személy valamennyi kárát, elmaradt vagyoni előnyét stb. megtéríti, amennyiben adatkezelési tevékenysége jogszabálysértő jellege megállapításra kerülne.
 - c. kijelenti, hogy az intézménnyel kötött megbízási szerződés szerinti feladata teljesítése körében személyes adatokat kizárólag az intézmény utasításai alapján kezel – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is – , kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; mely esetben erről a jogi előírásról az intézményt az adatkezelést megelőző 10 munkanapon belül értesíti, kivéve, ha ezen értesítést az adott jogszabály fontos közérdekből tiltja. Vállalja, hogy haladéktalanul tájékoztatja az intézményt, ha úgy ítéli meg, hogy az utasítása sérti az Általános adatvédelmi rendeletet (GDPR) vagy a tagállami vagy uniós adatvédelmi rendelkezéseket.
 - d. vállalja a személyes adatok kezelésével összefüggő titoktartási kötelezettséget.
 - e. rögzíteni kell az adatbiztonság megvalósulása érdekében megtett intézkedéseit
 - f. nyilatkoznia kell a további adatfeldolgozó igénybevételéről
 - g. vállalja, hogy az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében minden szükséges intézkedést megtesz, elősegíti az intézmény kötelezettségeinek teljesítését, az intézmény adatvédelmi tisztviselőjével együttműködik
 - h. segíti az intézményt az adatbiztonság, az adatvédelmi incidensek kezelésében, az adatvédelmi hatásvizsgálatban, a hatósággal történő előzetes konzultációban, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat
 - i. vállalja, hogy az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő.
 - j. az intézmény rendelkezésére bocsát minden olyan információt, amely a vállalt kötelezettségei teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.
3. Az informatikai feladatokat ellátó adatfeldolgozóval szemben támasztott követelményeket a jelen szabályzat, valamint az intézmény Informatikai Biztonsági szabályzata tartalmazza.

VII. AZ INTÉZMÉNY ÁLTAL VÉGZETT ADATKEZELÉS

1. AZ ADATKEZELÉS ALAPELVEI

- 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. Az adatkezelés jogalapját az adatkezelési tájékoztatók tartalmazzák.

A tisztesség megköveteli az érintetti autonómia érvényre juttatását, az interakciót az adatkezelő és az érintett között, a megtévesztés tilalmát, a hátrányos megkülönböztetés tilalmát, a kockázatátíthatóság tilalmát.

Az átláthatóság 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.
- 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 és az adatkezelési tájékoztatók tartalmazzák.

A személyes adatokat az intézmény nem kezeli a célokkal össze nem egyeztethető módon.
- 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.
- 4. Pontosság elve**

Az intézmény törekszik a személyes adatok pontosságára naprakészségére, melynek betartása érdekében a jelen szabályzatba foglalt intézkedéseket teszi meg.
- 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.
- 6. Integritás és bizalmas jelleg elve**

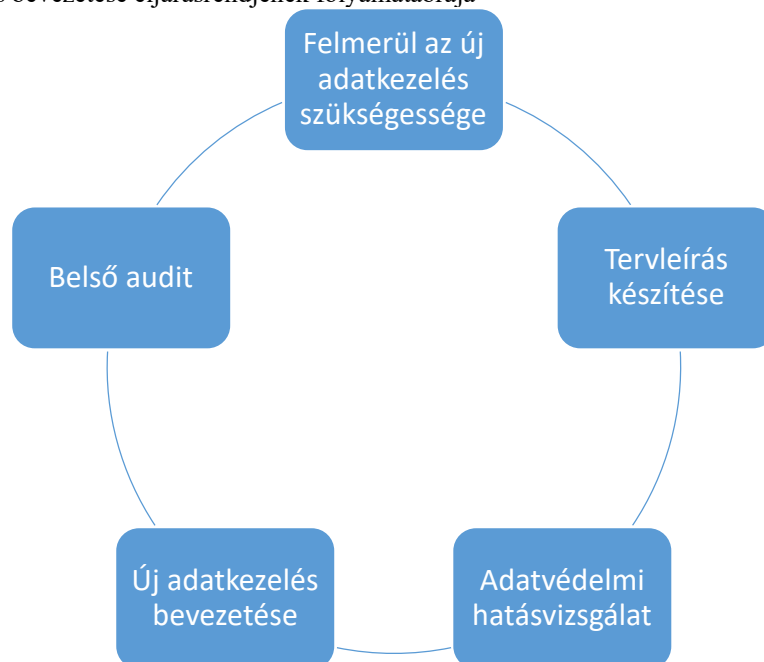
A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni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

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

2. ÚJ ADATKEZELÉS BEVEZETÉSÉVEL ÖSSZEFÜGGŐ ELJÁRÁSREND ÉS A HATÁSVIZSGÁLAT

- 1. Az intézmény bármely dolgozója kezdeményezheti a szakmai vezetője támogatásával az intézményvezetőnél új adatkezelés megkezdését.**

2. Az intézményvezető a javasolt, vagy felmerülő új adatkezelés részleteit és az új adatkezelés bevezetésének folyamatát, a hatásvizsgálatot megelőzően egyeztetni az adatvédelmi tisztviselővel, továbbá az érintett szakmai vezetőkkel, foglalkoztatottakkal. Az egyeztetésről adatkezelési tervleírás készül, mely az adatvédelmi hatásvizsgálat alapja. A tervleírásban rögzíteni kell különösen a tervezett adatkezelés folyamatait, módszeres leírását, az adatkezelés céljainak ismertetését, az adatkezelés körülményeit, jellegét, a személyes adatok és érintettek kategóriáit.
3. Az Intézmény a tervezett adatkezelés megkezdését megelőzően felméri, hogy a tervezett adatkezelés, annak körülményeire, így különösen céljára, az érintettek körére, az adatkezelési műveletek során alkalmazott technológiára tekintettel várhatóan milyen hatásokat fog gyakorolni az érintetteket megillető alapvető jogok érvényesülésére.
4. A hatásvizsgálathoz a <https://www.naih.hu/hatasvizsgalati-szoftver> honlapon elérhető szoftver alkalmazására is sor kerülhet.
5. Az adatkezelő az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő szakmai tanácsát köteles kikérni.
6. A hatásvizsgálat kiterjed legalább:
 - a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;
 - az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
 - az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és
 - a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.
7. Amennyiben megállapításra kerül a hatásvizsgálat eredményeként, hogy az adatkezelés végezhető, abban az esetben a hatásvizsgálat alapján megtervezésre kerülnek a szükséges technikai és szervezési intézkedések, melybe bevonásra kerülnek az érintett szakmai vezetők.
8. Az adatkezelő szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.
9. Az új adatkezelés bevezetése eljárásrendjének folyamatábrája



3. AZ ADATKEZELÉSI TEVÉKENYSÉGEK NYILVÁNTARTÁSA

1. Az intézmény a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet, továbbiakban adatkezelési tevékenységek nyilvántartása. Az adatkezelési tevékenységek nyilvántartását jelen szabályzat 3. számú melléklete tartalmazza.
2. Az adatkezelési tevékenységek nyilvántartásának módosítására a belső adatvédelmi és adatbiztonsági szabályzat módosítására vonatkozó szabályokat megfelelően alkalmazni kell.
3. A nyilvántartás a következő információkat – táblázatos formában - tartalmazza:
 - a) az adatkezelő nevét és elérhetőségét,
 - b) az adatvédelmi tisztviselőnek a nevét és elérhetőségét (postai cím, elektronikus levél cím);
 - c) az adatkezelés céljait;
 - d) az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetését;
 - e) olyan címzettek kategóriáit, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
 - f) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információkat, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint az Általános adatvédelmi rendelet 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírását;
 - g) a különböző adatkategóriák törlésére előírt határidőket, amennyiben az lehetséges;
 - h) az adatvédelem és adatbiztonság érdekében a technikai és szervezési intézkedések általános leírását.
4. Az adatkezelési tevékenységek nyilvántartása vezetésének szükségességét alátámasztó tényeket az adatkezelési tevékenységek nyilvántartása tartalmazza és az alábbi körülményeket kell megvizsgálni:
 - foglalkoztatottak száma
 - az adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár-e
 - az adatkezelés alkalmi jellegű-e
 - az intézmény folytat-e a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése adatkezelést
 - a büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok kezelését végzi-e.
5. A 4. pont szerinti leírást az adatkezelési tevékenységek nyilvántartásában „igen” „nem” jelöléssel kell ellátni, és aláhúzással kell jelölni a végkövetkeztetést.
6. A mérlegelésen alapuló adatkezelési tevékenység nyilvántartás vezetési kötelezettség esetében a végkövetkeztetést indokolással kell ellátni, melyet az adatkezelési tevékenységek nyilvántartása tartalmazza. Az indokolásnak egyértelműnek és a végkövetkeztetés megállapítására alkalmasnak kell lennie.

4. AZ ADATKEZELÉSI TEVÉKENYSÉGEK JOGSZERŰSÉGE

1. Az intézmény által végzett adatkezeléssel kapcsolatos rendelkezéseket tartalmazhatja:
 - jogszabály, különösen jelen szabályzat III. pontjában hivatkozott jogszabályok
 - a jelen szabályzat
 - az intézményi szabályzatok adatkezeléssel kapcsolatos részei, melyek kiegészíthetik jelen szabályzat rendelkezéseit
 - az adatkezelési tevékenységek nyilvántartása
 - az adatkezelési tájékoztatók
2. Az adatkezelési tevékenységeket az intézmény elsődlegesen jogszabályi felhatalmazás és közérdekű feladatainak ellátása keretében végez a feladatainak ellátásához szükséges mértékben. Az adatkezelési tevékenységek nyilvántartása adatonként – táblázatos formában – tartalmazza az adott adat kezelésének jogalapját. Az intézményi adatkezelésekhez kapcsolódó információkat az adatkezelési tájékoztatók tartalmazzák. Amennyiben intézményi szabályzat külön adatkezelésre vonatkozó rendelkezéseket tartalmaz, akkor azt jelen szabályzattal összhangban, azt kiegészítve kell értelmezni és alkalmazni.

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 adatkezelési tevékenységre, cél tekintetében külön is tartalmazza a hozzájárulást.
4. Az írásbeli hozzájárulás esetén a hozzájárulást a 6. számú melléklet szerinti formanyomtatványokon, vagy az intézmény által a Szervezeti és Működési Szabályzat mellékleteként használt formanyomtatványon, vagy a jogszabály alapján rendszeresített formanyomtatványon, vagy bármilyen olyan formában kell megadni, ami alkalmas az érintett akaratának igazolására.
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.
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. 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 következtetni hozzájárulás visszavonásának kell tekinteni. Az érintett az adatkezeléshez hozzájárulása visszavonását a 8. számú melléklet szerinti formanyomtatványon is bejelentheti.

5. AZ ÉRINTETT JOGAI ÉS GYAKORLÁSÁHOZ KAPCSOLÓDÓ ELJÁRÁSI SZABÁLYOK

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
2. Az intézmény minden dolgozója köteles az érintettek jogainak érvényesülése érdekében szükséges intézkedéseket elősegíteni.
3. Az érintetti joggyakorláshoz kapcsolódó ellenőrzési nyomvonalat a 2. számú melléklet tartalmazza.

5.1. TÁJÉKOZTATÁSHOZ VALÓ JOG

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 következményekkel 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.
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.
3. Az érintett tájékoztatása négy lépésben történik meg.

1. lépés:

A belső adatvédelmi és adatbiztonsági szabályzat és mellékletei elektronikus formában és papír alapon közzétételre kerül. Elektronikusan kerül közzétételre az intézmény honlapjára történő feltöltéssel, míg papír alapon az intézmény székhelyén és telephelyein történő kifüggesztéssel vagy rendelkezésre tartással.

Az intézmény honlapján jól látható helyen „adatvédelem” elnevezéssel létrehozásra került egy fül, melyre feltöltésre került az intézmény belső adatvédelmi és adatbiztonsági szabályzata és mellékletei, külön figyelemfelhívással ellátva az adatvédelmi tisztviselő elérhetőségei.

A belső adatvédelmi és adatbiztonsági szabályzat az intézmény székhelyén és telephelyén nyomtatott formában rendelkezésre áll. A belső adatvédelmi és adatkezelési szabályzat mellékleteiként megfogalmazott adatkezelési tájékoztatók jól látható helyen, az adott épület hirdetőtábláján kifüggesztésre is kerültek. Az intézmény dolgozói kérésre kötelesek az adatkezelési tájékoztatókból az érintettnek másolatot adni.

2. lépés

Az érintett részére az adatkezelés megkezdése előtt a dolgozó rövid, tömör, érthető, hétköznapi nyelven megfogalmazott szóbeli tájékoztatást nyújt a VII. 4.1.1. pontban foglaltakról és meggyőződik arról, hogy az érintett az elmondottakat megértette. A szóbeli tájékoztatásnak ki kell térni arra is, hogy a szóbeli tájékoztatást írásos formában az érintett hol érheti el.

Az érintett jogairól, köztük a tiltakozáshoz való jogról külön is tájékoztatni kell.

3. lépés

Az érintett részére az adatkezelés megkezdése előtt át kell adni a megkezdeni kívánt adatkezelési tevékenységhez kapcsolódó adatkezelési tájékoztatót, melyet jelen belső adatvédelmi és adatbiztonsági szabályzat mellékletei tartalmaznak. Az érintettnek lehetőséget kell biztosítani, hogy tanulmányozza az adatkezelési tájékoztatót, melynek keretében kellő időt és az áttanulmányozáshoz szükséges nyugodt körülményeket biztosítunk.

Az adatkezelés megkezdése előtt, de a szóbeli tájékoztatás és az írásos tájékoztató átadása után az érintett részére át kell adni a jelen belső adatvédelmi és adatbiztonsági szabályzat 9. számú melléklete szerinti nyilatkozatot, amelyen az érintett aláírásával igazolja a szóbeli tájékoztatás megtörténtét és az írásbeli tájékoztató átvételét. Az 9. számú mellékleten a tájékoztatást megadó személy a kipontozott részen feltünteteti annak az adatkezelési tájékoztatónak a nevét, amelyet átadott az érintettnek tanulmányozásra és amelyet ismertetett.

4. lépés

Az érintettnek lehetőséget kell biztosítani arra, hogy az adatvédelmi tisztviselőhöz forduljon kérdéseivel, vele egyeztetést kezdeményezzen, így az érintettet tájékoztatni kell ezen lehetőségről és kérésére az adatvédelmi tisztviselővel történő személyes konzultációt meg kell szervezni.

5.2. AZ ÉRINTETT HOZZÁFÉRÉSI JOGA ÉS IRATBETEKINTÉSHEZ VALÓ JOG

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 veszélyeztettségének a jelen szabályzatban megfogalmazott esetét
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.
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.
4. Az érintett által benyújtott, a hozzáférési jogosultság érvényesítésére irányuló kérelmet a lehető legrövidebb időn belül, legfeljebb annak benyújtásától számított harminc napon belül bírálja el az intézmény és döntéséről az érintettet írásban vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti.
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.
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.
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.
 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.
 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.
A zárt borítékon feltüntetésre kerül az iktatószám és az érintett TAJ száma, mellyel az adott akcióval való kapcsolata megteremthető.
 10. 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.
 11. Az iratbetekintési jog gyakorlásához az intézmény a 10. számú melléklet szerinti formanyomtatványt bocsátja az érintett rendelkezésére, azonban az iratbetekintés iránti kérelem bármely formában előterjeszhető. Az intézmény az iratbetekintési kérelmet egyben személyes adatokhoz való hozzáféréshez való joggyakorlásnak is tekinti.

5.3. A HELYESBÍTÉSHEZ VALÓ JOG

1. A személyes adatokat pontosan kell rögzíteni a belső adatvédelmi és adatbiztonsági szabályzat VII.1.4. pontjában foglalt alapelv rendelkezéseinek megfelelően.
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.
3. Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat.
4. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok kiegészítését.
5. Az érintett által benyújtott, a helyesbítési jogosultság érvényesítésére irányuló kérelmet annak benyújtásától számított legrövidebb időn belül, legfeljebb harminc napon belül bírálja el az intézmény és döntéséről az érintettet írásban vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti.
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.
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.

5.4. A TÖRLÉSHEZ VALÓ JOG („AZ ELFELEDTETÉSHEZ VALÓ JOG”)

1. Az intézmény személyes adatokat a jogszabályban, valamint az adatkezelési tevékenységek nyilvántartásában megjelölt időtartamban kezeli.
2. Az időtartam lejártával a személyes adatokat az intézmény törli.
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;
 - e) a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
4. Nem alkalmazandó az érintett törléshez való joga, amennyiben az adatkezelés szükséges:
 - a) 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;
 - b) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.
5. A személyes adatok törlésére és iratok megsemmisítésére az iratkezelési szabályzat szerint van lehetőség azzal, hogy amennyiben az irat olyan személyes adatokat tartalmaz, melynek kezelésére az intézmény nem jogosult, akkor az iratot anonimizálni szükséges, amennyiben arra nincs mód, akkor a személyes adatot törölni, az adathordozót szükség szerint megsemmisíteni kell jegyzőkönyv felvétele mellett (26. szám alatti melléklet)
6. Az érintett által benyújtott, a törlési jogosultság érvényesítésére irányuló kérelmet annak benyújtásától számított legrövidebb időn belül, legfeljebb harminc napon belül bírálja el az intézmény és döntéséről az érintettet írásban vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti.
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.
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.

5.5. AZ ADATKEZELÉS KORLÁTOZÁSÁHOZ VALÓ JOG

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.
2. Az érintett által benyújtott, a korlátozási jogosultság érvényesítésére irányuló kérelmet annak benyújtásától számított legrövidebb időn belül, legfeljebb harminc napon belül bírálja el az intézmény és

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

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.
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.

5.6. A SZEMÉLYES ADATOK HELYESBÍTÉSÉHEZ VAGY TÖRLÉSÉHEZ, ILLETVE AZ ADATKEZELÉS KORLÁTOZÁSÁHOZ KAPCSOLÓDÓ ÉRTESÍTÉSI KÖTELEZETTSÉG

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.
2. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.
3. Azt, hogy mi minősül lehetetlennek, vagy aránytalanul nagy erőfeszítésnek az adatvédelmi tisztviselő állásfoglalása alapján az intézményvezető állapítja meg.

5.7. AZ ADATHORDOZHATÓSÁGHOZ VALÓ JOG

1. Az érintett által benyújtott, az adathordozhatósághoz való jogosultság érvényesítésére irányuló kérelmet annak benyújtásától számított legrövidebb időn belül, legfeljebb harminc napon belül bírálja el az intézmény és döntéséről az érintettet írásban vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti.
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.
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.
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.
5. Az adathordozhatósághoz kapcsolódó költségekről az intézmény, a kérelem teljesítése előtt tájékoztatást küld. A költségek minimum összege, 1.000.-Ft/személyes adat, de minimum 100.000.-Ft.

5.8. A TILTAKOZÁSHOZ VALÓ JOG

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.
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.

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.
4. Az érintett által benyújtott, a tiltakozáshoz való jogosultság érvényesítésére irányuló kérelmet annak benyújtásától számított legrövidebb időn belül, legfeljebb harminc napon belül bírálja el az intézmény és döntéséről az érintettet írásban vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti.
5. 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.
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.

6. AZ INTÉZMÉNNYEL FOGLALKOZTATÁSI JOGVISZONYBAN ÁLLÓ TERMÉSZETES SZEMÉLYEK ADATAINAK KEZELÉSE

6.1. ÁLTALÁNOS SZABÁLYOK

1. A munkavállalótól/foglalkoztatottól csak olyan adat közlése kérhető, amely személyiségi jogát nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges.
2. A jogviszony létesítésekor a munkavállaló átadja a szerződés megkötéséhez, kinevezéshez, illetve a munkáltató társadalombiztosítási bejelentési kötelezettsége teljesítése érdekében szükséges személyes adatait tartalmazó dokumentumokat, igazolványokat, melyeken található adatokról az intézmény munkatársa adatfelvételi lapot vesz fel. Amennyiben a bizonyítékul szolgáló okirat személyazonosításra alkalmas okmány, úgy annak valóságát a Magyarország által működtetett okmányok érvényességének ellenőrzésére szolgáló szolgáltatás igénybevételével ellenőrzi¹.
3. Az igazolványokról másolat nem készül.
4. A személyes adatok és az adatfelvételi lap a személyi nyilvántartásban kerülnek rögzítésre.
5. A hozzájáruláson alapuló adatkezelés esetén a munkavállaló írásbeli hozzájárulását be kell szerezni. A hozzájárulás szövegét a 12. számú melléklet tartalmazza.
6. A foglalkoztatási jogviszonyban álló érintett tájékoztatására megfelelően alkalmazni kell jelen szabályzatnak a VII.4.4.1. pontban foglalt rendelkezéseit is. A munkaviszonyban állók adatkezelési tájékoztatóját jelen szabályzat melléklete tartalmazza.
7. A foglalkoztatottnak a 13. számú melléklet szerinti nyilatkozatot kell aláírniuk a tájékoztatás megtörténtének igazolása érdekében.
8. A munkavállalók részére az intézmény – kérésre- 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.

6.2. MOBILTELEFON HASZNÁLATÁHOZ KAPCSOLÓDÓ ADATKEZELÉSI TEVÉKENYSÉG

1. Az adatkezelő a munkavállalók meghatározott csoportja részére **mobiltelefont** bocsát rendelkezésre, hogy a munkavállalók ezen keresztül tartsák egymással a kapcsolatot, vagy a munkáltató képviselőjében az ügyfelekkel, más személyekkel, szervezetekkel.
2. A telefonon folytatott beszélgetések rögzítésére, illetve a beszélgetésekbe történő belehallgatására nem kerül sor.
3. A munkáltató adatokat gyűjthet a kimenő és bejövő hívások idejéről, időtartamáról, a beszélgető partner telefonszámáról azaz híváslistát kérhet a szolgáltatótól a pénzügyi elszámolás megkönnyítése érdekében. A munkáltató nem gyűjt adatokat a telefon tartózkodási helyéről sem.
4. Az intézményi mobiltelefonokon csak olyan személyes adat tárolható, mely az intézményi munkavégzéshez kapcsolódik. A nem munkavégzéshez kapcsolódó személyes adatok tárolása tilos. Az eszköz ellenőrzésére az e-mail cím használta ellenőrzésének a szabályai megfelelően irányadóak.

6.3. AZ E-MAIL CÍM HASZNÁLATÁHOZ KAPCSOLÓDÓ ADATKEZELÉSI TEVÉKENYSÉG

1. Az adatkezelő a foglalkoztatottak meghatározott csoportja részére **e-mail címet** tart fenn, hogy a foglalkoztatottak ezen keresztül tartsák egymással a kapcsolatot, vagy az intézmény képviselőjében az ügyfelekkel, más személyekkel, szervezetekkel.

¹ <https://www.nyilvantarto.hu/ugyseged/OkmanyErvenyességLekerdezes.xhtml>

2. Az e-mail címet csak olyan szolgáltatón keresztül lehet fenntartani, amelynek szervei az Európai Unió területén vannak.
3. A foglalkoztatott rendelkezésére bocsátott e-mail fiók személyes levelezési célra nem használható.
4. Az e-mail fiókba történő belépési jelszó megváltoztatására az intézményvezető felhatalmazása alapján az informatikus jogosult.
5. Az e-mail fiók ellenőrzésére, a levelezés lementésére és tárolására az intézmény képviselőjében 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.
6. Az adatkezelő rögzíti, hogy nem kívánja megismerni és tárolni az e-mail címeken folytatott magánlevelezések tartalmát, így az ellenőrzés során az intézmény tudomására jutott személyes adatok kezelésére nem kerül sor, annak az intézményi levelezőrendszerből történő eltávolítására a foglalkoztatott kerül felhívásra. A kötelezettség elmulasztása esetén a személyes adat az e-mail fiókból törlésre kerül.
7. 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 elvülési időn belül megindítja.

6.4. A SZÁMÍTÓGÉPEK HASZNÁLATÁHOZ KAPCSOLÓDÓ ADATKEZELÉSI TEVÉKENYSÉG

1. Az adatkezelő a foglalkoztatottak meghatározott csoportja részére **számítógépet** (beleértve lap top, táblagép, notebook, ipad, pen drive stb.) és **okos telefont** tart fenn.
2. A foglalkoztatott rendelkezésére bocsátott eszközök személyes célra nem használhatóak.
3. A belépési jelszó megváltoztatására az intézményvezető felhatalmazása alapján az informatikus jogosult. A jelszavakat 3 havonta kötelező megváltoztatni.
4. Az eszközök ellenőrzésére, a rajta lévő személyes adatok lementésére és tárolására az intézmény képviselőjében 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.
5. Az adatkezelő rögzíti, hogy nem kívánja megismerni és tárolni az eszközökön tárolt személyes adatokat, így az ellenőrzés során az intézmény tudomására jutott személyes adatok kezelésére nem kerül sor, annak az intézményi eszközökről történő eltávolítására a foglalkoztatott kerül felhívásra.
6. 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 segítségével igénybe vehető a törlés elvégzéséhez. A kötelezettség elmulasztása esetén a személyes adat az eszközökről törlésre kerül.
7. 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 elvülési időn belül megindítja.

6.5. AZ INTÉZMÉNYHEZ MUNKÁRA JELENTKEZŐK SZEMÉLYES ADATAIHOZ KAPCSOLÓDÓ ADATKEZELÉSI TEVÉKENYSÉG

6.5.1. ÁLTALÁNOS SZABÁLYOK

1. Az adatkezelő elkötelezett tevékenységének fejlesztése iránt, így a munkafolyamatokat a feladat ellátására legalkalmasabb munkavállalókkal kívánja elvégeztetni. A pályázati eljárás keretében az adatkezelő személyes adatokat kezel.

2. Az adatkezelési tájékoztató elérhetőségét a pályázati felhívásban rögzíteni kell.
3. Az anonimizált álláshirdetések közzététele tilos. A betöltendő álláshelyek esetében az adatkezelő, mint jövőbeni foglalkoztató nevét fel kell tüntetni.
4. Az adatkezelőhöz megérkező pályázatokat a pályázat benyújtására nyitva álló idő elteltéig a HR munkatárs zárható szekrényben a pályázattal nem érintettek személyes adataitól elkülönülten tárolja, továbbá a pályázati anyagokat elektronikus formába átalakítja és a szerveren kizárólagos hozzáférésű mappába lementi. Az elektronikus fájlok az intézményvezető és a leendő munkáltatói jogkör gyakorlója elektronikus levél címére megküldésre kerül.
5. Az adatkezelőhöz megérkező pályázatokat a pályázat benyújtására nyitva álló idő elteltét követő 30. napig a HR munkatárs, az intézményvezető és a leendő munkáltatói jogkör gyakorló áttekinti. A pályázati anyagokról feljegyzések, az érintettől levont következtetések nem készülnek.
6. A kiválasztás lezárását követően az intézményvezető és a leendő munkáltatói jogkör gyakorlója a személyes adatokat tartalmazó elektronikus fájlt a levelezési rendszeréből a kiválasztási folyamat lezárását követő 1 munkanapon belül törli.
7. A kiválasztás lezárását követően a HR munkatárs a ki nem választott pályázókat 30 napon belül értesíti, mely értesítési napot követő 60. napon a pályázati anyagokat meg kell semmisíteni, az elektronikus fájlokat törölni kell oly módon, hogy azok ne legyenek helyreállíthatóak. A ki nem választott pályázók részére a 14. melléklet szerinti értesítést kell megküldeni.
8. Megőrzésre kerülnek 365 napra a sikertelen pályázatok a pályázó erre irányuló kérelme esetén az adatkezelési tevékenységek nyilvántartásában megjelölt célból. A sikertelen pályázatról szóló 10/A. melléklete szerint értesítés mellett meg kell küldeni a pályázóknak a 15. számú kérelmet is.
9. A pályázók részére szóló adatvédelmi tájékoztatót a 25. számú melléklet tartalmazza, melyet a pályázóknak a pályázat elküldése előtt elérhetővé kell tenni.

6.5.2. AZ INTÉZMÉNYHEZ MUNKÁRA JELENTKEZŐK KÖZÖSSÉGI PROFILJÁNAK MEGTEKINTÉSE

1. A betöltendő álláshelyre jelentkezőket előzetesen a pályázat benyújtását megelőzően tájékoztatni kell, amennyiben az intézmény a jelentkező nyilvános közösségi profilját ellenőrizni kívánja. Főszabály szerint a közösségi profil ellenőrzésére nem kerül sor.
2. Az intézmény nem tekinti meg azokat az adatokat, melyet ugyan nyilvánosságra hozott a jelentkező, de a jogviszony létesítéséhez nem szükséges, így különösen a fajra, nemzetiségre, családi állapotra, gyermekek számára, szexuális hovatartozásra, szakszervezethez, politikai szervezethez tartozáshoz kapcsolódó adatokat.
3. Tilos létrehozni közösségi oldalon álprofil, illetve a jelentkező által a nem mindenki számára nyilvánossá tett adatainak a megismerése érdekében bármilyen intézkedést tenni.

6.6. AZ INTÉZMÉNNYEL JOGVISZONYBAN ÁLLÓ TERMÉSZETES SZEMÉLYEK ALKALMASSÁGI VIZSGÁLATAIVAL KAPCSOLATOS ADATOK KEZELÉSE

1. A foglalkoztatottal szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet a jogviszonyra vonatkozó szabály ír elő, vagy amely a jogviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.
2. A fizikai munkakörben dolgozó munkavállalók egészségügyi orvosi vizsgálaton vesznek részt.
3. A „nem alkalmas” vagy „feltételekkel alkalmas” foglalkoztatottak esetében kizárólag az orvosi igazolás kerül nyilvántartásba. Az eredményeket a vizsgált foglalkoztatottak, illetve a vizsgálatot végző szakember ismerhetik meg. Az intézmény csak azt az információt kaphatja meg, hogy a vizsgált személy a munkára alkalmas-e vagy sem, illetve milyen feltételek biztosítandók ehhez. A vizsgálat részleteit, illetve annak teljes dokumentációját azonban nem ismerheti meg.

4. A foglalkoztatottakkal pszichológiai vagy személyiségjegyeket kutató tesztlapok kitöltethetők, amennyiben arra egyértelműen munkaviszonnyal kapcsolatos, a munkafolyamatok hatékonyabb ellátása, megszervezése érdekében kerül sor amennyiben az elemzés során felszínre került adatok nem köthetők az egyes konkrét munkavállalókhoz, vagyis anonim módon történik az adatok feldolgozása.
5. A tréningeken, csapatépítéseken a különböző alkalmassági vizsgálatok keretén belül elvégzett személyiségtesztek megismerésére, tárolására, nyilvántartására nem kerül sor.

6.7. AZ INTÉZMÉNNYEL FOGLALKOZTATÁSI JOGVISZONYBAN ÁLLÓ TERMÉSZETES SZEMÉLYEK FÉNYKÉPEINEK KEZELÉSE

1. A foglalkoztatottakról készített fényképek kezelésére sor kerül.
2. Az intézmény által szervezett programokon történő részvétel során a foglalkoztatottak dönthetnek arról, hogy a programról készített felvételen jelen kívának-e lenni. Részvételük esetén „Az ellátottakról készített fénykép és videofelvétel készítése” adatkezelési tevékenység adatkezelési tájékoztatót megfelelően alkalmazzuk.

6.8. SZOCIÁLIS ALAP-, MESTER-, ÉS SZAKKÉPZÉSBEN RÉSZTVEVŐ HALLGATÓK FOGADÁSA /TEREPGYAKORLAT BIZTOSÍTÁSA/

1. Az intézmény elkötelezett a szociális területen dolgozni kívánó hallgatók gyakorlati képzése iránt.
2. A hallgatók foglalkoztatására együttműködési megállapodás alapján kerül sor. Az adatkezelés megkezdése előtt az érintett tájékoztatására megfelelően alkalmazni kell jelen szabályzatnak a VII.4.4.1. pontban foglalt rendelkezéseit is.
3. Az adatkezelési tájékoztatót a 25. számú melléklet tartalmazza.

7. COOKIE-K ALKALMAZÁSA ÉS KÖZÖSSÉGI OLDALON PROFIL FENNTARTÁSA

1. Az intézmény a honlapot meglátogató felhasználó számítógépén adatsomagot (ún. „cookie”-t) nem helyez el.
2. Az intézmény közösségi oldalon hivatalos 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.
3. Az intézmény a közösségi profilt az ügyfelek gyors és közvetlen tájékoztatására használja, konkrét ügyre vonatkozó, személyes adatot tartalmazó üzenetváltásra nem kerül sor.
4. A közösségi oldalon létrehozott intézményi profilt az intézmény hivatalos e-mail címével kell regisztrálni, az oldalhoz hozzáférést biztosító jelszót és felhasználónevet az intézményvezető őrzi.

8. GÉSA SZOFTVER ALKALMAZÁSA

1. Az intézmény a bentlakók adataira és ápolási- illetve gyógyszerelési igényeik tárolása céljából Gondozást Segítő Alkalmazást tart fenn. A szoftverben személyes és egészségügyi adatok is tárolásra kerülnek.
2. A szoftver az e-mailekhez hasonlóan a Gizella Otthon saját Microsoft Azure platformján, biztonságosan kerül tárolásra.
3. A szoftverben az adatokhoz való hozzáférés korlátozott, az egyes munkakörökben dolgozók csak a mindennapi munkához elengedhetetlenül szükséges információhoz jutnak hozzá, illetve indokolt esetben tudják azt szerkeszteni. Az alábbi munkakörök különülnek el:
 - Adminisztrátor
 - Főnövér
 - Gyógyszerelő
 - Ápoló
 - Orvos
 - Mentálhigiénés szakember
 - Recepció

- Gazdasági munkatárs
4. A szoftverhez való hozzáférés módja, a belépési adatok és a jelszó kezelése megegyezik az e-mail címekhez valós hozzáférés módjával.

9. SZÁMÍTÓGÉP MEGOSZTOTT ADATTARTALMA

1. Az adatkezelő alkalmazhatja a számítógép megosztás technikai megoldását, melynek célja, hogy egy könyvtárba mentve az adott szakmai egység dolgozói valamennyi adatot elérjék a munkájukhoz szükséges mértékben saját számítógépükről.
2. A dolgozók kötelesek a megosztott könyvtárat használni, amennyiben az adott szakmai egységnél ez kialakításra került.

10. AZ INTÉZMÉNYI TEVÉKENYSÉGGEL KAPCSOLATOS ADATKEZELÉSI ELŐÍRÁSOK

1. Az intézmény dolgozói a feladataik teljesítése során a jogszabályok, a szakmai protokoll és az intézményi szabályzatok előírásait betartva kötelesek eljárni.
2. Az intézménnyel kapcsolatba kerülő ügyfelet azonosítani szükséges. Az azonosítás a személyi igazolvány, a lakcímkártya és a TAJ kártya elkérésével és megtekintésével valósul meg.
3. A dolgozók részére az intézmény által kiállított igazolványt - az ügyféllel történő első kapcsolatfelvétel alkalmával, illetve amikor az ügyfél kéri - be kell mutatni.
4. A személyazonosítására szolgáló igazolványok, egyéb iratok, dokumentumok másolására csak az adatkezelési tevékenységek nyilvántartásában megjelölt tevékenységeknél az ott megjelölt célból és alapon van lehetőség.
5. A Magyar Államkincstár központi szerve (a továbbiakban: Központ) a szociális, gyermekjóléti és gyermekvédelmi szolgáltatók, intézmények és hálózatok hatósági nyilvántartásának (a továbbiakban: szolgáltatói nyilvántartás) adatai alapján, egységes adatbázisban vezeti
 - a) a szociális igazgatásról és szociális ellátásokról szóló 1993. évi III. törvény (a továbbiakban: Szt.) 20/C. §-a szerinti, a személyes gondoskodást nyújtó szociális ellátások, szolgáltatások finanszírozásának ellenőrzése céljából, valamint a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény (a továbbiakban: Gyvt.) 139. § (2) bekezdése szerinti, a személyes gondoskodást nyújtó gyermekjóléti alapellátások és gyermekvédelmi szakellátások finanszírozásának ellenőrzése céljából vezetett nyilvántartást (a továbbiakban együtt: igénybevevői nyilvántartás),
 - b) az Szt. 20/B. §-a és a Gyvt. 141/A. §-a szerinti országos jelentési rendszert és
 - c) az Szt. 20. § (2a) bekezdése szerinti adatszolgáltatás rendszerét²
6. Az adatszolgáltatás teljesítésére belépési jogosultsággal rendelkező személyt jelölt ki a fenntartó (a továbbiakban: e-képviselő). Az adatszolgáltatás teljesítésére az e-képviselő - az engedélyes vagy a fenntartó munkatársai közül - belépési jogosultsággal rendelkező személyt vagy személyeket köteles kijelölni (a továbbiakban: adatszolgáltató munkatárs). Az adatszolgáltató munkatárs a nyilvántartások informatikai rendszerében jelölhető ki. A kijelöléshez meg kell adni az adatszolgáltató munkatárs ügyfélkapu használatára jogosító személyazonosító adatait, és meg kell jelölni azokat az engedélyeseket, amelyek tekintetében az adatszolgáltató munkatárs adatszolgáltatásra jogosult. Csak olyan munkatárs jelölhető ki, aki a feladat teljesítését és az ügyfélkapu adatok szolgáltatását önként vállalja.
7. Az intézmény nyilvántartásba veszi a szolgáltatásra vonatkozó igényeket, melyeket az ügyfelek (az intézmény munkatársának segítségével) fogalmaznak meg. Az adatszolgáltatás a jogszabályban meghatározott határidőn belül kerül sor.

² a szociális, gyermekjóléti és gyermekvédelmi igénybevevői nyilvántartásról és az országos jelentési rendszerről 415/2015. (XII. 23.) Korm. rendelet 1.§

8. Az adatkezelés megkezdése előtt a VII.4.4.1. pontban foglalt tájékoztatási szabályokat alkalmazzuk. Az általános adatkezelési tájékoztatót a jelen szabályzat mellékletei tartalmazzák.
9. A szolgáltatást igénybe vevőket illeti személyes adatainak védelme, valamint a magánéletükkel kapcsolatos titokvédelem. Az igénybevételi eljárás során különös figyelmet kell fordítani arra, hogy az ellátást igénylő adataihoz csak az arra jogosult személyek férjenek hozzá.

11. CÉGKAPU MŰKÖDTETÉSÉHEZ KAPCSOLÓDÓ ADATKEZELÉSI RENDELKEZÉSEK

1. Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (továbbiakban: E-ügyintézési tv.) 9. § (1) bekezdés a) pont aa) alpontja értelmében a gazdálkodó szervezet elektronikus ügyintézésre kötelezett.
2. A polgári perrendtartásról szóló 2016. évi CXXX. törvény 7. § 6. pontja értelmében az alapítványok gazdálkodó tevékenységükkel összefüggő polgári jogi kapcsolataik vonatkozásában gazdálkodó szervezetnek minősülnek. Erre figyelemmel az alapítvány az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet (továbbiakban: Vhr.) 89. § (1) bekezdése értelmében cégkapu használatára jogosult.
3. A Cégkapu egy elektronikus postafiók a gazdálkodó szervezetek számára, ahol minden érintett és arra jogosultsággal rendelkező személy egy helyen férhet hozzá az adott cég vagy szervezet hivatalos levelezéséhez. A Cégkapuban az adminisztrációt végző cégkapumegbízott a rendszer segítségével megadhatja, hogy a cégből kik azok, akik dokumentumokat küldhetnek és fogadhatnak.
4. A Cégkapu regisztráció megtehető a szervezet törvényes képviselője, vagy annak meghatalmazottja által is. A Cégkapu kezelésére a későbbiekben az adott gazdálkodó szervezetnél az erre felhatalmazott természetes személy (a továbbiakban: Cégkapumegbízott) vagy az általa regisztrált, a gazdálkodó szervezet által megbízott további felhasználók jogosultak (a továbbiakban: Ügykezelők).
5. A regisztrációt végző személy, mind a cégkapu-megbízott számára előfeltétel, hogy az állam által kötelezően nyújtott azonosítási szolgáltatás útján (Ügyfélkapu, Részleges kódú telefonos azonosítás, Elektronikus személyazonosító igazolvány) azonosítsa magát.
6. Az intézménynél cégkapumegbízott csak az intézménnyel munkaviszonyban álló személy lehet. A cégkapumegbízott nem kötelezhető az állam által kötelezően nyújtott azonosítási szolgáltatás azonosító adatainak az intézmény részére történő átadására.

12. ADOMÁNYOSZTÁS

1. Az intézménnyel kapcsolatba kerülő elláttal – amennyiben az adományokra jogosultság és az igény felmerül – hozzájáruló nyilatkozatot kell aláíratni, hogy az adományozható személyek nyilvántartásába felvételre kerülhessen.
2. Az intézmény az adományozható személyekről nyilvántartást vezet. A nyilvántartás tartalmazza az érintett nevét és elérhetőségi adatait és a rászorultság körét. A nyilvántartás adatait zártan kell kezelni.
3. A nyilvántartásból adat az adatkezelési tevékenységek nyilvántartásában megjelölt célból továbbítható harmadik személy részére.

13. EGÉSZSÉGÜGYI SZOLGÁLTATÁSOKHOZ KAPCSOLÓDÓ KIEGÉSZÍTŐ ADATKEZELÉSI SZABÁLYOK

1. Az intézmény Belső adatvédelmi és adatbiztonsági szabályzatában foglalt rendelkezéseket a jelen fejezetben foglaltakra is figyelemmel kell megfelelően alkalmazni.
2. Az adatkezelés tárgyát képező személyes adatok minden további másolatért miniszteri rendeletben meghatározott költségelemek alapján kell díjat fizetni. Az adatokhoz való hozzáféréshez való jogot az érintett ellátásának időtartama alatt az általa írásban felhatalmazott személy, az érintett ellátásának befejezését követően az általa teljes bizonyító erejű magánokiratban felhatalmazott személy jogosult.

14. ADATTOVÁBBÍTÁS

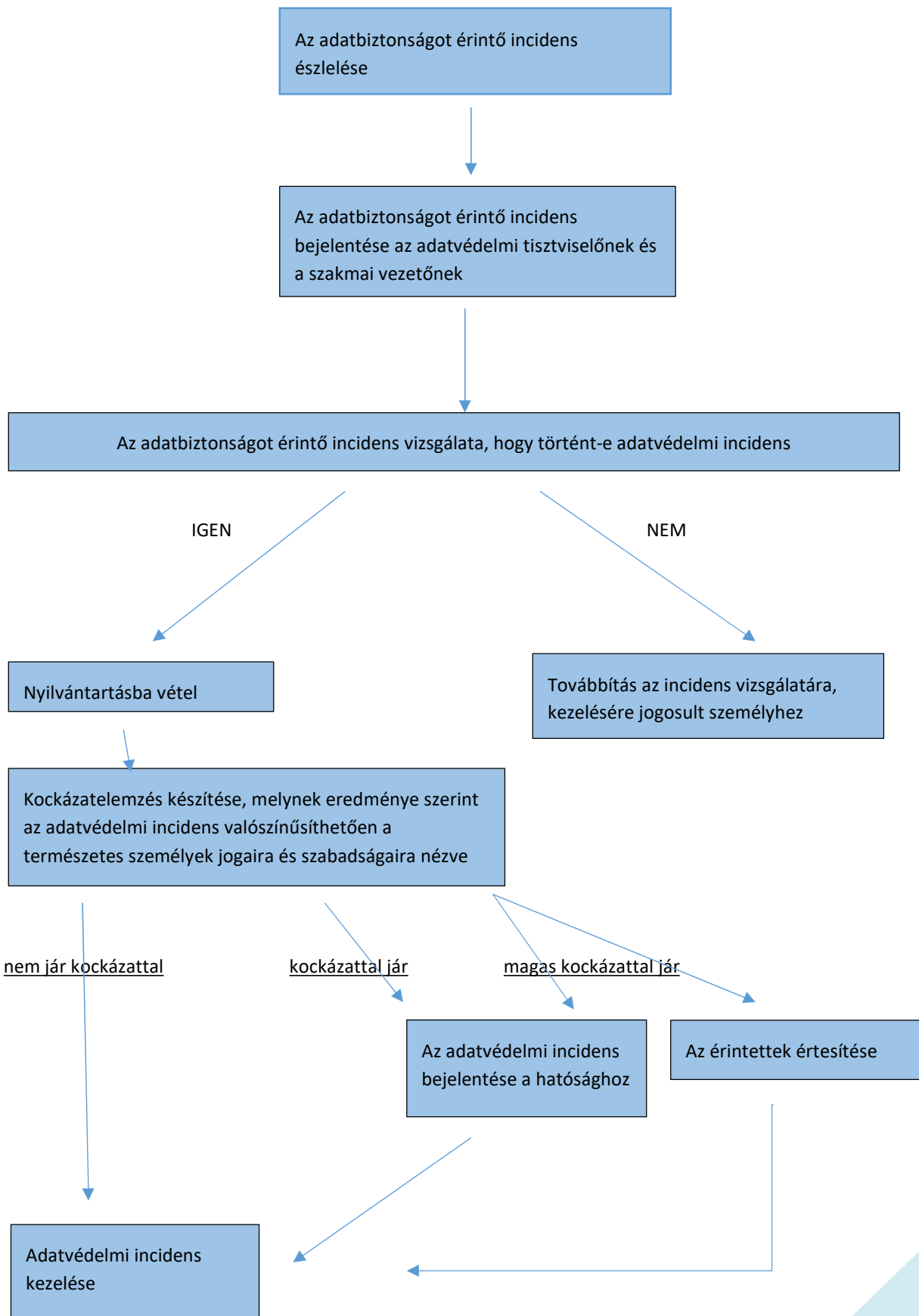
1. Az adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.
2. Az adattovábbítást megelőzően a szakmai vezető megvizsgálja a továbbítandó személyes adatok pontosságát, teljességét és naprakészségét.
3. Ha a vizsgálat eredményeként a szakmai vezető azt állapítja meg, hogy a továbbítandó adatok pontatlanok, hiányosak vagy már nem naprakészek, azokat kizárólag abban az esetben továbbíthatja, ha
 - a) az az adattovábbítás céljának megvalósulásához elengedhetetlenül szükséges, és
 - b) az adattovábbítással egyidejűleg tájékoztatja a címzettet az adatok pontosságával, teljességével és naprakészségével összefüggésben rendelkezésre álló információkról és
 - c) az adatvédelmi tisztviselő az adattovábbítás teljesíthetőségével egyetértett.

16. 1. MAGYAR ÁLLAMKINCSTÁR FELÉ TÖRTÉNŐ ADATTOVÁBBÍTÁS

1. A Magyar Államkincstár központi szerve (a továbbiakban: Központ) a szociális, gyermekjóléti és gyermekvédelmi szolgáltatók, intézmények és hálózatok hatósági nyilvántartásának (a továbbiakban: szolgáltatói nyilvántartás) adatai alapján, egységes adatbázisban vezeti
 - a) a szociális igazgatásról és szociális ellátásokról szóló 1993. évi III. törvény (a továbbiakban: Szt.) 20/C. §-a szerinti, a személyes gondoskodást nyújtó szociális ellátások, szolgáltatások finanszírozásának ellenőrzése céljából, valamint a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény (a továbbiakban: Gyvt.) 139. § (2) bekezdése szerinti, a személyes gondoskodást nyújtó gyermekjóléti alapellátások és gyermekvédelmi szakellátások finanszírozásának ellenőrzése céljából vezetett nyilvántartást (a továbbiakban együtt: igénybevevői nyilvántartás),
 - b) az Szt. 20/B. §-a és a Gyvt. 141/A. §-a szerinti országos jelentési rendszert és
 - c) az Szt. 20. § (2a) bekezdése szerinti adatszolgáltatás rendszerét
2. Az adatszolgáltatás teljesítésére ügyfélkapu belépési jogosultsággal rendelkező személyt jelölt ki a fenntartó (a továbbiakban: e-képviselő). Az adatszolgáltatás teljesítésére az e-képviselő - az engedélyes vagy a fenntartó munkatársai közül - ügyfélkapu belépési jogosultsággal rendelkező személyt vagy személyeket köteles kijelölni (a továbbiakban: adatszolgáltató munkatárs). Az adatszolgáltató munkatárs a nyilvántartások informatikai rendszerében jelölhető ki. A kijelöléshez meg kell adni az adatszolgáltató munkatárs ügyfélkapu használatára jogosító személyazonosító adatait, és meg kell jelölni azokat az engedélyeseket, amelyek tekintetében az adatszolgáltató munkatárs adatszolgáltatásra jogosult. Csak olyan munkatárs jelölhető ki, aki a feladat teljesítését és az ügyfélkapu adatok szolgáltatását önként vállalja.
3. Az intézmény nyilvántartásba veszi a szolgáltatásra vonatkozó igényeket, melyeket az ügyfelek (az intézmény munkatársának segítségével) fogalmazznak meg. Az adatszolgáltatás a jogszabályban meghatározott határidőn belül kerül sor.

VIII. Az adatvédelmi incidens és kezelése

1. AZ ADATVÉDELMI INCIDENS KEZELÉSÉNEK FOLYAMATÁBRÁJA



2. AZ ADATVÉDELMI INCIDENS ÉSZLELÉSE

1. Az a foglalkoztatott, 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 a közvetlen vezetője útján haladéktalanul az adatvédelmi tisztviselőnek 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.
2. Amennyiben az adatvédelmi incidens informatikai rendszert érintően következett be, akkor az adatvédelmi tisztviselő tájékoztatja az informatikai rendszert felügyelő személyt.
3. Az adatvédelmi tisztviselő - 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.
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
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

1. Az adatvédelmi incidenst az adatvédelmi tisztviselő 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-incidensbejelent--rendszer.html>), kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Az ENISA módszertani útmutatójának alkalmazásával megállapított alacsony és közepes kockázatot úgy tekintjük, hogy az nem jár a természetes személyek jogaira és szabadságaira nézve kockázattal a GDPR szempontjából, így azt bejelenteni nem szükséges.
Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.
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.
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 kockázatoság megállapításához az intézmény az Európai Unió 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. A kockázátértékelés eredményeként megállapított alacsony, közepes, magas, nagyon magas kockázat nem az adatvédelmi hatósághoz történő bejelentés körében értékelendő kockázat szintjét állapítja meg, hanem az iránymutatás az intézménynek az érintett jogaira és szabadságaira nézve megállapítható kockázat tekintetében.

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:

$$SE = DPC \times EI + CB$$

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.).
$2 \leq SE < 3$	közepes kockázat	Az egyének jelentős nehézségeket tapasztalhatnak, amelyeket képesek lesznek leküzdni (többletköltségek, szolgáltatásokhoz való hozzáférés megtagadása, félelem, megértés hiánya, stressz, stb.).
$3 \leq SE < 4$	magas kockázat	Az egyének jelentős következményekkel is szembesülhetnek (feketelistázás, vagyoni kár, munkahely elvesztése, egészségromlás stb.).
$4 \leq SE$	nagyon magas kockázat	Az egyének jelentős vagy akár visszafordíthatatlan következményekkel is szembesülhetnek, amelyeket nem lehet, vagy számottevő nehézség árán lehet leküzdni (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		Pontszám
	életrajzi adatok, elérhetőségek, teljes név, adatok az oktatásról, a családi életről, a szakmai tapasztalatról	
	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		Pontszám
	hely, forgalmi adatok, személyes preferenciákkal és szokásokkal kapcsolatos adatok	
	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		Pontszám
	Bármilyen típusú pénzügyi adatok (például jövedelem, pénzügyi tranzakciók, bankszámlakivonatok, befektetések, hitelkártyák, számlák stb.). Tartalmazza a pénzügyi információkhoz kapcsolódó szociális jóléti adatokat.	
	Előzetes alapérték: Amikor a jogsértés "pénzügyi adatokat" érint és az adatkezelő nem ismer súlyosító vagy enyhítő tényezőket.	3
	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 fentiekől 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 fentiekől 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

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)

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

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

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 rosszhiszemű jogsértések magukban foglalják az érintettek károsítását célzó lopás és hackelés eseteit.

+ 0,5	A rosszhiszemű szándékosság megállapítható
-------	--------------------------------------------

4. ADATVÉDELMI INCIDENSEK NYILVÁNTARTÁSA

Az adatvédelmi incidensről az adatvédelmi tisztviselő a 4. sz. melléklet szerinti adattartalommal nyilvántartást vezet. A nyilvántartásba történő bejegyzésről az adatvédelmi tisztviselő értesítést küld az intézményvezetőnek.

IX. 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

Bizalmasság elve

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

Sértetlenség elve

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

Rendelkezésre állás elve

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

2. AZ ADATBIZTONSÁGI ELLENŐRZÉS

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. Az adatbiztonsági ellenőrzést az adatvédelmi tisztviselő vezeti. Az ellenőrzésről jegyzőkönyv felvételére kerül sor. A jegyzőkönyvmintát a 5. számú melléklet tartalmazza. A jegyzőkönyvet az ellenőrzés során jelen lévő személyek aláírásukkal látják el. A jegyzőkönyv alapján az adatvédelmi tisztviselő értékelést és intézkedési tervet készít, melyet átad az intézményvezetőnek.
3. Az adatbiztonsági ellenőrzés folyamata:
 - I. A védelmi igény feltárása: ki kell választani az intézmény lényeges adatkezeléssel érintett rendszereit, amelyeket az intézmény védeni akar.
 - II. Fenyegetettség-elemzés: azoknak a fenyegető tényezőknek a feltárása, amelyek az előbbi adatokra, alkalmazásokra veszélyesek lehetnek.
 - III. Kockázatelemzés: a fenyegető tényezők hatását kell megvizsgálni az informatikai rendszerre, meghatározni a lehetséges károk bekövetkezésének gyakoriságát és a kárértékeket.
 - IV. Kockázatkezelés: a megfelelő intézkedések kiválasztása és értékelése a károk csökkentésére.

2.1. A VÉDELMI IGÉNY FELTÁRÁSA

1. Az intézményi adatkezelés védelme három összetevőjű, áll fizikai védelemből, eljárásvédelemből és informatikai védelemből.
2. A fizikai védelem a helyiségek, objektumok védelméből, valamint a papír alapú és más hagyományos dokumentumok védelméből áll.
3. Az eljárásvédelem az adatvédelmi és adatbiztonsági szabályok meghatározása, betartása és betartásának ellenőrzését, az intézményi dolgozók tudatosságának fejlesztését foglalja magában.
4. Az informatikai védelem a hardver és szoftvervédelemből áll.

2.2. FENYEGETETTSÉG-ELEMZÉS

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.
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).

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.

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).

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.

A szoftverekhez kapcsolódó veszélyforrások:

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

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.

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.

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 képzettség vagy külső ráhatás következményeként;
- d) jogosulatlan hozzáférés;
- e) az ellenőrzés hiánya

2.3. KOCKÁZATELEMZÉS

1. A 2.1. és a 2.2. pontokban meghatározott tényezők összevetése és a tudomány mindenkori állásának megfelelő előfordulásának meghatározása.
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, vihkár)
 - c. reális előfordulási lehetőség (pl. betörés, vírusfertőzés)
 - d. minden bizonnyal be fog következni (pl. téves adatfelvétel)
3. Az adatbiztonság ellenőrzési jegyzőkönyvben meghatározott fenyegető tényezőket értékelni kell a 2. pont szerinti besorolás szerint. A kockázat értékelésére külső szakember igénybe vehető, az informatikai szempontú kockázatok értékelését az intézmény informatikusa végzi.

2.4. 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. A szervezeti integritását sértő események kezelésének eljárásrendjére vonatkozó szabályzat rendelkezéseit a kockázatok kezelésére megfelelően alkalmazni kell.

3. ADATBIZTONSÁGI ELŐÍRÁSOK ÉS ELJÁRÁSI SZABÁLYOK

3.1. BELÉPTETÉS ÉS ELEKTRONIKUS MEGFIGYELÉSI RENDSZER

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 25. számú melléklet tartalmazza.
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 16. számú melléklet szerinti tartalommal kerül felvételre.
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. Az intézmény nem végezhet megfigyelést olyan helyiségekben, ahol ez az emberi méltóságot sértheti, illetve olyan helyiségben sem, ahol a munkavállaló a munkaközi szünetét tölti.
5. Az érintettek az intézmény területére történő belépéssel elismerik és tudomásul veszik a kamerás megfigyelés tényét. A megfigyelő rendszer létéről és működéséről a kötelezettségének megfelelően az intézmény figyelemfelhívó jelzést helyez el arról, hogy az adott területen elektronikus megfigyelőrendszert alkalmaz. A figyelemfelhívó jelzés mellett a 25. számú melléklet szerinti adatvédelmi tájékoztatót is ki kell helyezni.

6. Az, akinek jogát vagy jogos érdekét a képfelvétel rögzítése érinti, a képfelvétel rögzítésétől számított tíz munkanapon belül jogának vagy jogos érdekének igazolásával kérheti, hogy az adatot az Intézmény ne semmisítse meg, illetve ne törölje.
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.
8. Az intézményvezető a 3.1. pont 7. alpont szerinti feladatkörét delegálhatja telephelyvezető vagy más munkavállaló, vagy az intézménnyel adatfeldolgozói szerződést kötő harmadik személy részére.
9. Bíróság vagy más hatóság megkeresésére a rögzített képfelvételt, valamint más személyes adatot a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni.
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.
11. A tájékoztatás és a rögzítés kérése ingyenes.
12. Az adatok tárolására a kameraszerveren kerül sor.

3.2. IRATOK TÁROLÁSA, HELYISÉGEK ŐRZÉSE

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, ügyintézésé céljából.
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.
3. Az iratok tárolására szolgáló helyiségben csak az intézményvezető által kijelölt személyek tartózkodhatnak. Ezen személyekről az intézményvezető listát vezet a 18. számú 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. 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.
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.
6. Az iratok elzárását lehetővé tevő szekrények és irodák kulcsairól listát kell vezetni a 17. számú melléklet szerinti tartalommal. A kulcshasználat külön szabályzatban került rendezésre.
7. A belső adatvédelmi és adatbiztonsági szabályzat VII.4.2. szerinti zártan kezelendő személyes adatok lezárt borítékban, széfben kerülnek tárolásra, melyhez kizárólag az intézményvezető, illetve az általa feljogosított személynek van hozzáférése. A széf méretének olyannak kell lennie, hogy az két ember erejével ne legyen megmozdítható. A széfet a falhoz és a padlóhoz is rögzíteni kell. Törekedni kell a tűzbiztosságára.

8. 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.

3.3. INFORMATIKAI BIZTONSÁGI ELŐÍRÁSOK

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.
2. A szervert és az informatikai rendszerek ellenőrzését és karbantartását meg kell szervezni, szünetmentes áramforrást kell biztosítani, érintésvédelmi és villámvédelmi szabályzatot kell létrehozni.
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 21. számú melléklet tartalmazza. A teljesítési igazolást át kell adni a mentés után haladéktalanul az intézményvezetőnek, aki azt őrizni köteles.
4. A személyes adatokhoz az adatkezelési tevékenységek nyilvántartása szerinti rögzített személyek férhetnek hozzá, a munkaköri leírásokban történő külön rögzítés mellett.
5. Az informatikai rendszereket jelszóval kell védeni. A jelszavakat tartalmazó adattáblát a 19. számú melléklet szerinti tartalommal kell elkészíteni. A jelszavak megváltoztatására csak az intézményvezető jogosult. A jelszavakat az adott felhasználó harmadik személynek nem adhatja ki.
6. Hálózati tűzfalak, hálózati forgalom szűrése és korlátozása, hálózaton terjedő vírusok és kémprogramok ellen védelmet kell kialakítani.
7. Számítógépes programok letöltésére csak az intézményvezető, illetve az informatikai rendszereket ellenőrző személy jogosult.
8. Az intézményi eszközöket idegen adathordozókhoz (pl. pendrive) csatlakoztatni tilos.
9. Az informatikai biztonsági szabályzat további informatikai biztonsági szabályokat fogalmazhat meg.

3.4. OKTATÁS

1. Az adatvédelemmel, adatbiztonsággal kapcsolatos jogokról és kötelezettségekről oktatást, előadást kell a foglalkoztatottak részére szervezni szükség szerint, de évente legalább egy alkalommal.
2. Minden újonnan belépő munkavállaló részére az oktatást meg kell szervezni.
3. A foglalkoztatott az oktatás megtörténtét aláírásával igazolja. A foglalkoztatotti nyilatkozat a személyi nyilvántartás része.
4. A jelen szabályzat 20. számú melléklete tartalmazza az oktatás megtörténtének igazolására alkalmazandó nyomtatványt.
5. Az oktatás anyagát az adatvédelmi tisztviselő állítja össze.
6. Az oktatás megszervezésében az intézményvezető segítséget nyújt az adatvédelmi tisztviselőnek.
7. Az oktatás megtartását követően a tudásszint felmérésére ellenőrző teszt alkalmazható.

1. SZÁMÚ MELLÉKLET – A BELSŐ ADATVÉDELMI ÉS Adatbiztonsági szabályzat megismerésének a jegyzéke

Jelen nyilatkozat aláírásával kijelentem, hogy az intézmény Belső adatvédelmi és adatbiztonsági szabályzatát a mai napon megismertem:

Sorszám	Név	Beosztás	Megismerés dátuma	Aláírás

2. SZÁMÚ MELLÉKLET - ELLENŐRZÉSI NYOMVONAL

Sorszám	Folyamat lépései	Jogszabály, belső szabályozás	Előkészítés	Keletkezett dokumentum	Feladatgazda	Határidő	Ellenőrzés	Utalvány ellenjegyzés	Pénzügyi teljesítés	Elszámolás
1.	Érintetti joggyakorlás iránti kérelem átvétele	Belső adatvédelmi és adatbiztonsági szabályzat, GDPR	Szakmai vezető kijelöli az átvételnél közreműködő foglalkoztatottat és sor kerül az átvételre	Érintetti joggyakorlás iránti iktatott kérelem	Szakmai vezető	Egyedileg meghatározott	Intézmény vezető	né	né	né
2.	Érintetti joggyakorlás iránti kérelem vizsgálata	Belső adatvédelmi és adatbiztonsági szabályzat, GDPR	Szakmai vezető által kijelölt foglalkoztatottat és az adatvédelmi tisztviselő előkészíti az érintetti joggyakorlás teljesítéséhez szükséges teendőket, a kérelmet megvizsgálják	Érintett részére válasz tervezete	Szakmai vezető és adatvédelmi tisztviselő	Egyedileg meghatározott	Intézmény vezető	né	né	né
3.	Érintetti joggyakorlás teljesítése/visszaautásítása	Belső adatvédelmi és adatbiztonsági szabályzat, GDPR	Szakmai vezető által kijelölt foglalkoztatottat és az adatvédelmi tisztviselő előkészíti az érintetti joggyakorláshoz kapcsolódó kérelemre a választ	Érintett részére válasz	Szakmai vezető és adatvédelmi tisztviselő	Egyedileg meghatározott	Intézmény vezető	né	né	né
4.	Adatvédelmi incidens jelzése adatvédelmi tisztviselő felé	Belső adatvédelmi és adatbiztonsági szabályzat, GDPR	Az intézményi foglalkoztatott észleli az adatvédelmi incidenst	Jelzés az adatvédelmi tisztviselő felé	Az adatvédelmi incidenst észlelő személy	Az észleléstől számított 60 perc	Intézmény vezető	né	né	né
5.	Adatvédelmi incidens kockázatelemzése	Belső adatvédelmi és	A kockázatelemzés elkészítése	Kockázatelemzés	Adatvédelmi tisztviselő	Az adatvédelmi incidens	Intézmény vezető	né	né	né

		adatbiztonsági szabályzat, GDPR				foglalkoztatói tudomásszerzésétől számított 72 óra				
6.	Adatvédelmi incidens jelentése a NAIH felé és nyilvántartásba vétel	Belső adatvédelmi és adatbiztonsági szabályzat, GDPR	Annak eldöntése, hogy az adatvédelmi incidenst jelenteni kell-e a NAIH felé	Bejelentés és nyilvántartásba vétel	Adatvédelmi tisztviselő	Az adatvédelmi incidens foglalkoztatói tudomásszerzésétől számított 72 óra	Intézmény vezető	né	né	né
7.	Adatbiztonsági ellenőrzés	Belső adatvédelmi és adatbiztonsági szabályzat, GDPR	A kockázatelemzést el kell készíteni	Adatbiztonsági ellenőrzésről felvett jegyzőkönyv	Szakmai vezető, informatikus és adatvédelmi tisztviselő	Egyedileg meghatározott	Intézmény vezető	né	né	né
8.	Kockázatkezelés	Belső adatvédelmi és adatbiztonsági szabályzat, GDPR	A kockázatelemzést alapján kockázatkezelési tervet kell készíteni	Kockázatkezelési terv	Intézményvezető	Egyedileg meghatározott	Intézmény vezető	né	né	né
9.	Oktatás	Belső adatvédelmi és adatbiztonsági szabályzat, GDPR	Az oktatás előkészítése	Oktatási napló	Adatvédelmi tisztviselő	Évente egy alkalommal, új dolgozók esetében szükség szerint	Intézmény vezető	né	né	né
10.	Új adatkezelés bevezetéséhez tervleírás készítése	Belső adatvédelmi és adatbiztonsági szabályzat, GDPR	Az intézményvezető a javasolt, vagy felmerülő új adatkezelés részleteit és az új adatkezelés bevezetésének folyamatát, a hatásvizsgálatot	Tervleírás	Adatvédelmi tisztviselő	Egyedileg meghatározott	Intézmény vezető	né	né	né

			megelőzően egyeztetni az adatvédelmi tisztviselővel, továbbá az érintett szakmai vezetőikkel, foglalkoztatottakkal.							
11.	Adatvédelmi hatásvizsgálat	Belső adatvédelmi és adatbiztonsági szabályzat, GDPR	Az intézményvezető az új adatkezelés megkezdése előtt adatvédelmi hatásvizsgálatot végez	Adatvédelmi hatásvizsgálat	Intézményvezető	Egyedileg meghatározott	Adatvédelmi tisztviselő	né	né	né

3. SZÁMÚ MELLÉKLET – AZ ADATKEZELÉSI TEVÉKENYSÉGEK NYILVÁNTARTÁSA

Külön okiratba foglalva tartalmazza a méretére tekintettel.

4. SZÁMÚ MELLÉKLET- ADATVÉDELMI INCIDENSEK NYILVÁNTARTÁSA MINTA

I. Az adatkezelő adatai és elérhetőségei

Név:
Cím:
Telefon:
Email:
Weboldal:
Adatvédelmi tisztviselő neve:
Adatvédelmi tisztviselő elérhetősége:

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

5. SZÁMÚ ADATBIZTONSÁGI ELLENŐRZÉS RŐL 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 ³				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							

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

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 ⁴				Eddigi védelem leírása	A kockázat csökkentése re tett javaslat	Határidő
	Nem fordulhat elő	Kismértékű előfordulási lehetőség	Reális előfordulási lehetőség	Minde n bizonyul 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.							
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 ⁵				Eddigi védelem leírása	A kockázat csökkentés ére tett javaslat	Határidő
	Nem fordulhat elő	Kismértékű előfordulási lehetőség	Reális előfordulási lehetőség	Minde n bizonyul			

⁴ X-et kell tenni abba a négyzetbe, melynek legnagyobb a valószínűsége

⁵ X-et kell tenni abba a négyzetbe, melynek legnagyobb a valószínűsége

		si lehetőség		előford ul			
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 jogtiszt, ismeretlen szoftver alkalmazása							
szoftverhiba							
jogosulatlan hozzáférés, másolás lehetősége							
szoftver ellenőrizetlen bevitelle az informatikai rendszerbe							
vírusveszély							
szándékos vagy gondatlan kezelési, karbantartási hiba							
a szoftver sérülése, károsodása hardverhiba miatt							
adatvesztés, károsodás hardver- vagy szoftverhiba miatt							
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

6. SZÁMÚ MELLÉKLET – ADATKEZELÉSI HOZZÁJÁRULÁS

Alulírott

születési név:

születési hely, idő:.....

anyja neve:.....

lakcím:.....

jelen nyilatkozat aláírásával hozzájárulok ahhoz, hogy a

.....

személyes adatomat az intézmény kezelje a ügyel 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]

7. SZÁMÚ MELLÉKLET – HOZZÁJÁRULÁS A SZEMÉLYES ADATOKNAK A SZOCIÁLIS ALAP-, MESTER-, ÉS SZAKKÉPZÉSBEN RÉSZTVEVŐ HALLGATÓK

Alulírott⁶

születési név:

születési hely, idő:.....

anyja neve:.....

lakcím:.....

jelen nyilatkozat aláírásával hozzájárulok ahhoz, hogy a

.....
személyes adatomat az intézmény a szociális alap-, mester-, és szakképzésben résztvevő hallgatója megismerje.

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]⁷

.....

[Név, aláírás]

⁶ Személyi igazolványon és lakcímet igazoló hatósági igazolványon szereplő adatokkal kitöltendő

⁷ Az aláírás helye és dátuma

8. SZÁMÚ MELLÉKLET – ADATKEZELÉSHEZ HOZZÁJÁRULÁS VISSZAVONÁSA FORMANYOMTATVÁNY

Alulírott⁸

születési név:

születési hely, idő:.....

anyja neve:.....

lakcím:.....

jelen nyilatkozat aláírásával visszavonom a naponügyben
.....személyes adatok tekintetében megadott adatkezelési hozzájárulásomat.

[Keltetés helye, ideje]⁹

.....

[Név, aláírás]

⁸ Személyi igazolványon és lakcímet igazoló hatósági igazolványon szereplő adatokkal kitöltendő

⁹ Az aláírás helye és dátuma

9. SZÁMÚ MELLÉKLET – NYILATKOZAT ADATKEZELÉSI TÁJÉKOZTATÁS MEGTÖRTÉNTÉRŐL ÉS ADATKEZELÉSI TÁJÉKOZTATÓ MEGISMERÉSÉRŐL

Alulírott az alábbiakban nyilatkozom, hogy az intézmény munkatársa tájékoztatott a(z) tevékenységhez kapcsolódó adatkezelésről, a iktatószámú adatkezelési tájékoztatót megismertem, így tisztában vagyok azzal, hogy ki, milyen jogalapról, milyen célból, milyen időtartamig kezeli az adataimat.

Tudomásul veszem, hogy a szolgáltatás igénybevétele esetén a személyes adataimat az adatkezelő munkatársa megismeri, a vonatkozó nyilvántartásban rögzíti, az adatkezelési tájékoztatóban rögzített célból kezeli és ott meghatározott ideig tárolja. Tudomásul veszem, hogy a személyes adataimat (kiskorú adatait) az adatkezelő kizárólag a szolgáltatás igénybevételének elősegítése céljából más adatkezelő(k) felé továbbíthatja.

Tudomásul veszem, hogy adataim kezelésével kapcsolatban – ha azt jogszabály nem korlátozza, vagy ki nem zárja – a következő jogok illetnek meg: tájékoztatáshoz 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. Az adatkezeléssel összefüggő jogaimról az adatkezelési tájékoztató elolvasásával tájékoztatást kaptam.

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

Megértettem, hogy amennyiben a megítélésem szerint a személyes adataimnak az intézmény általi kezelése sérti a vonatkozó jogszabályokat, jogosult vagyok az adatvédelmi felügyeleti hatóságnál panaszt tenni vagy bírósághoz fordulni. Magyarországon az adatvédelmi felügyeleti hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság (1055 Budapest, Falk Miksa utca 9-11, postacím: 1363 Budapest, Pf.: 9.) 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: Budapest,év.....hó.....napon

.....
Igénybevevő/Szülő/Törvényes képviselő¹⁰

.....
Gyermek/fiatal¹¹

.....
Szülő/Törvényes képviselő¹²

Az adatkezelési tájékoztató szerinti és a hozzájárulásomon alapuló adattovábbításhoz hozzájárulok.

Dátum: Budapest,év.....hó.....napon

.....
Igénybevevő/ Törvényes képviselő¹³

.....
Törvényes képviselő¹⁴

¹⁰ A megfelelő aláhúzendó

¹¹ Gyermekjóléti szolgáltatásban érintettekkel

¹² Szükség esetén

¹³ A megfelelő aláhúzendó

¹⁴ Szükség esetén

Feljegyzés szóbeli adatkezelési tájékoztatásról¹⁵

Alulírott és, mint a Intézmény munkatársai kijelentjük, hogy

Név:.....

Születési név:.....

Születési hely, idő:.....

Anyja neve:.....

részére kérésére szóbeli tájékoztatást nyújtottunk a tevékenységhez kapcsolódó adatkezelésről az érintett személyazonosságának ellenőrzését követően, aki szóban a tájékoztatást tudomásul vette, azzal egyetértett.

Keltezés helye, ideje

.....
intézményi munkatárs aláírása

.....
intézményi munkatárs aláírása

¹⁵ Elsősorban azokban az esetekben alkalmazzuk, amikor látássérült vagy írni, olvasni nem tudó személy részére kell az adatkezelési tájékoztatást megadni

12. SZÁMÚ MELLÉKLET – FOGLALKOZTATOTT ADATKEZELÉSI HOZZÁJÁRULÁSA

Adatkezeléshez hozzájárulás

Alulírott (születési név:, születési hely, idő:....., anyja neve:.....) jelen nyilatkozat aláírásával hozzájárulok ahhoz, hogy a személyes adataimat az Intézmény 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]

13. SZÁMÚ MELLÉKLET – FOGLALKOZTATOTTI NYILATKOZAT ADATKEZELÉSI TÁJÉKOZTATÓ MEGISMERÉSÉRŐL

Alulírott

Név:.....¹⁶
Születési név:.....
Születési hely, idő:.....
Anyja neve:.....

jelen nyilatkozat aláírásával kijelentem, hogy az intézménynek a foglalkoztatásomhoz kapcsolódó adatkezelési tájékoztatóját elolvastam, annak tartalmát megismertem, így tudomásom van az adatkezelő és az adatvédelmi tisztviselő személyéről, elérhetőségeiről, az Intézmény, mint munkáltató által kezelt adatok köréről, annak jogalapjáról, az adatkezelés céljáról, az adatok őrzésének időtartamáról, az adattovábbítás körülményeiről, feltételeiről.

Kijelentem, hogy tájékoztatást kaptam a munkáltatóm által végrehajtott adatbiztonsági intézkedésekről.

Tudomásom van arról, hogy megillet az adataim kezelésével összefüggésben a tájékoztatáshoz való jog, mely alapján kérhetem, hogy az Intézmény milyen személyes adataimat, milyen jogalapon, milyen adatkezelési cél miatt, milyen forrásból, mennyi ideig kezeli, az Intézmény kinek, mikor, milyen jogszabály alapján, mely személyes adataimhoz biztosított hozzáférést vagy kinek továbbította a személyes adataimat.

Tudomásom van arról, hogy megillet a személyes adataim helyesbítéséhez való jog, a törléshez való jog, a zároláshoz való jog, tiltakozáshoz való jog, adathordozhatóság joga, melyek példákval illusztrált tartalmát a tájékoztatókból megértettem.

Tudomásom van arról, hogy amennyiben a munkáltatóm általi adatkezelés hozzájárulásomon alapul, akkor megillet a hozzájárulás visszavonásának a joga, azaz bármilyen jogkövetkezmény nélkül dönthetek arról, hogy a hozzájárulásomat a továbbiakban nem tartom fent.

Tudomásul vettem az adatkezelési tájékoztató jogorvoslatra vonatkozó tájékoztatását, illetve tudomással bírok arról, hogy a munkáltató az adatkezelési tevékenységeiről nyilvántartást vezet és minden egyes adatkezelési tevékenységéhez külön tájékoztató készült, melyet bármikor elérhetek elektronikusan az intézmény honlapján, vagy papír alapon nyitvatartási időben az Intézmény székhelyén, telephelyein.

¹⁶ Olvashatóan kiírva

[Keltezés helye, ideje]

.....
[Név, aláírás]¹⁷

14. SZÁMÚ MELLÉKLET - ÉRTESÍTÉS SIKERTELEN PÁLYÁZATRÓL

[Címzett neve]

[értesítési címe]

Tisztelt Pályázó!

Megköszönve Intézményünk irányába mutatott érdeklődését, sajnálattal értesítjük, hogy a meghirdetett állásra nem Ön került kiválasztásra.

Tájékoztatjuk, hogy a pályázati anyaga és az abban megadott személyes adatai a jelen értesítés elküldésének napjától számított 60. napon fizikailag megsemmisítésre, illetve helyreállíthatatlanul törlésre kerülnek. Az Intézmény a pályázat anyagában megadott személyes adatait - az adatok törlésére és megsemmisítésére nyitva álló határidő lejártával - nem kezeli, adatot nem tart nyilván.

Amennyiben szeretné, hogy az Intézmény az Ön által betölthető üres álláshelyekről értesítést küldjön az Ön részére, akkor a mellékelt nyilatkozatot a jelen levél keltétől számított 60. napig történő megérkezéssel az Intézmény szám alatti címére megküldeni szíveskedjen.

Tájékoztatom, hogy a mellékelt nyilatkozat visszaküldése esetén a pályázati anyagát 365 napig megőrizzük és nyilvántartásba vesszük, Ön által betölthető álláshely esetén értesítést küldhetünk. Az adatkezelés jogalapja az Ön hozzájárulása, melyet bármikor visszavonhat, az adatkezelés célja az Ön értesítése az Ön által betölthető álláshelyekről. Tájékoztatom, hogy harmadik személy felé az adatai nem kerülnek továbbításra.

A jelen levélben megfogalmazottól bővebb adatkezelési tájékoztató elérhető elektronikusan az intézmény honlapján az alábbi linken:....., illetve papír alapon az Intézmény székhelyén, és telephelyein.

[Keltezés helye, ideje]

¹⁷ A nevet olvashatóan ki kell írni, az aláírás a személyi igazolványban szereplő aláírással megegyező formájú

Tisztelettel:

.....
intézményvezető

15. SZÁMÚ MELLÉKLET - KÉRELEM PÁLYÁZAT ŐRZÉSÉHEZ

(Intézmény címe)

Tisztelt (Intézmény neve)!

Alulírott(születési név:....., születési hely, idő:....., anyja neve:....., lakcím:....., telefonszám:.....) tudomásul veszem, hogy nem kerültem kiválasztásra a meghirdetett álláshelyre, azonban kérem, hogy amennyiben általam betölthető üres álláshely ismételen felmerül, akkor részemre értesítést küldeni szíveskedjenek.

Kijelentem, hogy az adatkezelési tájékoztatót megismertem.

Jelen levelemmel hozzájárulok ahhoz, hogy a korábban benyújtott pályázatom anyagát, valamint az abban megjelölt személyes adataimat a jelen hozzájárulás keltétől számított 365 napig, vagy a hozzájárulásom visszavonásáig megőrizték és szükség esetén részemre értesítést küldjenek az általam betölthető álláshelyekről.

[Keltezés helye, ideje]

Tisztelettel:

.....
[Név, aláírás]

16. SZÁMÚ MELLÉKLET – ELHELYEZETT KAMERÁK ÉS MEGFIGYELT TERÜLETEK LEÍRÁSA

Sorszám	Kamera helye	Megfigyelt terület	Adattárolás helye

17. SZÁMÚ MELLÉKLET – KULCS-NYILVÁNTARTÁS

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

18. SZÁMÚ MELLÉKLET – ADOTT HELYISÉGBEN ÖNÁLLÓAN TARTÓZKODHATÓ SZEMÉLYEK LISTÁJA

Helyiség száma	Helyiség megnevezése	Önállóan bent tartózkodható személyek pozíciójának megnevezése

Keltezés helye, ideje

19. 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

20. 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. Az Intézmény 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 aláhúzendó

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.			

21. SZÁMÚ MELLÉKLET – NEM AUTOMATIKUS ADATMENTÉSRŐL FELVETT TELJESÍTÉSI IGAZOLÁS

A mentést végezte:.....

A mentés elvégzésének időpontja:.....

A mentést végző aláírása:.....

A mentés során tapasztaltak leírása:

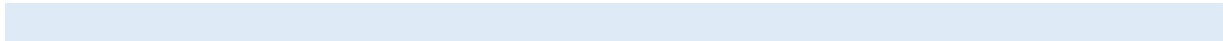
.....
.....
.....

Egy példányt a mai napon átvettem:

(Keltezés helye, ideje)

.....

intézményvezető



22. SZÁMÚ MELLÉKLET – IGAZOLÁS GYÓGYSZEREK ÁTVÉTELÉRE TÖRTÉNŐ FELHATALMAZÁSRÓL

Alulírott(név)

Születési név:.....

Születési hely:.....

Születési idő:.....

Lakcím:.....

TAJ:....., mint ellátott és

a(székhely:, adószám:, telephely
címe:.....képviseli:), mint szolgáltató

kijelentjük, hogy együttműködési megállapodást kötöttünk, mely alapján a, mint szolgáltató alkalmazottai (igazolványszámaik:.....) jogosultak ellátott nevében és helyett az orvosi recepteket átvenni, a gyógyszereket kiváltani, átvenni és azokat ellátott részére eljuttatni.

Az együttműködési megállapodás és jelen igazolás hatálya: ideig szól.

Az adatkezelő a, adatvédelmi tisztviselő: dr. Anda Péter (elérhetősége: [.....](#)).

Az adatkezelés jogalapja az Európai Parlament és a Tanács 2016/679. rendeletének 6. cikk (1) bekezdés b. pontja, azaz az adatkezelés az érintettel kötött szerződés teljesítéséhez szükséges.

Az adatkezelés célja a megállapodás és jogszabályi kötelezettség teljesítése, illetve az ellátott akadályozottsága esetén a szükséges gyógyszerek és orvosi iratok beszerzése.

Jelen nyilatkozat az illetékes Egészségügyi Szolgáltató és Gyógyszertár előtti eljárás érdekében került kiadásra, mely igazolja a megállapodás létrejöttét, a felvett adatok helyességét, a fenti igazolványszámmal rendelkező dolgozók eljárási jogosultságát.

Kiállítás helye és kelte:.....,évhónapján

.....
(név) ellátott

.....
szolgáltató
képv.:.....

23. SZÁMÚ MELLÉKLET – IGAZOLÁS ORVOSI IRATOK ÁTVÉTELÉRE TÖRTÉNŐ FELHATALMAZÁSRÓL

Alulírott(név)

Születési név:.....

Születési hely:.....

Születési idő:.....

Lakcím:.....

TAJ:....., mint ellátott és

a (székhely:, adószám:, telephely
címe:.....képviseli:,) mint szolgáltató

kijelentjük, hogy együttműködési megállapodást kötöttünk, mely alapján a, mint szolgáltató alkalmazottai (igazolványszámaik:.....) jogosultak ellátott nevében és helyett az egészségügyi adatokat tartalmazó leleteket, zárójelentéseket átvenni és azokat ellátott részére eljuttatni.

Az együttműködési megállapodás és jelen igazolás hatálya: ideig szól.

Az adatkezelő a, adatvédelmi tisztviselő: dr. Anda Péter (elérhetősége:).

Az adatkezelés jogalapja az Európai Parlament és a Tanács 2016/679. rendeletének 6. cikk (1) bekezdés b. pontja, azaz az adatkezelés az érintettel kötött szerződés teljesítéséhez szükséges.

Az adatkezelés célja a megállapodás és jogszabályi kötelezettség teljesítése, illetve az ellátott akadályozottsága esetén a szükséges gyógyszerek és orvosi iratok beszerzése.

Az adatkezelés célja a megállapodás és jogszabályi kötelezettség teljesítése, illetve az ellátott akadályozottsága esetén a szükséges gyógyszerek és orvosi iratok beszerzése.

Jelen nyilatkozat az érintett kezelését végző bármely egészségügyi szolgáltató előtti eljárás érdekében került kiadásra, mely igazolja a megállapodás létrejöttét, a felvett adatok helyességét, a fenti igazolványszámmal rendelkező dolgozók eljárási jogosultságát.

Kiállítás helye és kelte:.....,évhónapján

.....
(név) ellátott

.....
szolgáltató

képv.:.....

24. SZÉMÚ MELLÉKLET – SZEMÉLYES ADAT TÖRLÉSÉRE JEGYZŐKÖNYV, ADATHORDOZÓ
MEGSEMMISÍTÉSÉRŐL JEGYZŐKÖNYV

Készült (év) (hónap) (nap) a intézmény
..... sz. alatti székhelyén.

A bizottság tagjai:

- | | | |
|-----------------|-------|----------|
| (1) | (név) | aláírás) |
|(beosztás) | | |
| (2)..... | (név) | aláírás) |
|(beosztás) | | |
| (3)..... | (név) | aláírás) |
|(beosztás) | | |
| (4)..... | (név) | aláírás) |
|(beosztás) | | |

A törlés/megsemmisítés megkezdésének és befejezésének időpontja:

.....(tól) - (ig)

Az intézményhez iktatószámmon érkezett irat és mellékletei.

A levél és a melléklet megnyitását követően megállapítást nyert, hogy olyan személyes adatokat tartalmaz, mely a ügyhöz kapcsolódóan kifejtett intézményi tevékenységhez nem szükségesek, ügyviteli értéke megszűnt, az intézményünk hatósági jogkörrel nem rendelkezik.

Szövegtartalom esetén:

Az irat és annak mellékletei iktatószámú levéllel továbbításra kerültek a gyámhatóságnak és a rendőrségnek és egyúttal értesítettük a címzettet a iktatószámú levéllel, hogy a megküldött dokumentum olyan személyes adatokat tartalmazott, melynek kezelésére az intézmény nem jogosult.

Az adattovábbítást követően a célhoz kötöttség és adatkészletezés tilalma alapelveknek eleget téve az adatok helyreállíthatatlan törlése vagy (papír alapú adathordozó esetén) megsemmisítése szükséges.

A törléssel/megsemmisítéssel a bizottság tagjai egyetértenek, nincs olyan szakmai indok, ami az ügy vitele érdekében alátámasztaná a személyes adat tárolásának szükségességét:

- | | |
|----------|----------|
|(1) |(2) |
|(3) |(4) |

Az iratok megsemmisítését jóváhagyom, végrehajtását elrendelem.

.....

szakmai vezető

A törlés/megsemmisítés év.....hó.....napperckor megtörtént, a törlést/megsemmisítést
elvégezte



Alulírott

Név:.....

Születési név:.....

Születési hely:.....

Születési idő:.....

Anyja neve:.....

hozzájárulok ahhoz, hogy a által szervezettelnevezésű táborban/rendezvényen/konferencián ¹⁸tartózkodásom ideje alatt rólam fénykép - vagy videofelvétel készüljön és ezen felvételek az intézmény honlapján közzétételre kerüljenek az intézményi élet, szervezett program bemutatása okán.

nem járulok hozzá ahhoz, hogy a által szervezettelnevezésű táborban/rendezvényen/konferencián tartózkodásom ideje alatt rólam fénykép - vagy videofelvétel készüljön és ezen felvételek az intézmény honlapján közzétételre kerüljenek az intézményi élet, szervezett program bemutatása okán.

hozzájárulok ahhoz, hogy a által szervezettelnevezésű táborban/rendezvényen/konferencián ¹⁹tartózkodásom ideje alatt rólam fénykép - vagy videofelvétel készüljön és ezen felvételek az intézmény közösségi oldalain:..... közzétételre kerüljenek az intézményi élet, szervezett program bemutatása okán.

nem járulok hozzá ahhoz, hogy a által szervezettelnevezésű táborban/rendezvényen/konferencián tartózkodásom ideje alatt rólam fénykép - vagy videofelvétel készüljön és ezen felvételek az intézmény közösségi oldalain:..... közzétételre kerüljenek az intézményi élet, szervezett program bemutatása okán.

hozzájárulok ahhoz, hogy a által szervezettelnevezésű táborban/rendezvényen/konferencián tartózkodásom ideje alatt rólam fénykép - vagy videofelvétel készüljön és ezen felvételek az intézmény épületében közzétételre kerüljenek az intézményi élet, szervezett program bemutatása okán.

nem járulok hozzá ahhoz, hogy a által szervezettelnevezésű táborban/rendezvényen/konferencián tartózkodásom ideje alatt

¹⁸ A megfelelő aláhúzendó

¹⁹ A megfelelő aláhúzendó

rólam fénykép - vagy videofelvétel készüljön és ezen felvételek az intézmény épületében közzétételre kerüljenek az intézményi élet, szervezett program bemutatása okán.

hozzájárulok ahhoz, hogy a által szervezettelnevezésű táborban/rendezvényen/konferencián tartózkodásom ideje alatt rólam fénykép - vagy videofelvétel készüljön és ezen felvételek intézmény által kiadott kiadványban közzétételre kerüljenek az intézményi élet, szervezett program bemutatása okán.

nem járulok hozzá ahhoz, hogy a által szervezettelnevezésű táborban/rendezvényen/konferencián tartózkodásom ideje alatt rólam fénykép - vagy videofelvétel készüljön és ezen felvételek intézmény által kiadott kiadványban közzétételre kerüljenek az intézményi élet, szervezett program bemutatása okán.

hozzájárulok ahhoz, hogy a által szervezettelnevezésű táborban/rendezvényen/konferencián tartózkodásom ideje alatt rólam fénykép - vagy videofelvétel készüljön és ezen felvételek kutatásban, továbbképzésben résztvevő intézményi munkatársak, az intézményben szakmai gyakorlatukat töltő különböző oktatási intézményben tanulók általi megfigyelések és munkájuk dokumentálása okán felhasználásra kerüljenek.

nem járulok hozzá ahhoz, hogy a által szervezettelnevezésű táborban/rendezvényen/konferencián tartózkodásom ideje alatt rólam fénykép - vagy videofelvétel készüljön és ezen felvételek kutatásban, továbbképzésben résztvevő intézményi munkatársak, az intézményben szakmai gyakorlatukat töltő különböző oktatási intézményben tanulók általi megfigyelések és munkájuk dokumentálása okán felhasználásra kerüljenek.

Kijelentem, hogy a fenti hozzájárulásom megadása előtt „Az intézmény által szervezett eseményeken résztvevőkről készített fénykép és videofelvétel készítése” adatkezelési tájékoztatót 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 az adatkezelési tevékenységeiről nyilvántartást vezet, mely adatkezelési tevékenységek nyilvántartása a 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)