Útkeresés Segítő Szolgálat

Adatvédelmi, adat- és információbiztonsági, valamint közzétételi szabályzat

Dunaújváros, 2021. május 17.
Felülvizsgálva: 2024. február 15.
2025. február 28.
2026. július 01.

Tartalomjegyzék

I. Bevezető szabályok....5
I.1. A szabályzat célja....5
I.2. A szabályzat hatálya....5
I.3. Fogalmak....6
II. Alapelvek....8
II.1. A személyes adatok kezelésére vonatkozó alapelvek....8
II.2. A jogszerűség, tisztességes eljárás és átláthatóság....9
II.2.1. A jogszerűség, tisztességes eljárás és átláthatóság elve....9
II.2.2. A személyes adatok kezelésének jogszerűsége....9
II.2.2.1. Az érintett hozzájárulása....10
II.2.2.2. A kötelező adatkezelés jogalapja....10
II.2.2.3. Az adatok eredeti gyűjtési céljától eltérő gyűjtése....11
II.2.3. Az elvhez kapcsolódó jogok....11
II.3. A célhoz kötöttség....11
II.3.1. A célhoz kötöttség elve....11
II.3.2. Az elvhez kapcsolódó jogok....12
II.4. Az adattakarékosság....12
II.4.1. Az adattakarékosság elve....12
II.4.2. Az elvhez kapcsolódó jogok....12
II.5. A pontosság....12
II.5.1 A pontosság elve....12
II.5.2. Az elvhez kapcsolódó jogok....12
II.6. A korlátozott tárolhatóság....12
II.6.1. A korlátozott tárolhatóság elve....12
II.6.2. Az elvhez kapcsolódó jogok....13
II.7. Az integritás és bizalmas jelleg....13
II.7.1. Az integritás és bizalmas jelleg elve....13
II.7.2. Az elvhez kapcsolódó jogok....13
III. Az érintett jogai....13
III.1. Az érintett személyes adatokkal kapcsolatos jogai....13
III.2. Az átlátható tájékoztatáshoz és kommunikációhoz való jog, valamint a joggyakorlásra vonatkozó intézkedésekkel összefüggő jogok....13
III.3. Az információkhoz való jog, ha a személyes adatokat az intézmény az érintettől gyűjti....15
III.3.1. Az információ biztosítás tartalma....15
III.3.2. Az információ biztosítás szükségtelensége....16
III.3.3. Az információ biztosításáért való felelősség....16
III.4. Az információkhoz való jog, ha az adatokat az intézmény nem az érintettől szerzi meg....16
III.4.1. Az információ biztosítás tartalma....16
III.4.2. Az információ biztosítás határideje....17
III.4.3. Az információ biztosítás szükségtelensége....17
III.4.4. Az információ biztosításáért való felelősség....17
III.5. A hozzáférési jog....17
III.5.1. Az információ biztosítás tartalma....17
III.5.2. Az információ biztosítás szabályai....18
III.6. A helyesbítéshez való jog....18
III.7. A törléshez való jog....18
III.7.1. Az adatok törlése....18
III.7.2. Az adattörlési kötelezettség alóli kivételek....19
III.7.3. Az adatok törlésével kapcsolatos felelősség....19
III.8. Az adatkezelési korlátozáshoz való jog....19
III.9. Az adathordozhatósághoz való jog....20
III.10. A tiltakozáshoz való jog....20
III.11. Az automatizált döntéshozatallal kapcsolatos jogok....21
IV. Az adatkezelő....21
IV.1. Az adatkezelő feladatai....21
IV.2. Az adatvédelem....21
IV.2.1. Adatvagyon leltár....22
IV.2.1.1. Az adatvagyon leltár területek....22

IV.2.1.2. Az adatvagyon leltár tartalma....22
IV.2.1.3. Az adatvagyon leltár készítéséért felelős személyek....23
IV.2.2. Az adatok, adatbázisok biztonsági osztályba sorolása....23
IV.2.3. Az adatkezelés ellenőrzése....24
IV.2.4. Új adatkezelési helyzetek....24
IV.2.5. Az adatvagyon leltár felülvizsgálata....25
IV.2.6. Az adatvagyon leltárba való felvétel tilalma....25
IV.3. Adatkezelési nyilvántartás....25
IV.4. Együttműködés a felügyeleti hatósággal....26
V. Az adatfeldolgozó....26
V.1. Az adatfeldolgozó....26
VI. Adatbiztonság....26
VI.1. Általános adatbiztonsági követelmények....26
VI.1.1. Az intézmény adminisztratív adatvédelmi intézkedései....27
VI.1.2. Adatvédelmi incidens kezelése....27
VI.1.2.1. Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak....27
VI.1.2.2. Adatvédelmi incidens nyilvántartás....28
VI.1.2.3. Az érintett tájékoztatása az adatvédelmi incidensről....28
VI.1.3. Az intézmény fizikai adatvédelmi intézkedései....29
VI.1.3.1. Az adatok szállítása, intézményen kívüli kezelése....30
VI.1.4. Az intézmény logikai adatvédelmi intézkedései....30
VI.1.4.1. Az adatok kezelésére használt rendszerek és szolgáltatások....30
VII. Adatvédelmi hatásvizsgálat....31
VII.1. Adatvédelmi hatásvizsgálat....31
VII.1.1. Adatvédelmi hatásvizsgálat végzési kötelezettség....31
VII.1.1.1. Kötelező adatvédelmi hatásvizsgálat....31
VII.1.1.2. Az adatvédelmi hatásvizsgálat mellőzése....32
VII.1.2. Az adatvédelmi hatásvizsgálat elvégzése....32
VII.1.3. Az adatvédelmi hatásvizsgálat folyamata....33
VII.1.4. Az adatvédelmi hatásvizsgálat nyilvánosságra hozatala....33
VII.2. Előzetes konzultáció....33
VIII. Az adatvédelem szervezeti háttere....33
VIII.1. A személyes adatok védelmével kapcsolatos szerepkörök....33
VIII.1.1. Az intézményvezető....34
VIII.1.1.1. Az intézményvezető feladatai:....34
VIII.1.1.2. Az adatvédelmi tisztviselő kijelölése....34
VIII.1.2. Az adatvédelmi tisztviselő....34
VIII.1.2.1. Az adatvédelmi tisztviselő jogállása....34
VIII.1.2.2. Az adatvédelmi tisztviselő feladatai....35
VIII.1.3. Az adatkezelést végző személy....36
VIII.1.4. Az adatkezelő nevében eljáró közalkalmazott és munkavállaló....36
VIII.2. A feladat és felelősség dokumentálása....36
IX. Az intézménnyel foglalkoztatási jogviszonyban álló természetes személyek adatainak kezelése....37
IX.1. Általános szabályok....37
IX.1.1. Mobiltelefon használatához kapcsolódó adatkezelési tevékenység....37
IX.1.2. Az e-mail cím használatához kapcsolódó adatkezelési tevékenység....38
IX.1.3. A számítógépek használatához kapcsolódó adatkezelési tevékenység....38
IX.2. Az intézménnyel jogviszonyban álló természetes személyek alkalmassági vizsgálataival kapcsolatos adatok kezelése....39
IX.3. Az intézménnyel foglalkoztatási jogviszonyban álló természetes személyek fényképeinek kezelése....39
X. Az intézményhez munkára jelentkezők személyes adataihoz kapcsolódó adatkezelési tevékenység....39
X.1. Általános szabályok....40
XI. Az intézményi alaptevékenységgel kapcsolatos adatkezelési előírások....40
XI.1. Adattovábbítás....41
XI.1.1. Magyar Államkincstár felé történő adattovábbítás....41
XI.1.2. Gyermekeink védelmében elnevezésű informatikai rendszer....41
XI.2. Adományosztás....42
XI.3. Cégkapu működtetéséhez kapcsolódó adatkezelési rendelkezések....42
XII. KÖZÉRDEKŰ ADATOK MEGISMERÉSÉRE VONATKOZÓ SZABÁLYOK....43
XII.1. Közérdekű adatok megismerése....43

XII.1.1 A közérdekű adat megismerésére irányuló igények benyújtásának módja....43
XII.2. Közérdekű adatok közzétételére vonatkozó szabályok....44
XII.2.1. A közérdekű adatok közzétételének rendje....44
XIII. A szabályzat nyilvánossága....45
XIV. A belső együttműködés szabályai....45
XV. A szabályzat felülvizsgálata....46
XVI. Záró rendelkezések....46

Az Útkeresés Segítő Szolgálat a továbbiakban: Intézmény) vezetője a természetes személyek személyes adatainak kezelése védelme érdekében:

– a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló az Európai Parlament és a Tanács 2016/679. számú rendelete, (továbbiakban: Általános adatvédelmi rendelet),

– az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Info tv.),

– Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény,

– a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet,

– a 305/2005. (XII. 25.) Korm. rendelet a közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról,

– a 301/2016. (IX. 30.) Korm. rendelet a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről,

– a 18/2005. (XII. 27.) IHM rendelet a közzétételi listákon szereplő adatok közzétételéhez szükséges közzétételi mintákról, valamint

– Dunaújváros Megyei Jogú Város Gazdálkodási Rendelete

figyelembevételével a következők szerint határozza meg a személyes adatok védelmének helyi szabályait.

I. Bevezető szabályok

I.1. A szabályzat célja

A szabályzat célja, hogy meghatározza:

- a személyes adatok kezelésére vonatkozó védelmi előírásokat, ennek során az adatkezelői feladatokat,
- a természetes személyeknek az adataik védelméhez kapcsolódó alapvető jogait és szabadságát.

I.2. A szabályzat hatálya

A szabályzat **tárgyi hatálya** kiterjed:

- a személyes adatok részben vagy egészben automatizált módon történt kezelésére,
- a nem automatizált módon történő személyes adatok kezelésére:
    - amelyek a nyilvántartási rendszer részét képezik, vagy
    - amelyeket egy nyilvántartási rendszer részévé kívánnak tenni.

A szabályzat hatálya tehát kiterjed minden, az intézmény által folytatott olyan adatkezelésre és feldolgozásra, amely természetes személy adataira vonatkozik, függetlenül attól, hogy az:

- teljesen vagy részben automatizált eszközzel, vagy
- manuális módon

történik-e.

A szabályzat **szervezeti hatálya** az intézményre terjed ki.
Az intézmény megbízásából történő bármely adatkezelést és feldolgozást végzőre a szabályzat a vonatkozó szerződés, illetve megállapodás alapján terjed ki.

A szabályzat **személyi hatálya** kiterjed:

- az intézmény teljes személyi állományára, valamint
- minden olyan természetes és jogi személyre, aki az intézményben tárolt, kezelt személyes adatokkal kapcsolatba kerül, vagy kerülhet, így jellemzően:
  - az intézménynél külső ellenőrzést végző személyekre, szervekre,
  - az intézménnyel szerződéses kapcsolatban álló személyekre, szervekre.

I.3. Fogalmak

-**„személyes adat”**: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;
-”különleges adat”: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló 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;
-**„adatkezelés”**: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;
-**„az adatkezelés korlátozása”**: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;
-**„profilalkotás”**: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;
-**„álnevesítés”**: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;

-**„nyilvántartási rendszer”**: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;
-**„adatkezelő”**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;
-**„adatfeldolgozó”**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;
-**„címzett”**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;
-**„harmadik fél”**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;
-**„az érintett hozzájárulása”**: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;
- **„adatvédelmi incidens”**: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;
-**„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 említett természetes személyből vett biológiai minta elemzéséből ered;
-**„biometrikus adat”**: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;
-**„egészségügyi adat”**: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;
-**„képviselő”**: az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által az Általános adatvédelmi rendelet 27. cikk alapján írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában;

-**„vállalkozás”**: gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is;
-**„felügyeleti hatóság”**: egy tagállam által az Általános adatvédelmi rendelet 51. cikknek megfelelően létrehozott független közhatalmi szerv;
-**„érintett felügyeleti hatóság”**: az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érintett:

a) az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel;
b) az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy
c) panaszt nyújtottak be az említett felügyeleti hatósághoz;

-**„személyes adatok határokon átnyúló adatkezelése”**:

a) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy
b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket;

-**„releváns és megalapozott kifogás”**: a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy ezt a rendeletet megsértették-e, illetve hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét;
-**„az információs társadalommal összefüggő szolgáltatás”**: az (EU) 2015/1535 európai parlamenti és tanácsi irányelv 1. cikke (1) bekezdésének b) pontja értelmében vett szolgáltatás;
-**„nemzetközi szervezet”**: a nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei, vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre, vagy amely ilyen megállapodás alapján jött létre.

II. Alapelvek

II.1. A személyes adatok kezelésére vonatkozó alapelvek

A személyes adatok kezelése során az intézménynél be kell tartani az alábbi hat alapelvet:

1. A jogszerűség, tisztességes eljárás és átláthatóság elvét,
2. A célhoz kötöttség elvét,
3. Az adattakarékosság elvét,
4. A pontosság elvét,
5. A korlátozott tárolhatóság elvét,
6. Az integritás és bizalmas jelleg elvét.

Az alapelvek betartása, érvényesítése az intézmény valamennyi dolgozójának, illetve a személyes adatokkal kapcsolatba kerülő más személyek feladata is.

II.2. A jogszerűség, tisztességes eljárás és átláthatóság

II.2.1. A jogszerűség, tisztességes eljárás és átláthatóság elve

A jogszerűség, tisztességes eljárás és átláthatóság elve érvényesülése érdekében az intézményben a személyes adatok kezelését:

- jogszerűen,
- tisztességesen,
- az érintett számára átlátható módon

kell végezni.

II.2.2. A személyes adatok kezelésének jogszerűsége

Az intézmény - a jelen szabályzatban rögzített eljárásrendnek megfelelően - minden személyes adat kezelés megkezdése előtt megvizsgálja, hogy fenn áll-e a személyes adat kezelésének jogszerűségi feltétele.

<u>Az adatkezelés általános jogszerű feltételei</u>

A jogszerűségi feltételek:

- az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
- az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
- az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges; (kötelező adatkezelés)
- az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
- az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges; (kötelező adatkezelés)

  Ide tartozik:
  - a törvény alapján, vagy
  - a törvény felhatalmazása alapján helyi önkormányzat által

  elrendelt adatkezelés;
- az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek. (Ezt az elvet nem kell alkalmazni az intézmény által a feladatai ellátása során végzett adatkezelésre.)

<u>A különleges adatok adatkezelésének jogszerűségi feltételei</u>

Alapvető szabály, hogy **tilos**:

- 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.

Az intézmény abban az esetben kezelhet különleges adatot, ha:

- az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha jogszabály úgy rendelkezik, hogy a tilalom nem oldható fel az érintett hozzájárulásával;
- az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező kollektív szerződés ezt lehetővé teszi;
- az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;
- az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
- az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges;
- az adatkezelés jelentős közérdek miatt szükséges jogszabály alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;
- az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, jogszabály alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, továbbá a vonatkozó feltételekre és garanciákra figyelemmel.

A büntetőjogi felelősséggel kapcsolatos és bűncselekményekre vonatkozó személyes adatok kezelésének feltétele

Ilyen adatokat csak közhatalmi szerv kezelhet.

II.2.2.1. Az érintett hozzájárulása

Az intézmény - a jelen szabályzatban rögzített eljárásrendnek megfelelően - személyes adatot az érintett hozzájárulása jogalapra hivatkozva csak akkor kezelhet, ha a hozzájárulás megadása az érintett részéről tevőleges, önkéntes, és egyértelmű.
Fontos, hogy a hozzájárulás megadásának bizonyíthatónak kell lennie, tehát arról:

- írásos, (papír vagy elektronikus) dokumentumnak kell rendelkezésre állnia, vagy
- hang, illetve videó felvételnek kell lennie.

A hozzájárulás szövegének tartalmaznia kell azt, hogy az érintett beleegyezik az adott célra, vagy több célra történő adatkezelésbe.

II.2.2.2. A kötelező adatkezelés jogalapja

Az intézmény - a jelen szabályzatban rögzített eljárásrendnek megfelelően - biztosítja a kötelező adatkezelés jogalapjára vonatkozó alapelv érvényesülését.

A kötelező adatkezelés körébe tartozó jogszerűségi feltételek:
- az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges,
- az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.

Ezekben az esetekben az adatkezelés célját a konkrét jogalapra hivatkozással kell meghatározni. Fontos, hogy az adatkezelést meghatározó törvényben, illetve helyi rendeletben rögzítetteket kell figyelembe venni:
- a kezelendő adatok fajtája,
- az adatkezelés célja és konkrét feltételei,
- az adatok megismerhetősége,
- az adatkezelés időtartama

tekintetében.

II.2.2.3. Az adatok eredeti gyűjtési céljától eltérő gyűjtése

Az intézmény - a jelen szabályzatban rögzített eljárásrendnek megfelelően - biztosítja az adatok eredeti gyűjtési céljától eltérő gyűjtésére vonatkozó alapelv érvényesülését.

Az intézmény ilyen esetekben vizsgálja:
- a személyes adatok gyűjtésének céljait és a tervezett további adatkezelés céljai közötti esetleges kapcsolatokat,
- a személyes adatok gyűjtésének körülményeit, különös tekintettel az érintettek és az adatkezelő közötti kapcsolatokra,
- a személyes adatok jellegét, különösen pedig azt, hogy a személyes adatok különleges kategóriáinak kezeléséről van-e szó, illetve, hogy büntetőjogi felelősség megállapítására és bűncselekményekre vonatkozó adatoknak a kezeléséről van-e szó,
- azt, hogy az érintettekre nézve milyen esetleges következményekkel járna az adatok tervezett további kezelése,
- a megfelelő garanciák meglétét, ami jelenthet titkosítást vagy álnevesítést is.

II.2.3. Az elvhez kapcsolódó jogok

Az elv érvényesüléséhez közvetlenül kapcsolódnak az alábbi jogok:
- az átláthatósággal kapcsolatos jogok és intézkedések,
- az adatkezeléssel kapcsolatos tájékoztatáshoz való jog:
    - ha a személyes adatokat az érintettől gyűjtik,
    - ha a személyes adatokat nem az érintettől szerezték meg,
- az érintett hozzáférési joga.

II.3. A célhoz kötöttség

II.3.1. A célhoz kötöttség elve

A célhoz kötöttség elve alapján az intézményben:
- a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet,
- a személyes adatok nem kezelhetőek célokkal össze nem egyeztethető módon.

(Ezen elv alól kivételt képez a közérdekű archiválás, a tudományos és történelmi kutatási cél vagy a statisztikai célból történő további adatkezelés.)

II.3.2. Az elvhez kapcsolódó jogok

Az elv érvényesüléséhez közvetlenül kapcsolódnak az alábbi jogok:
- az érintett hozzáférési joga.

II.4. Az adattakarékosság

II.4.1. Az adattakarékosság elve

Az intézmény az adattakarékosság elve érdekében a személyes adatok közül annyi és olyan adatot kezelhet, amelyek az adatkezelési cél szempontjából megfelelőek és meghatározóak. Tehát csak a ténylegesen szükséges adatokat kell és szabad kezelni.

II.4.2. Az elvhez kapcsolódó jogok

Az elv érvényesüléséhez közvetlenül kapcsolódó jog elsősorban az érintett hozzáférési joga.

II.5. A pontosság

II.5.1 A pontosság elve

A pontosság elvének érvényesítése során az intézménynek szem előtt kell tartania azt, hogy csak a helyes, pontos adatot kezelje, tartsa nyilván. Ennek érdekében törekedni kell:
- a kezelt adatok pontosságára,
- a naprakészség biztosítására,
- a szükséges törlések vagy helyesbítések elvégzésére.

II.5.2. Az elvhez kapcsolódó jogok

Az elv érvényesüléséhez közvetlenül kapcsolódnak az alábbi jogok:
- az érintett hozzáférési joga,
- a helyesbítéshez való jog,
- a törléshez való jog.

II.6. A korlátozott tárolhatóság

II.6.1. A korlátozott tárolhatóság elve

Az intézmény a korlátozott tárolhatóság elve érvényesítése érdekében szem előtt tarja, hogy a személyes adat tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.
(A további tárolás csak közérdekű archiválás, a tudományos és történelmi kutatási cél vagy statisztikai célból történhet.)

II.6.2. Az elvhez kapcsolódó jogok

Az elv érvényesüléséhez közvetlenül kapcsolódó jog az érintett hozzáférési joga.

II.7. Az integritás és bizalmas jelleg

II.7.1. Az integritás és bizalmas jelleg elve

Az integritás és bizalmas jelleg elve érdekében a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága. A megfelelő biztonság során gondoskodni kell:

- az adatok jogosulatlan vagy jogellenes kezelése,
- az adatok véletlen elvesztése,
- az adatok megsemmisítése vagy károsodása,

elleni védelemről.

II.7.2. Az elvhez kapcsolódó jogok

Az elv érvényesüléséhez közvetlenül kapcsolódó jog különösen: az érintett hozzáférési joga.

III. Az érintett jogai

III.1. Az érintett személyes adatokkal kapcsolatos jogai

Az érintett személyes adatokkal kapcsolatos jogai:

a) az átláthatóság és az érintett jogainak gyakorlására vonatkozó intézkedések körében:
- az átlátható tájékoztatáshoz és kommunikációhoz való jog, valamint
- a joggyakorlásra vonatkozó intézkedésekkel összefüggő jogok,

b) a tájékoztatás és a személyes adatokhoz való hozzáférés témakörében:
- az információkhoz való jog, ha a személyes adatokat az intézmény az érintettől gyűjti,
- információkhoz való jog, ha az adatokat az intézmény nem az érintettől szerzi meg,
- a hozzáférési jog,

c) a helyesbítés és törlés témakörében:
- a helyesbítéshez való jog,
- a törléshez való jog,
- az adatkezelési korlátozáshoz való jog,
- az adathordozhatósághoz való jog,

d) a tiltakozáshoz való jog és az automatizált döntéshozatal témakörében:
- a tiltakozáshoz való jog,
- az automatizált döntéshozatallal kapcsolatos jogok.

III.2. Az átlátható tájékoztatáshoz és kommunikációhoz való jog, valamint a joggyakorlásra vonatkozó intézkedésekkel összefüggő jogok

Az intézmény az átlátható adatkezelés érdekében - a jelen szabályzatban meghatározott intézkedéseket hozza - annak érdekében, hogy az érintett részére a személyes adatok kezelésre

vonatkozó valamennyi információ és tájékoztatás átlátható, érthető, világos, közérthető és tömör legyen.

Az intézménynek a fenti követelményt kell érvényesítenie az alábbi
a) információk tekintetében:
- az érintettől való közvetlen, illetve
- a nem közvetlenül az érintettől való
adatgyűjtése során;
b) a tájékoztatások tekintetében az érintett:
- a hozzáférési jogával,
- a helyesbítéshez való jogával,
- a törléshez való jogával,
- az adatkezelés korlátozásához való jogával,
- az adatkezelő értesítési kötelezettségével,
- az adathordozhatósághoz való jogával,
- a tiltakozáshoz való jogával,
- az adatvédelmi incidenssel kapcsolatos tájékoztatási jogával
kapcsolatos tájékoztatás alkalmával.

A tájékoztatás és információ átadás alkalmazott módjai:
- írásos,
- elektronikus út,
- szóbeli - ha az érintett személyazonosságának igazolása megfelelően megtörtént.

A joggyakorlás segítése

Az intézmény valamennyi dolgozója köteles elősegíteni az érintett egyes jogainak gyakorlását, így különösen:
- a hozzáférési jogával,
- a helyesbítéshez való jogával,
- a törléshez való jogával,
- az adatkezelés korlátozásához való jogával,
- az adatkezelő értesítési kötelezettségével,
- az adathordozhatósághoz való jogával,
- a tiltakozáshoz való jogával,
összefüggő joggyakorlást.

A tájékoztatás megadásának határideje

Az előző jogok gyakorlása iránti kérelem teljesítését az intézmény csak akkor tagadhatja meg, ha bizonyítható, hogy az érintettet nem lehet azonosítani. A tájékoztatás megtagadásáról az adatvédelmi tisztviselő dönthet.

Az érintett dolgozó a hozzá beérkező adatkezeléssel kapcsolatos kérelmet köteles haladéktalanul továbbítani az adatvédelmi tisztviselőnek, aki aktívan közreműködik a kérelmek teljesítésében, vagy közvetlenül teljesíti azokat.

Az adatkezeléssel kapcsolatos kérelmek alapján:
- a tájékoztatást a kérelem beérkezését követően haladéktalanul,

- ha a haladéktalan tájékoztatás nem lehetséges, akkor a kérelem beérkezésétől számított egy hónapon belül

meg kell adni.
Kivételes esetben lehetőség van a határidő két hónappal történő meghosszabbítására. Erről azonban tájékoztatni kell az érintettet a kérelem benyújtását követő 1 hónapon belül, megadva a határidő hosszabbítás okát, mely a következő lehet:

- a kérelem összetettsége,
- a benyújtott kérelmek száma.

A tájékoztatás elmaradása

Ha az intézmény a kérelmet valamely okból nem tudja teljesíteni, az adatvédelmi tisztviselő a kérelem beérkezésétől számított 1 hónapon belül tájékoztatja az érintettet a tájékoztatás elmaradásáról, valamint arról hogy panasszal élhet valamely felügyeleti hatóságnál, és élhet a bírósági jogorvoslati jogával.

Az információnyújtás és tájékoztatás megtagadása

Az intézmény nevében az adatvédelmi tisztviselő dönt az információ, illetve a tájékoztatás nyújtásának megtagadásáról akkor, ha a kérelem egyértelműen megalapozatlan vagy túlzó. Ebben az esetben az érintettel a kérelem benyújtását követő 1 hónapon belül közölni kell a kérelem megtagadásának okát.

Díj felszámítása

Az intézmény az információ nyújtás és tájékoztatás megtagadására okot adó körülmények esetén jogosult észszerű összegű díjat felszámítani a tájékoztatás, illetve információnyújtás miatt.

A díj felszámításáról, illetve összegéről az adatvédelmi tisztviselő dönt.

III.3. Az információkhoz való jog, ha a személyes adatokat az intézmény az érintettől gyűjti

III.3.1. Az információ biztosítás tartalma

Ha az intézmény az érintettre vonatkozó személyes adatokat közvetlenül az érintettől gyűjti, az intézmény, mint adatkezelő a személyes adatok megszerzésének időpontjában köteles az érintett rendelkezésére bocsátani az alábbi:

a) alapvető információkat:

- az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kilétét és elérhetőségeit,
- az adatvédelmi tisztviselő elérhetőségeit, ha van ilyen,
- a személyes adatok tervezett kezelésének célját, valamint az adatkezelés jogalapját,
- az adatkezelő vagy egy harmadik fél jogos érdekének érvényesítésén alapuló adatkezelés esetén, az adatkezelő vagy harmadik fél jogos érdekeit,

- adott esetben a személyes adatok címzettjeit, illetve a címzettek kategóriáit, ha van ilyen,

b) kiegészítő információkat (az adatkezelés tisztességének és átláthatóságának érdekében):

- a személyes adatok tárolásának időtartamát, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjait,
- az érintett azon jogát, 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,
- az érintett hozzájárulásán alapuló vagy az érintett különleges adatainak kezeléséhez kifejezett hozzájárulásán alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jogát, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
- a felügyeleti hatósághoz címzett panasz benyújtásának jogát;
- azt, 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;

- az automatizált döntéshozatal tényét ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információkat, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

III.3.2. Az információ biztosítás szükségtelensége

Az intézménynek nem kell biztosítani az információkat akkor, ha az érintett már a vonatkozó információkkal rendelkezik.

III.3.3. Az információ biztosításáért való felelősség

Az információk jelen szabályzat szerinti biztosításáért elsősorban az adatvédelmi tisztviselő felelős.

III.4. Az információkhoz való jog, ha az adatokat az intézmény nem az érintettől szerzi meg

III.4.1. Az információ biztosítás tartalma

Ha az intézmény a személyes adatokat nem az érintettől szerezte meg, köteles az érintett rendelkezésére bocsátani a következő:

a) alapvető információkat:

- az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kilétét és elérhetőségeit,
- az adatvédelmi tisztviselő elérhetőségeit, ha van ilyen,
- a személyes adatok tervezett kezelésének célját, valamint az adatkezelés jogalapját,
- az érintett személyes adatok kategóriáit,
- a személyes adatok címzettjeit, illetve a címzettek kategóriáit, ha van ilyen;

b) kiegészítő információkat:

- a személyes adatok tárolásának időtartamát, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjait,
- ha az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítésén alapul, az adatkezelő vagy harmadik fél jogos érdekeiről,
- az érintett azon jogát, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat a személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogát;
- az érintett hozzájárulásán alapuló vagy az érintett különleges adatainak kezeléséhez kifejezett hozzájárulásán alapuló adatkezelés esetén a hozzájárulás bármely időpontban való visszavonásához való jogát, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
- a valamely felügyeleti hatósághoz címzett panasz benyújtásának jogát,
- a személyes adatok forrását és adott esetben azt, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e; és
- az automatizált döntéshozatal tényét, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információkat, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

III.4.2. Az információ biztosítás határideje

Az intézmény nevében az adatvédelmi tisztviselő köteles az információkat az alábbi határidők betartásával biztosítani:
- alapesetben - a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, - a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül,
- ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával,
- ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor.

III.4.3. Az információ biztosítás szükségtelensége

Az intézménynek nem kell biztosítani az információkat akkor, ha:
- az érintett már a vonatkozó információkkal rendelkezik,
- az információ biztosítása lehetetlen,
- az adat megszerzését vagy közlését jogszabály írja elő.

III.4.4. Az információ biztosításáért való felelősség

Az információk jelen szabályzat szerinti biztosításáért elsősorban az adatvédelmi tisztviselő felelős.

III.5. A hozzáférési jog

III.5.1. Az információ biztosítás tartalma

Az érintett jogosult arra, hogy az intézménytől visszajelzést kapjon:
a) arról, hogy személyes adatainak kezelése folyamatban van-e,

b) a folyamatban lévő adatkezelés esetén az alábbi információkról:
- az adatkezelés céljairól;
- az érintett személyes adatok kategóriáiról,
- azon címzettek vagy címzettek kategóriáiról, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják,
- adott esetben a személyes adatok tárolásának tervezett időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól,
- az érintett azon jogairól, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen,
- a valamely felügyeleti hatósághoz címzett panasz benyújtásának jogáról,
- ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információról,
- az automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

III.5.2. Az információ biztosítás szabályai

Az intézmény adatvédelmi tisztviselője, vagy az általa adott ügyben felkért dolgozó az érintett kérelmére az adatkezelés tárgyát képező személyes adatokról másolatot készít és azt térítés nélkül a rendelkezésére bocsátja. A további másolatokért észszerű mértékű díjat lehet felszámítani. A díj felszámításáról, illetve a fizetendő díjról az adatvédelmi tisztviselő dönt.

III.6. A helyesbítéshez való jog

Az érintett jogosult arra, hogy kérésére az intézmény, mint adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat.
Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését is.

A helyesbítéssel kapcsolatos kérelemről, észrevételről az adatvédelmi tisztviselőt haladéktalanul értesíteni kell, aki áttekinti a kérelmet, és dönt a kérelem tárgyában.

III.7. A törléshez való jog

III.7.1. Az adatok törlése

Meghatározott feltételek fennállása mellett:
- az érintett joga, hogy kérje a rá vonatkozó személyes adatok törlését,
- az intézménynek, mint adatkezelőnek pedig kötelessége, hogy a személyes adatokat indokolatlan késedelem nélkül törölje.

Az adatokat akkor kell törölni, ha az alábbi indokok közül legalább egy fennáll:
- a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték,

- az érintett visszavonja az adatai kezelésre adott hozzájárulását vagy a különleges adatai kezelésére vonatkozó kifejezett hozzájárulását, és az adatkezelésnek nincs más jogalapja,
- az érintett tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,
- a személyes adatokat jogellenesen kezelték,
- a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell,
- a személyes adatok gyűjtésére az információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

III.7.2. Az adattörlési kötelezettség alóli kivételek

Az intézménynek nem kell törölni azokat az adatokat, melyek kezelése:
- a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából szükséges,
- a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó jogszabály szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából indokolt,
- a népegészségügy területét érintő közérdek alapján szükséges,
- a jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges.

III.7.3. Az adatok törlésével kapcsolatos felelősség

Az adatvédelmi tisztviselő dönt az érintettek adattörlési kérelmei ügyében, és szükség szerint intézkedik az adatok törléséről.

III.8. Az adatkezelési korlátozáshoz való jog

Az érintettnek joga van arra, hogy kérje, hogy az adatkezelő korlátozza a személyes adatai kezelését.

Az intézmény, mint adatkezelő az adatkezelés korlátozására irányuló kérést akkor köteles teljesíteni, ha az alábbi feltételek valamelyike teljesül:
- az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát,
- az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését és helyette kéri azok felhasználásának korlátozását,
- az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;
- az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Az adatkezelő az adatkezelési korlátozás feloldásáról köteles előzetesen tájékoztatni az érintettet.

Az adatvédelmi tisztviselő dönt az érintettek adatkezelési korlátozási joggal kapcsolatos kérelmei ügyében, és szükség szerint intézkedik az adatkezelés korlátozásáról.

III.9. Az adathordozhatósághoz való jog

Az érintett:
- a hozzájárulásán alapuló személyes adatkezelés,
- a kifejezett hozzájárulásán alapuló különleges adatok kezelése,
- a személyes adatok megadásával kötendő szerződések teljesítéséhez szükséges személyi adatkezelés,
- illetve az automatizált adatkezelés esetén

jogosult az adathordozhatóság jogának gyakorlására.

Az adathordozhatóság érdekében az érintett jogosult:
- hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja,
- arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta,
- arra, hogy kérésére az adatkezelő az adatokat közvetlenül másik adatkezelőnek továbbítsa akkor, ha ez technikailag megvalósítható.

Az érintett nem gyakorolhatja az adathordozhatósághoz való jogát:
- a közérdekű adatkezelés,
- vagy az adatkezelő közhatalmi feladatai ellátása keretében végzett adatkezelés

esetén.

Az adatvédelmi tisztviselő dönt az érintettek adathordozhatósági joggal kapcsolatos kérelmei ügyében, és teljesítendő kérelem esetében biztosítja az adathordozhatóságot. A tevékenységébe szükség esetén bevonja az adatkezelést ténylegesen végző személyt.

III.10. A tiltakozáshoz való jog

<u>A nem üzletszerzés érdekében történő adatkezeléssel kapcsolatos tiltakozási jog</u>
Az érintett joga, hogy a saját helyzetével kapcsolatos okokból tiltakozzon a személyes adatainak:
- közérdekű, vagy az intézmény rá ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához, illetve,
- az intézmény, vagy egy harmadik fél jogos érdekének érvényesítéséhez

szükséges adatkezelése ellen.

A tiltakozást követően:
- az intézmény az adatokat nem kezelheti tovább,
- csak akkor kezelheti tovább, ha az intézmény bizonyítja, az adatkezelés elsőbbségét az érintett jogaival szemben, vagy a jogi igények előterjesztéséhez, érvényesítéséhez, vagy védelméhez szükséges adatkezelés tényét.

<u>Az üzletszerzés érdekében történő adatkezeléssel kapcsolatos tiltakozási jog</u>
Az érintett joga, hogy ebben az esetben bármikor tiltakozzon a rá vonatkozó személyes adatok kezelése ellen.

Az adatvédelmi tisztviselő feladatai:
- megvizsgálja az érintettek adatkezeléssel kapcsolatos tiltakozását,
- a jogos tiltakozás alapján intézkedik arról, hogy az intézmény az adatokat tovább ne kezelje,
- a tiltakozás ellenére történő adatkezelés esetén írásban dokumentálja a további adatkezelés okait.

III.11. Az automatizált döntéshozatallal kapcsolatos jogok

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

Az adatvédelmi tisztviselő kivizsgálja az automatizált döntéshozatallal kapcsolatos jogok gyakorlására vonatkozó ügyeket, és gondoskodik e jog biztosításáról.

IV. Az adatkezelő

IV.1. Az adatkezelő feladatai

Az intézmény, mint adatkezelő feladata, hogy megfelelő:
- technikai és
- szervezési

intézkedéseket hozzon és működtessen.

Az intézkedések célja, hogy a személyes adatok kezelése:
- megfelelően történjen,
- és a megfelelő adatkezelés bizonyítható legyen.

Az intézmény adatkezeléssel kapcsolatos legfontosabb intézkedéseit a jelen adatvédelmi szabályzat tartalmazza, figyelemmel az adatkezelések:
- jellegére,
- hatókörére,
- körülményeire és céljaira, és
- a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatra.

A jelen szabályzatban meghatározott intézkedéseket, illetve a szabályzat alapján hozott intézkedéseket az intézmény:
- rendszeresen – eltérő rendelkezések hiányában évente – felülvizsgálja, és
- szükség szerint aktualizálja, naprakésszé teszi.

IV.2. Az adatvédelem

Az intézmény, mint adatkezelő az egyes adatkezelési intézkedéseket annak érdekében hozza meg, hogy:

- azok biztosítsák az adatvédelmi elveket,
- hozzájáruljanak a személyes adatkezelésre vonatkozó jogszabályi előírásokban meghatározott követelmények teljesítéséhez,
- az érintettek jogainak védelméhez szükséges garanciák beépítésre kerüljenek az adatkezelés folyamatába,
- kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott cél szempontjából szükségesek.

Az előbbiek érvényre jutása érdekében az intézmény gondoskodik arról, hogy:
- naprakész adatvagyon leltár álljon rendelkezésre,
- az adatkezelés az adatvagyon leltárban meghatározottak szerint történjen,
- az adatvagyon leltárban nem szereplő, új adatkezelési helyzetek vizsgálatra kerüljenek az adat és információ védelem szempontjaiból, és a vizsgálat eredményeképpen az adatkezelés megszüntetésre, törlésre kerüljön, vagy pedig felvételre kerüljön az adatvagyon leltárba,
- az adatvagyon leltár rendszeresen, de legalább 3 évente tartalmilag felülvizsgálatra kerüljön.

IV.2.1. Adatvagyon leltár

Az intézmény, mint adatkezelő az adatvédelmi szabályok betartása érdekében adatvagyon leltárt készít és azt folyamatosan aktualizálja.
Az adatvagyon leltárnak tartalmazni kell mindazokat az adatokat, amelyeket az intézmény kezel, függetlenül attól, hogy az hatósági ügy, vagy egyszerű tájékoztatás vagy akár az intézményhez érkező bejelentés, mely során adatok (nevek, címek, elérhetőségek stb.) feljegyzésre kerülnek.
Az adatvagyon leltár a teljesség, valamint a pontos feladat- és felelősség lehatárolása érdekében úgynevezett leltározási területenként készül.

IV.2.1.1. Az adatvagyon leltár területek

Az adatvagyon leltár területeket az adatvédelmi tisztviselő határozza meg, és vizsgálja felül legalább évente. (A felülvizsgálatot írásban - az adatvagyon leltár területei és felelősök dokumentumra feljegyzi.)
Az adatvagyon leltár elkészítésért felelős személyeket az adatvédelmi tisztviselő javaslatára az intézményvezető jelöli ki az *1. számú melléklet* alkalmazásával. Személyi változás esetén a kijelölést haladéktalanul meg kell tenni.

IV.2.1.2. Az adatvagyon leltár tartalma

Az adott területre vonatkozó adatvagyon leltárnak tartalmaznia kell:
- az adat, illetve adatbázis megnevezését,
- az adat, illetve adatbázis megjelenési formáját (papír alapú, elektronikus),
- az adatkezelés jogalapját (a szabályzat 5.2.2. pontja szerinti jogalapok szerint, jogszabályok esetén a pontos jogszabályi hivatkozás is),
- tárolási helyét (fizikai tárolási hely, illetve az elektronikus információs rendszer neve),
- az adatkezelő megnevezését,
- a biztonsági osztályba sorolását,

- az adat, adatbázis értékét (az adat, adatbázis becsült piaci értékét, ha van ilyen),
- az adatok felhasználási, feldolgozási folyamatait, eseményeit,
- az adathoz való hozzáférési jogosultságokat.

Az alkalmazandó adatvagyon leltár mintát a *2. számú melléklet* tartalmazza.

IV.2.1.3. Az adatvagyon leltár készítéséért felelős személyek

Az adatvagyon leltár elkészítéséért az adatvagyon területért felelős személyek tartoznak felelősséggel.
Az adatvédelmi tisztviselő a feladat ellátásához maximális szakmai támogatást nyújt, és elvégzi az adatbázisok biztonsági osztályba sorolását.

IV.2.2. Az adatok, adatbázisok biztonsági osztályba sorolása

Az intézmény, mint adatkezelő gondoskodik arról, hogy a kezelt adatok, adatbázisok biztonsági osztályba sorolása megtörténjen.

A biztonsági osztályba sorolás alapját a Magyarország kiberbiztonságáról 2024. évi LXIX. törvény, valamint a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet képezi azzal, hogy az intézmény ezen biztonsági osztályokat mint az elektronikus, mind a fizikai adatok és adatbázisok vonatkozásában egységesen alkalmazza.

A biztonsági osztályba sorolás a következő három biztonsági osztály alkalmazásával történik:

„Alap” biztonsági osztály

Az „alap” biztonsági osztály esetében legfeljebb csekély káresemény következhet be, mivel:

- az információs rendszerben jogszabály által nem védett adat vagy legfeljebb kis mennyiségű személyes adat sérülhet,
- a szervezet ügymenete szempontjából csekély értékű vagy csak belső (szervezeti) szabályzóval védett adat vagy rendszer sérülhet,
- a lehetséges társadalmi-politikai hatás a szervezeten belül kezelhető, vagy
- a közvetlen és közvetett anyagi kár a szervezet éves költségvetésének vagy nettó árbevételének 1%-át nem haladja meg.

„Jelentős” biztonsági osztály:

A „jelentős” biztonsági osztály esetében közepes káresemény következhet be, mivel:

- nagy mennyiségű személyes adat, illetve különleges személyes adat sérülhet,
- személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket),
- a szervezet ügymenete szempontjából érzékeny folyamatokat kezelő rendszer, információt képező adat vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet,

- a káresemény lehetséges társadalmi-politikai hatásai a szervezettel szemben bizalomvesztést eredményezhetnek, a jogszabályok betartása vagy végrehajtása elmaradhat, vagy a szervezet vezetésében személyi felelősségre vonást kell alkalmazni, vagy
- a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 1%-át, de nem haladja meg annak 10%-át.

„Magas" biztonsági osztály:

A „magas" biztonsági osztály esetében nagy káresemény következhet be, mivel

- különleges személyes adat nagy mennyiségben sérülhet,
- emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be,
- nemzeti adatvagyon helyreállíthatatlanul megsérülhet,
- az ország, a társadalom működőképességének fenntartását biztosító kritikus infrastruktúra rendelkezésre állása nem biztosított,
- a szervezet ügymenete szempontjából nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer vagy információt képező adat tömegesen vagy jelentősen sérülhet,
- súlyos bizalomvesztés állhat elő a szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok is sérülhetnek, vagy
- a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 10%-át.

IV.2.3. Az adatkezelés ellenőrzése

Az adatvédelmi tisztviselő rendszeresen, évente legalább 1 alkalommal ellenőrizni köteles, hogy az adatkezelés az adatvagyon leltárban meghatározottak szerint történik-e.

Az ellenőrzés során köteles közreműködni az adatvagyon leltár naprakészen tartásáért felelős személy.

Az adatvédelmi tisztviselő az adatkezelés ellenőrzéséről olyan nyilvántartást vezet, melyből egyértelműen megállapítható:
- az ellenőrzési kötelezettsége teljesítése,
- az, hogy az ellenőrzés talált-e nem megfelelőséget.

A nyilvántartást az áttekinthetőség érdekében adatvagyon leltár területenként külön-külön kell vezetni.
A nyilvántartás formáját a *3. számú melléklet - Az adatkezelési ellenőrzési nyilvántartás* tartalmazza.

A nem megfelelőség észleléséről, az intézkedésekről, és azok eredményeiről az adatvédelmi tisztviselő külön jegyzőkönyvet vesz fel.

IV.2.4. Új adatkezelési helyzetek

Az intézmény valamennyi adatot kezelő dolgozójának feladata, hogy közvetlenül ismerje a területéhez tartozó adatvagyont és annak adatvédelmi előírásait.
Ha a dolgozó a tevékenysége során adatvagyon leltárban nem szereplő, új adatkezelési helyzetet tapasztal, haladéktalanul értesíteni kell a területén az adatvagyon leltár elkészítéséért, naprakészen tartásáért felelős személyt.
Az érintett személy köteles megvizsgálni, hogy az új adatkezelési helyzet:
- valóban új adatkezelési helyzetet jelent,
- olyan adatkezelés körébe tartozik, ami tiltásra került, vagy
- beleillik egy korábban már meghatározott adatkezelési körbe.

Amennyiben az adatvagyon leltárért felelős személy véleménye szerint is új adatkezelési helyzet merült fel, haladéktalanul jelzi az adatvédelmi tisztviselőnek.

Az adatvédelmi tisztviselő ebben az esetben megvizsgálja az adatvédelmi hatásvizsgálat végzésének szükségességét, és indokolt esetben a hatásvizsgálatot elvégzi. /Lásd 32. pont./

IV.2.5. Az adatvagyon leltár felülvizsgálata

Az adatvédelmi tisztviselő felhívására az adatvagyon leltár elkészítéséért és naprakészen tartásáért felelős személy rendszeresen, de legalább 3 évente tartalmilag felülvizsgálja az adatvagyonleltárba felvett adatokat.
A felülvizsgálatnak ki kell térnie a nyilvántartásban szereplő valamennyi megállapításra, és ellenőrizni kell azok helytállóságát.

Az elkészült felülvizsgálatról jegyzőkönyvet kell felvenni.

IV.2.6. Az adatvagyon leltárba való felvétel tilalma

Az adatvédelmi tisztviselő felelős azért, hogy az adatvagyon leltárba ne szerepeljen olyan adatkezelés, amely nem felel meg az adatvédelmi előírásoknak, illetve amely vonatkozásában nem biztosítható a megfelelő védelem.

Az adatvagyon leltárba fel nem vehető adatok, adatbázisok körét a *4. számú melléklet* tartalmazza.

Az adatvagyon leltárba fel nem vehető adatokat, illetve adatbázisokat el kell távolítani.

IV.3. Adatkezelési nyilvántartás

Az intézmény, mint adatkezelő köteles a felelősségi körébe tartozón végzett adatkezelési tevékenységről nyilvántartást vezetni.

Az adatkezelési nyilvántartással kapcsolatban az adatvédelmi tisztviselő köteles:
- betartani a nyilvántartás tartalmi követelményeire vonatkozó jogszabályi előírásokat,
- a nyilvántartást naprakészen vezetni.

A nyilvántartást az *5. számú melléklet* szerinti formában kell vezetni.

Az intézmény adatkezelési nyilvántartásában - mivel 250 főnél kevesebb személyt foglalkoztat - azokat az adatkezeléseket kell nyilván tartani, amelyek:

- az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal járnak,
- során az adatkezelés nem alkalmi jellegű,
- kiterjednek a különleges adatokra,
- a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkoznak.

Az egyes adatkezelések nyilvántartásban való szerepeltetéséről az adatvédelmi tisztviselő dönt.

IV.4. Együttműködés a felügyeleti hatósággal

Az intézmény, mint adatkezelő együttműködik a felügyeleti hatósággal. A kapcsolattartásra elsősorban az intézményvezető és az adatvédelmi tisztségviselő jogosult.

V. Az adatfeldolgozó

V.1. Az adatfeldolgozó

Ha az adatkezelést az adatkezelő nevében más végzi, az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik, vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

Az adatkezelő köteles az adatfeldolgozóval olyan szerződést kötni, melyben szerepelnek a személyes adatok védelmével kapcsolatos garanciális szabályok.

A szerződések adatvédelmi szempontú előkészítését az adatvédelmi tisztviselő végzi. A szerződés tervezetet az intézményvezető hagyja jóvá.

VI. Adatbiztonság

VI.1. Általános adatbiztonsági követelmények

Az intézmény, mint adatkezelő az adatkezelés biztonsága érdekében - a jelen szabályzatban meghatározottak szerint - gondoskodik:

- a személyes adatok álnevesítéséről és titkosításáról,
- a személyes adatok kezelésére használt rendszerek és szolgáltatások:
    - folyamatos bizalmas jellegének biztosításáról,
    - integritásáról,
    - rendelkezésre állásáról és ellenálló képességéről,
- fizikai vagy műszaki incidens esetén az arra való képességről, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen állítani;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárásról.

Az intézmény az adatbiztonsági követelményeket különböző:
- adminisztratív,
- fizikai, illetve
- logikai

védelmi intézkedésekkel biztosítja.

VI.1.1. Az intézmény adminisztratív adatvédelmi intézkedései

Az intézmény adminisztratív adatvédelmi intézkedései keretében értelemszerűen alkalmazza az informatikai biztonsági szabályzatban meghatározott, és az adatok védelmére vonatkoztatható adminisztratív védelmi intézkedéseket.

Az intézmény adminisztratív adatvédelmi intézkedései körébe tartozik továbbá:
a) a szervezeti szinten ellátandó adminisztratív adatvédelmi tevékenység, ezen belül:
- kiadásra kerül a jelen *Adatvédelmi, adatbiztonsági és közzétételi szabályzat*, melyet az intézményvezető csak a hatályos adatvédelmi jogszabályhelyek tartalmi követelményeinek megléte esetén hagyhat jóvá,
- kijelölésre kerül az adatvédelmi tisztviselő, (a kijelölést a *6. számú melléklet* tartalmazza.)
- nyilvántartásra kerül az intézmény adatvagyona (ld. adatvagyon leltár),

b) az adatokkal kapcsolatos kockázatelemzést végez, ezen belül:
- működteti az előzetes adatvédelmi hatásvizsgálat rendszerét,
- megtiltja egyes adatok, adatbázisok kezelését,
- meghatározza az adatok adatvédelmi biztonsági osztályba sorolásának elveit,

c) a rendszer és szolgáltatás beszerzési alapfeladatok, melyek az adatok védelme érdekében az információ biztonsági szabályzatban meghatározottak szerint ellátásra kerülnek,
d) az ügymenet folytonosság tervezése érdekében az informatikai rendszerekkel érintett adatkezelésnél érvényesíteni kell az információ biztonsági szabályzatban meghatározott ügymenet folytonossági eljárásrendet, és tervet. Az elsődlegesen nem informatikai rendszerben kezelt, és felhasznált adatok esetében az adatokról olyan elektronikus másolatot kell készíteni, melynek a kezelése már informatikai rendszerben történik, s a rendszerek ügymenet folytonossága biztosítja az ilyen adatok tekintetében is az ügymenet folytonosságát.
e) a biztonsági események kezelésével összefüggő feladatok, ha azok adatvédelmi incidenst is jelentenek ezen belül különösen a nem informatikai rendszerben kezelt adattal összefüggő adatvédelmi incidens kezelésére a megfelelő eljárásrend meghatározása, (ld. *7. számú melléklet*)
f) az emberi tényezőket figyelembe vevő személyi biztonsági tevékenység, ezen belül személybiztonsági eljárásrend meghatározása, melyet a szabályzat *8. számú melléklete* tartalmaz.
g) a tudatossággal és képzéssel kapcsolatos alapvető feladatok ellátása a *9. számú melléklet* szerinti *Képzési eljárásrend* kerül kiadásra.

VI.1.2. Adatvédelmi incidens kezelése

Az incidenst követően az adatok visszaállíthatósága érdekében teendő intézkedéseket a jelen szabályzat *7. számú melléklete* az *Adatvédelmi incidens eljárásrendje* című melléklete tartalmazza.

VI.1.2.1. Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak

Az adatvédelmi incidenst a felügyeleti hatóságnak:
- nem kell bejelenteni, ha az incidens valószínűsíthetően nem jár kockázattal,
- be kell jelenteni, ha az incidens valószínűsíthetően kockázattal jár

a természetes személyek jogaira és szabadságaira nézve.

A bejelentés megtételének határideje

Az adatvédelmi incidens:
- indokolatlan késedelem nélkül,
- lehetőség szerint az incidens tudomására jutásától számított 72 órán belül

be kell jelenteni.

A bejelentésben:
- ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

VI.1.2.2. Adatvédelmi incidens nyilvántartás

Az adatvédelmi incidensről az intézmény, mint adatkezelő nyilvántartást vezet.
A nyilvántartásnak tartalmaznia kell:
- az incidens leírását,
- az incidenshez kapcsolódó tényeket,
- az incidens hatásait,
- az incidens orvoslására tett intézkedéseket.

A nyilvántartást az adatvédelmi tisztviselő vezeti.

VI.1.2.3. Az érintett tájékoztatása az adatvédelmi incidensről

Az intézmény, mint adatkezelő az érintetettet indokolatlan késedelem nélkül tájékoztatni köteles azokról az incidensekről, melyekkel kapcsolatban a felügyeleti szerv felé bejelentési kötelezettsége van.

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

Mellőzhető a tájékoztatás, ha:

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

VI.1.3. Az intézmény fizikai adatvédelmi intézkedései

Adat biztonsági osztálya	Fizikai védelmi intézkedés
„Alap”	- Az adatokat az adatkezelést követően az iratkezelés szabályai alapján kell tárolni. - Az adatokhoz való hozzáférést csak a hozzáférési jogosultságok szerint lehet biztosítani. - Az adatokat az adatkezelést követően zárható szekrényben, fiókban kell tárolni. - A számítógépet és okostelefont (függetlenül attól, hogy azt az intézmény biztosítja, vagy magáncélú eszköz), amelyen az e szabályzat szerinti adat merülhet fel (pl. munkahelyi e-mail fiók), használaton kívül zárolni kell, egyedi és biztonságos jelszóval. - Amennyiben az adatokat az intézményből munkavégzés céljából ki kell vinni, azokat úgy kell kezelni, hogy megismerésre jogosulatlanok ne férjenek hozzá: nem átlátszó mappában, nem látható (pl. gépjármű ülése) helyen szállítva és tárolva, az eszközt jelszóval lezárt állapotban. - Amennyiben az elektronikai eszközt intézményen kívüli használatra kell igénybe venni, úgy a felhasználónak tilos nyílt, jelszó nélküli vezeték nélküli hálózatra csatlakoznia. - A számítógépeken keletkezett és tárolt, az e szabályzat szerinti adatot tartalmazó fájlokról az intézmény által az adott szervezeti egység számára létrehozott szervermeghajtóra a feladatot végző munkatárs köteles havonta, manuálisan biztonsági mentést készíteni. - A számítógép használatára jogosult kolléga köteles az operációs rendszer, valamint a vírusirtó rendszeres, automatikus frissítését annak felmerülésének napján lehetővé tenni.
„Jelentős”	- Az Alap” biztonsági osztálynál leírtak, és - Az adatok intézményből történő kiszállítása az adatvédelmi tisztviselő jóváhagyásával történik.
„Magas”	- Az előző osztályokban leírtak, és - Az adatokat páncélszekrényben kell tárolni. - A tűzvédelmi előírások szigorítása az adat tárolással, és kezeléssel érintett helyiségekben. - A víz védelem biztosítása, - csővezetékek főelzáróhoz való

	hozzáférés biztosítása, illetve amennyiben adott helyiségben több ilyen osztályba sorolt adat kerül tárolásra, a csővezeték kiváltása, áthelyezése. - Az adatok intézményből történői kiszállításának intézményvezetői engedélyezése, írásban dokumentálása.

VI.1.3.1. Az adatok szállítása, intézményen kívüli kezelése

A nem informatikai rendszerben megjelenő személyes adatok esetén a dokumentumok **intézményből való kivitele, kezelése** csak indokolt esetben lehetséges. Az ilyen esetek meghatározását és feltételeit a *11. számú melléklet* szerinti minta alapján az adatvédelmi tisztviselő határozza meg az adatvagyon leltár adott területének összeállításáért felelős személy közreműködésével, adatvagyonleltár területenként külön-külön, és a jelen szabályzat mellékleteként kezeli.
A szállítási és intézményen kívüli kezelési előírásokat az adatvagyon leltár módosításakor felül kell vizsgálni. A felülvizsgálatért az adatvédelmi tisztviselő tartozik felelősséggel.

VI.1.4. Az intézmény logikai adatvédelmi intézkedései

Az intézmény logikai adatvédelmi intézkedései körébe tartoznak:
a) az elsődlegesen elektronikus informatikai rendszerben tárolt, kezelt adatok tekintetében az Informatikai Biztonsági Szabályzatban meghatározott logikai védelmi intézkedések, ezen belül:
- az általános védelmi intézkedések,
- a tervezés,
- a rendszer és szolgáltatás beszerzés,
- a biztonsági elemzés,
- a tesztelés, képzés és felügyelet,
- a konfigurációkezelés,
- a karbantartás,
- az adathordozók védelme,
- az azonosítási és hitelesítési eljárásrend,
- a hozzáférés ellenőrzése,
- a rendszer és információ sértetlenség, ezen belül többek között az álnevesítés és a titkosítás (kriptográfiai kulcs előállítása és kezelése, és kriptográfiai védelem),
- a naplózás és elszámolhatóság,
- a rendszer és kommunikáció védelem;

b) az elsődlegesen nem elektronikus informatikai rendszerben tárolt, kezelt adatok tekintetében:
- a papír alapú dokumentumokról készült másolatokat helyileg elkülönítetten, lehetőség szerint más személy felelősségi körébe kell kezelni,
- a másolatok fellelhetőségi helyét külön, idegen számára hozzá nem férhető módon kell rögzíteni,
- ha az adatok jelentős értéket képviselnek, az adatállományt nem egyben, egy helyen kell tárolni, hanem több helyen. (A fellelhetőségi helyeket itt is idegenek számára hozzá nem férhető módon kell rögzíteni.)

VI.1.4.1. Az adatok kezelésére használt rendszerek és szolgáltatások

Biztonsági szint

Az adatkezelés során használt rendszerek és szolgáltatások biztonsági szintje meghatározásának alapja az adatkezelésből eredő olyan kockázatok, amelyek a tárolt, továbbított, vagy egyéb módon kezelt adatok:

- véletlen vagy jogellenes:
  - megsemmisítéséből,
  - elvesztéséből,
  - megváltoztatásából,
- jogosulatlan nyilvánosságra hozatalból vagy az azokhoz való jogosulatlan hozzáférésből erednek.

Ezek a szempontok érvényesülnek a hivatkozott Információ biztonsági szabályzat szerinti biztonsági szint besorolásnál is.

Az adatkezelést végző személyek közvetlen felelőssége

Az intézmény a szabályzatban meghatározott intézkedéssel biztosítja azt, hogy az informatikai rendszerben tárolt és kezelt személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag a szabályzatnak megfelelően kezelhessék az érintett adatokat.

VII. Adatvédelmi hatásvizsgálat

VII.1. Adatvédelmi hatásvizsgálat

VII.1.1. Adatvédelmi hatásvizsgálat végzési kötelezettség

Az adatvédelmi tisztviselő köteles eldönteni, hogy adott adatkezeléssel kapcsolatban:

- kell-e hatásvizsgálatot végezni, vagy
- a hatásvizsgálat mellőzhető.

VII.1.1.1. Kötelező adatvédelmi hatásvizsgálat

Az intézmény, mint adatkezelő az adatkezelést megelőzően hatásvizsgálatot köteles végezni akkor:

- ha az adatkezelés valószínűleg magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, így különösen az alábbi esetekben:
  - a természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek,
  - az érintett kifejezett hozzájárulása alapján kezelt személyes adatok különleges kategóriái, vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése,
  - a nyilvános helyek nagymértékű, módszeres megfigyelése.

A hatásvizsgálat célja annak megállapítása, hogy a tervezett adatkezelési műveletek milyen hatást gyakorolnak a személyes adatok védelmére.

A hatásvizsgálatnak olyannak kell lennie, amely 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.

VII.1.1.2. Az adatvédelmi hatásvizsgálat mellőzése

Nem kell adatvédelmi hatásvizsgálatot végezni, ha egyértelmű, hogy az adott, adatkezelési művelet a természetes személyek jogaira és szabadságaira nézve nem jár magas kockázattal.
(Ha ez a kérdés egyértelműen nem dönthető el, akkor az adatvédelmi tisztviselőnek a hatásvizsgálat elvégzéséről kell döntenie.)
Az adatvédelmi tisztviselő az adatvédelmi hatásvizsgálat mellőzéséről adatkezelésenként külön- külön írásos jegyzőkönyvet készít, melyben rögzíti a hatásvizsgálat mellőzésének okait.
Az okok között szerepelhet, hogy:
- az adatkezelés valószínűsíthetően nem jár magas kockázattal,
- már készült hasonló adatvédelmi hatásvizsgálat, (ahol az adatkezelés jellege, hatóköre, körülménye és célja egymáshoz nagyon hasonló)
- az adatkezelésnek jogalapja van,
- az adatkezelés szerepel abban az adatvédelemmel kapcsolatban a felügyeleti hatóság által kiadott jegyzékben, melyre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni.

VII.1.2. Az adatvédelmi hatásvizsgálat elvégzése

Az adatvédelmi hatásvizsgálatot az adatkezelés megkezdése előtt el kell végezni a tervezett adatkezelési folyamatok alapján.
Az adatkezelés tervezett folyamatának változása esetén indokolt esetben az adatvédelmi hatásvizsgálat egyes lépéseit meg kell ismételni. (Ennek szükségességéről az adatvédelmi tisztségviselő dönt.)

Az adatvédelmi hatásvizsgálat az adatvédelmi tisztviselő irányításával történik, melyben részt vesz:
- a tényleges adatkezelést végző, illetve
- ha az adott adatkezelésben adatfeldolgozó is érintett, akkor az adatfeldolgozói is.

Az adatvédelmi tisztviselő dönt arról, hogy az adott ügyben az adatvédelmi hatásvizsgálattal érintettek, illetve a képviselőik véleményét:
- ki kell-e kérni, vagy
- nem.

Ha a vélemény kikérés mellett dönt, meghatározza azt, hogy a véleménykérés milyen módon, tartalomban, és arányban történjen.

Amennyiben arról dönt, hogy nem kell az érintettek, illetve képviselőik véleményét kikérni, írásban dokumentálja a döntésének okát.

Az adatvédelmi hatásvizsgálat tekintetében alkalmazható módszer leírását a *10. melléklet* tartalmazza.

VII.1.3. Az adatvédelmi hatásvizsgálat folyamata

Az adatvédelmi tisztviselő felelős azért, hogy az adatvédelmi hatásvizsgálat az alábbiak szerint - újra és újra - ismétlődő körfogásban megtörténjen az alábbiak tekintetében:

- a tervezett adatkezelés leírása,
- az adatkezelés szükségességének és arányosságának vizsgálata,
- már tervezett intézkedések,
- a természetes személyek adatvédelmemmel kapcsolatos jogait és szabadságait érintő kockázatok vizsgálata,
- a kockázatok kezelésére irányuló intézkedések,
- a dokumentáció,
- a nyomon követés és felülvizsgálat.

Az adatkezelés ellenőrzése
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.

VII.1.4. Az adatvédelmi hatásvizsgálat nyilvánosságra hozatala

Az adatvédelmi tisztviselő az intézményvezetővel egyetértésben dönt az adott adatvédelmi hatásvizsgálat nyilvánosságra hozataláról, ezen belül:

- a nyilvánosságra hozatal módjáról,
- a nyilvánosságra hozatal mértékéről (teljes, vagy részleges dokumentáció).

VII.2. Előzetes konzultáció

Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az adatvédelmi tisztviselő konzultál a felügyeleti hatósággal.

VIII. Az adatvédelem szervezeti háttere

VIII.1. A személyes adatok védelmével kapcsolatos szerepkörök

A személyes adatok védelmével kapcsolatos szerepkörök:
a) az elektronikus informatikai rendszerhez kapcsolódó adatok, adatbázisok, illetve adatkezelés esetén az információ biztonsági szabályzatban meghatározott szerepkörök.
Az érintetteknek a személyes adatok kezelés során azonban figyelembe kell venni az adatvédelmi tisztviselő adatvédelmi iránymutatásait is.

b) a nem elektronikus információ rendszerben tárolt, kezelt adatok, adatbázisok, illetve adatkezelés esetén:

- az intézményvezető,
- az adatvédelmi tisztviselő,
- az adatkezelést végző személy,
- más intézményi dolgozó.

VIII.1.1. Az intézményvezető

Az intézményvezető köteles gondoskodni a személyes adatok védelméről.

VIII.1.1.1. Az intézményvezető feladatai:

- a személyes adatok védelmét szolgáló jelen szabályzat kiadása,
- a helyi adatvédelmi, és adatkezeléssel összefüggő belső szabályzatok alapján az adatok összehangolt kezelési rendjének kialakítása és működtetése,
- a személyes adatok védelmével kapcsolatos alapelvek betartása és intézményen belül betartatása,
- a személyes adatok kezelésével érintett személyek jogai gyakorlásának elősegítése,
- a hozzá beérkező adatkezeléssel kapcsolatos kérelmek adatvédelmi tisztviselőnek való továbbítása,
- részvétel az adatvédelemmel kapcsolatos kötelező tájékoztatásban,
- az adatvagyon leltár elkészítéséért adott területen felelős személyek kijelölése,
- együttműködés és kapcsolattartás a felügyeleti hatósággal,
- az adatfeldolgozóval kötendő szerződés jóváhagyása,
- az adatvédelmi tisztviselő kijelölése,
- a szabályzatban meghatározott feladatok ellátása,
- a szabályzat mellékleteiben meghatározott tevékenységek ellátása.

VIII.1.1.2. Az adatvédelmi tisztviselő kijelölése

Az intézményvezető a *6. számú mellékletben* meghatározott személyt jelöli ki adatvédelmi tisztviselőnek.

Az adatvédelmi tisztviselő azért kerül kijelölésre, mert az intézmény az adatkezelést közfeladatot ellátó szervként végzi.

Az adatvédelmi tisztviselő kijelölésekor figyelembe vételre kerül:

- az tisztviselő szakmai rátermettsége,
- az adatvédelmi jog és gyakorlatban való szakmai jártassága,
- az adatvédelmi tisztviselőként ellátandó feladatok ellátására való alkalmassága.

Az adatvédelmi tisztviselő adatvédelmi feladatainak ellátási módja

Az intézményvezető az intézményben jelentkező adatvédelmi feladatok nagyságrendje alapján az adatvédelmi tisztviselőt úgy jelöli ki, hogy a tisztviselő köteles ellátni:

- az adatvédelmi tisztviselői feladatokat, illetve
- más, az intézményvezető által meghatározott munkaköri feladatokat is.

VIII.1.2. Az adatvédelmi tisztviselő

VIII.1.2.1. Az adatvédelmi tisztviselő jogállása

Az intézményvezető biztosítja az adatvédelmi tisztviselő függetlenségét, így:
- az adatvédelmi tisztviselő e tevékenysége során csak a vezetőnek van alárendelve,
- az adatvédelmi tisztviselőt e tevékenységében csak a vezető utasíthatja,
- az adatvédelmi tisztviselő a feladatai ellátásával összefüggésben nem bocsátható el és szankcióval nem sújtható.

Az adatvédelmi tisztviselő joga, hogy:
- a személyes adatok védelmével kapcsolatos minden ügybe megfelelő módon és időben bekapcsolódjon,
- az intézmény támogassa a feladatai ellátásában, így biztosítva legyen számára azok a források, melyek szükségesek:
    - a feladatai végrehajtásához,
    - a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint
    - az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához.

Az adatvédelmi tisztviselő kötelessége, hogy a feladatai teljesítésével kapcsolatban betartsa a titoktartási kötelezettséget, illetve az adatok bizalmas kezelésére vonatkozó kötelezettséget.

Az adatvédelmi tisztviselő olyan személy, akihez az érintettek szabadon fordulhatnak az adatvédelemmel kapcsolatos jogaik gyakorlásával összefüggésben.

VIII.1.2.2. Az adatvédelmi tisztviselő feladatai

Az adatvédelmi tisztviselő alap feladatai:
– Részt vesz a személyes adatok védelmének szabályzata kidolgozásában és felülvizsgálatában.
– Közreműködik az adatvédelmi alapelvek tartásában, érvényesítésében.
– Elősegíti az adatkezeléssel érintett személyek számára az egyes jogaik gyakorlását.
– Dönt az adatkezeléssel érintett tájékoztatás iránti kérelmének megtagadásában, illetve közreműködik a tájékoztatásban. Dönt az információ, illetve tájékoztatás biztosításával kapcsolatos díj felszámításáról, illetve a díj összegéről.
– Dönt az adathelyesbítési, törlési jog iránti kérelmekben. Szükség szerint intézkedik a törlésről.
– Dönt az érintettek adatkezelési korlátozási joggal kapcsolatos kérelmei ügyében, és szükség szerint intézkedik az adatkezelés korlátozásáról.
– Megvizsgálja az érintettek adatkezeléssel kapcsolatos tiltakozását.
– Jogos tiltakozás alapján intézkedik arról, hogy az intézmény az adatokat tovább ne kezelje.
– A tiltakozás ellenére történő adatkezelés esetén írásban dokumentálja a további adatkezelés okait.
– Közreműködik az adatvagyon leltár elkészítésében.
– Ellenőrzi, hogy az adatkezelés az adatvagyonleltár szerint történik-e.
– Tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban.
– ellenőrzi az adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését.

– Ellátja az adatvédelmi hatásvizsgálatra vonatkozó feladatokat,
– Együttműködik a felügyeleti hatósággal; Az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.
– Ellátja a jelen szabályzatban, valamint annak mellékleteiben meghatározott feladatokat.

VIII.1.3. Az adatkezelést végző személy

Az adatkezelést végző személy feladata:
- A szabályzatban meghatározott alapelvek betartása, érvényesítése az adatkezelés során.
- Elősegíteni az adatkezeléssel érintett személyeket abban, hogy az adatkezeléssel érintett egyes jogaikat gyakorolhassák.
- A hozzá érkezett adatkezelésre irányuló kérelmeket továbbítsa az adatvédelmi tisztviselőnek.
- Részvétel a személyes adatok kezelésével érintettek személyek tájékoztatási feladataiban.
- Az adatvédelmi tisztviselő kérésére közreműködni a személyes adatok kezelésével érintett személyek részére nyújtandó információk biztosításában.
- A hozzá érkezett adathelyesbítési kérelemről az adatvédelmi tisztviselő tájékoztatása.
- Közreműködni az adattörlésben, ha az érintett személy adattörlési joga érvényesítésre benyújtott kérelme alapján az adattörlésnek helye van.
- Közreműködni az adathordozhatósági jog érvényesítésében.
- Kijelölés alapján a területére vonatkozóan adatvagyonleltár elkészítése és vezetése.
- Új adatkezelési helyzet jelzése az adatvédelmi tisztviselőnek.
- Az adatvagyon leltár felülvizsgálata - ha kijelölés alapján köteles az adatvagyon leltár elkészítésére.
- Ellátja a jelen szabályzatban, valamint annak mellékleteiben meghatározott feladatokat.

VIII.1.4. Az adatkezelő nevében eljáró közalkalmazott és munkavállaló

Az adatkezelő nevében eljáró közalkalmazott és munkavállaló feladata:
- A szabályzatban meghatározott alapelvek betartása, érvényesítése a tevékenysége során.
- Elősegíteni az adatkezeléssel érintett személyeket abban, hogy az adatkezeléssel érintett egyes jogaikat gyakorolhassák.
- A hozzá érkezett adatkezelésre irányuló kérelmeket továbbítsa az adatvédelmi tisztviselőnek.
- Részvétel a személyes adatok kezelésével érintettek személyek tájékoztatási feladataiban.
- Az adatvédelmi tisztviselő kérésére közreműködni a személyes adatok kezelésével érintett személyek részére nyújtandó információk biztosításában.
- A hozzá érkezett adathelyesbítési kérelemről az adatvédelmi tisztviselő tájékoztatása.
- Új adatkezelési helyzet jelzése az adatvédelmi tisztviselőnek.
- Ellátja a jelen szabályzatban, valamint annak mellékleteiben meghatározott feladatokat.

VIII.2. A feladat és felelősség dokumentálása

A munkaköri leírás elkészítéséért felelős személy köteles gondoskodni arról, hogy a munkaköri leírásban meghatározásra kerüljenek:
- legalább a jelen szabályzatra való hivatkozással a személyi adatok védelmére vonatkozó általános védelmi feladatok és felelősségek,

- a konkrét feladat- és felelősségi előírások, ha az érintett munkakör jellege indokolja. Ebben az esetben is elegendő a jelen szabályzat meghatározott pontjaira, témakörére vonatkozó utalás.

A szabályzattal kapcsolat feladat- és felelősség dokumentálása megtörténik a szabályzat megismerési záradékának aláírásával, mely feltétele a jelen szabályzatban meghatározott feladatok, tevékenységének ellátásnak.

IX. Az intézménnyel foglalkoztatási jogviszonyban álló természetes személyek adatainak kezelése

IX.1. Általános szabályok

1. A munkavállalótól csak olyan adat közlése kérhető, amely személyiségi jogát nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges.
2. A munkaviszony létesítésekor a munkavállaló átadja a munkaszerződés megkötéséhez, illetve a munkáltató társadalombiztosítási bejelentési kötelezettsége teljesítése érdekében szükséges személyes adatait tartalmazó dokumentumokat, igazolványokat, melyeken található adatokról az Útkeresés Segítő Szolgálat munkatársa adatfelvételi lapot vesz fel.
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 *14. számú melléklet* tartalmazza.
6. A közalkalmazotti jogviszonyban állók adatkezelési tájékoztatóját a *13. számú melléklet* tartalmazza.
7. A Dunaújvárosi Gazdaságellátó Szervezetnél központosított illetményszámfejtés biztosítja az intézménynél foglalkoztatott közalkalmazottak, munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban állók személyi juttatásainak (illetmények és a jogviszony alapján járó egyéb juttatások), egészségbiztosítási ellátásainak (táppénz, GYED, terhességi gyermekágyi segély, baleseti táppénz), illetve a munkáltatókat terhelő közterheknek elszámolását.
8. A központi illetményszámfejtés a Magyar Államkincstár által biztosított, fejlesztett és működtetett számítógépes programon (a továbbiakban: illetményszámfejtő program) keresztül valósul meg.
9. Az intézmény A Dunaújvárosi Gazdaságellátó Szervezeten keresztül a Magyar Államkincstár felé dokumentumokat elsődlegesen elektronikusan küld meg. Eredeti – foglalkoztatottnak címzett, vagy a rendelkezése alatt álló - iratnak a Magyar Államkincstár felé történő megküldése csak a foglalkoztatott írásbeli hozzájárulása alapján és a Magyar Államkincstár előzetes írásbeli kérése alapján van lehetőség.
10. A munkavállalók részére az intézmény igazolványt bocsát a rendelkezésére, melyet a munkavállaló köteles intézkedése előtt az érintettnek bemutatni. Az igazolvány tartalmazza a munkavállaló nevét, az igazolvány azonosító számát, valamint az intézmény nevét, székhelyét, a kiállító aláírását és a hivatalos bélyegzőlenyomatát.
11. Megbízólevél kerül kiállításra az óvodai és iskolai szociális segítő tevékenységet végzők részére. *(20. sz. melléklet)*

IX.1.1. Mobiltelefon használatához kapcsolódó adatkezelési tevékenység

Az Útkeresés Segítő Szolgálat a munkavállalók meghatározott csoportja részére mobiltelefont bocsát rendelkezésre, hogy a munkavállalók ezen keresztül tartsák egymással a kapcsolatot, vagy a munkáltató képviseletében az ügyfelekkel, más személyekkel, szervezetekkel.

A mobiltelefonon tárolt és kezelt adatok védelme érdekében a munkavállaló köteles a mobiltelefonra számokból álló jelkódot beállítani. Ennek megalkotása során mellőzni kell az egyszerű, személyes adatokból könnyen kitalálható kombinációkat, pl. születési dátum. A munkavállaló a jelkódot lezárt borítékban köteles annak beállítását követően haladéktalanul átadni a a szakmai egységvezetőnek, amelyet a vezető elzártan őriz. A jelkód megváltoztatása a szakmai egységvezető előzetes engedélyével történik, amelyet követően az új jelkódot a munkavállaló ismét köteles a vezetőnek átadni.

A telefonon folytatott beszélgetések rögzítésére, a beszélgetésekbe történő belehallgatására, illetve a mobiltelefon tartózkodási helyének lekérdezésére nem kerül sor.

A pénzügyi elszámolás megkönnyítése érdekében a munkáltató adatokat gyűjthet a kimenő és bejövő hívások idejéről, időtartamáról, a beszélgető partner telefonszámáról a *Vezetékes és Mobiltelefon Használatának Szabályzata* elnevezésű intézményi szabályzatban rögzítettek szerint híváslista megküldésére kötelezheti a munkavállalót, illetve a dokumentumot megkérheti a szolgáltatótól.

IX.1.2. Az e-mail cím használatához kapcsolódó adatkezelési tevékenység

Az Útkeresés Segítő Szolgálat a munkatársak részére e-mail-címet tart fenn, hogy a foglalkoztatottak ezen keresztül tartsák egymással a kapcsolatot.

A foglalkoztatott rendelkezésére bocsátott e-mail fiók személyes levelezési célra nem használható.

Az e-mail fiókba történő belépési jelszót úgy kell képezni, hogy az biztonságosnak minősüljön. Biztonságos az a jelszó, amely minimum tíz karakterből áll,tartalmaz kis- és nagybetűt, valamint számot is. A jelszó megalkotásakor mellőzni kell a személyes adatok használatát (pl. név, születési adat, lakcím). Az e-mail fiók címét, valamint a hozzá alkotott jelszót a munkavállaló lezárt borítékban köteles a szakmai vezető részére átadni, aki azt elzárva őrzi. A jelszó megváltoztatására a szakmai egységvezető engedélye mellett a foglalkoztatott jogosult azzal, hogy az új jelszót lezárt borítékban köteles a szakmai egységvezető részére átadni.

Az e-mail fiókok ellenőrzésére nem kerül sor, azonban a munkáltató felhívhatja a foglalkoztatottat arra, hogy az e-mail fiókban tárolt üzeneteket végérvényesen törölje, melyre jellemzően a foglalkoztatott jogviszonyának megszűnése esetén kerül sor.

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.

IX.1.3. A számítógépek használatához kapcsolódó adatkezelési tevékenység

Az Útkeresés Segítő Szolgálat a munkatársak részére számítógépet vagy laptopot, és okostelefont tart fenn, meghatározott munkakörben foglalkoztatottak számára esetenként pendrive-ot is biztosít.
A foglalkoztatott rendelkezésére bocsátott eszközök személyes célra nem használhatóak.

Az intézményi számítógép vagy laptop bejelentkezési jelszavának megváltoztatására a foglalkoztatott nem jogosult.

Az eszközökön tárolt adatok külön nem kerülnek ellenőrzése, mivel a foglalkoztatott köteles a számítógép/laptop tartalmát havi egy alkalommal, minden hónap utolsó napján az intézmény szerverén a saját nevével készült mappába manuálisan átmásolni.

Amennyiben a munkáltatónak tudomására jut, hogy a foglalkoztatott személyes adatokat tárol a munkahelyi számítógépen/laptopon, pendrive-on, vagy okostelefonon, a munkáltató felszólíthatja a foglalkoztatottat azon adatok törlésére. A foglalkoztatottnak az adatok törlésére nyitva álló ideje 2 munkanap. A foglalkoztatott az engedély nélkül tárolt személyes adatainak a törlését úgy köteles végrehajtani, hogy az intézmény által kezelt adatok ne sérüljenek. Az intézmény informatikai karbantartását végző munkatárs segítsége igénybe vehető a törlés elvégzéséhez. A kötelezettség elmulasztása esetén a személyes adat az eszközökről törlésre kerül.

IX.2. Az intézménnyel jogviszonyban álló természetes személyek alkalmassági vizsgálataival kapcsolatos adatok kezelése

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.
A munkavállalók egészségügyi orvosi vizsgálaton vesznek részt.

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.

A foglalkoztatottakkal pszichológiai vagy személyiségjegyeket kutató tesztlapok kitöltethetőek, ha arra egyértelműen munkaviszonnyal kapcsolatos, a munkafolyamatok hatékonyabb ellátása, megszervezése érdekében kerül sor és amennyiben az elemzés során felszínre került adatok nem köthetők az egyes konkrét munkavállalókhoz, vagyis anonim módon történik az adatok feldolgozása.

A tréningeken, csapatépítéseken a különböző alkalmassági vizsgálatok keretén belül elvégzett személyiségtesztek megismerésére, tárolására, nyilvántartására nem kerül sor.

IX.3. Az intézménnyel foglalkoztatási jogviszonyban álló természetes személyek fényképeinek kezelése

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

X. Az intézményhez munkára jelentkezők személyes adataihoz kapcsolódó adatkezelési tevékenység

X.1. Általános szabályok

Az Útkeresés Segítő Szolgálat elkötelezett tevékenységének fejlesztése iránt, így a munkafolyamatokat a feladat ellátására legalkalmasabb munkavállalókkal kívánja elvégeztetni. A pályáztatási eljárás keretében az Útkeresés Segítő Szolgálat személyes adatokat kezel.

Az anonimizált álláshirdetések közzététele tilos. A betöltendő álláshelyek esetében az Útkeresés Segítő Szolgálat, mint jövőbeni foglalkoztató nevét fel kell tüntetni.

Az Útkeresés Segítő Szolgálathoz megérkező pályázatokat a pályázat benyújtására nyitva álló idő elteltéig a Munkaügyi ügyintéző 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 levélcímére megküldésre kerülnek.

Az Útkeresés Segítő Szolgálathoz megérkező pályázatokat a pályázat benyújtására nyitva álló idő elteltét követő 30. napig a Gazdasági és munkaügyi ügyintéző, az intézményvezető és a leendő munkáltatói jogkör gyakorló áttekinti. A pályázati anyagokról feljegyzések, az érintettről levont következtetések nem készülnek.
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.

A Munkaügyi ügyintéző a ki nem választott pályázókat a kiválasztás lezárását követően 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 *16. melléklet* szerinti értesítést kell megküldeni.

XI. Az intézményi alaptevékenységgel kapcsolatos adatkezelési előírások

Az intézmény dolgozói a feladataik teljesítése során a jogszabályok, a szakmai protokoll és az intézményi szabályzatok előírásait betartva kötelesek eljárni.

Az intézménnyel kapcsolatba kerülő ügyfelet azonosítani szükséges. Az azonosítás a személyi igazolvány, a lakcímkártya és a TAJ kártya elkérésével és megtekintésével valósul meg.

A dolgozók részére az intézmény által kiállított igazolványt - az ügyféllel történő első kapcsolatfelvétel alkalmával, illetve amikor az ügyfél kéri - be kell mutatni.

A személyazonosítására szolgáló igazolványok, egyéb iratok, dokumentumok másolására csak az adatkezelési tevékenységek nyilvántartásában megjelölt tevékenységeknél az ott megjelölt célból és alapon van lehetőség.

Az egyes tevékenységekhez tartozó adatkezelési tájékoztatókat a *15, 17, 18, 19 sz. mellékletek* tartalmazzák.

A szolgáltatást igénybe vevőket megilleti személyes adataik 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.

XI.1. Adattovábbítás

Az adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Az adattovábbítást megelőzően a szakmai vezető megvizsgálja a továbbítandó személyes adatok pontosságát, teljességét és naprakészségét.

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 rendelkezésére álló információkról és c) az adatvédelmi tisztviselő az adattovábbítás teljesíthetőségével egyetértett.

XI.1.1. Magyar Államkincstár felé történő adattovábbítás

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 27
c) az Szt. 20. § (2a) bekezdése szerinti adatszolgáltatás rendszerét.

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.

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.

XI.1.2. Gyermekeink védelmében elnevezésű informatikai rendszer

A Gyermekeink védelmében elnevezésű informatikai rendszer (a továbbiakban: GYVR) került bevezetésre a gyermekjóléti és a gyermekvédelmi ágazat működésének átláthatósága, a hatékonyság javítása, a gyorsabb, hatékonyabb szakmai kommunikáció és feladatellátás, valamint az adminisztrációs terhek és a papíralapú kommunikáció csökkentése érdekében.

A GYVR elektronikus felület fogja tartalmazni a család- és gyermekjóléti szolgáltatás és a gyermekek átmeneti gondozása igénybevevőinek meghatározott adatait, továbbá itt kell dokumentálni a szociális segítő munkát.

A GYVR-be történő bejelentkezés kizárólag IDM-en (Identitás Menedzseren) keresztül, ügyfélkapus azonosítással történhet.

A Kormány a GYVR adatkezelőjeként a minisztert jelölte ki, amely nem jelenti azt, hogy az intézmény által felvett és tárolt adatok tekintetében az intézmény ne lenne adatkezelő. A Központ látja el a GYVR-rel kapcsolatos adatfeldolgozási feladatokat, üzemelteti a GYVR-t, gondoskodik az adatbiztonsági követelmények teljesítéséről, és biztosítja az adatok hozzáférhetőségét az arra jogosultak számára. A Központ a GYVR üzemeltetése során biztosítja, hogy arra jogosulatlan személyek a nyilvántartásba vett adatokhoz ne férjenek hozzá. A GYVR-rel kapcsolatos eseményeket az informatikai rendszer folyamatosan, visszakereshető módon naplózza, ideértve az adatrögzítéssel nem járó adatlekérdezéseket is.

XI.2. Adományosztás

Az intézménnyel kapcsolatba kerülő ellátottal – amennyiben az adományokra jogosultság és az igény felmerül – hozzájáruló nyilatkozatot kell aláíratni, hogy az adományozható személyek nyilvántartásába felvételre kerülhessen.

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.

A nyilvántartásból adat az adatkezelési tevékenységek nyilvántartásában megjelölt célból továbbítható harmadik személy részére.

XI.3. Cégkapu működtetéséhez kapcsolódó adatkezelési rendelkezések

A digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól2023. évi CIII. törvény (továbbiakban: Dáp. tv.) 19. § (1) a) aa) alpontja értelmében a költségvetési szerv elektronikus ügyintézésre kötelezett.

A polgári perrendtartásról szóló 2016. évi CXXX. törvény 7. § 6. pontja értelmében a költségvetési szervek gazdálkodó tevékenységükkel összefüggő polgári jogi kapcsolataik vonatkozásában gazdálkodó szervezetnek minősülnek. Erre figyelemmel a költségvetési szerv a digitális szolgáltatások, a digitális állampolgárság szolgáltatások és támogató szolgáltatások részletes műszaki követelményeiről szóló 322/2024. (XI. 6.) Korm. rendelet értelmében cégkapu használatára jogosult.

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 szervezetből kik azok, akik dokumentumokat küldhetnek és fogadhatnak.

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).

A regisztrációt végző személy és a cégkapu-megbízott számára egyaránt előfeltétel, hogy az állam által kötelezően nyújtott azonosítási szolgáltatás útján (Ügyfélkapu, Részleges kódú telefonos azonosítás, Elektronikus személyazonosító igazolvány) azonosítsa magát.

Az intézménynél cégkapumegbízott csak az intézménnyel közalkalmazotti jogviszonyban álló személy lehet. A cégkapumegbízott nem kötelezhető az állam által kötelezően nyújtott azonosítási szolgáltatás azonosító adatainak az intézmény részére történő átadására.

XII. KÖZÉRDEKŰ ADATOK MEGISMERÉSÉRE VONATKOZÓ SZABÁLYOK

XII.1. Közérdekű adatok megismerése

Az intézmény közzétételi listáin nem szereplő közérdekű, vagy közérdekből nyilvános adatot bárki igényelhet írásban, elektronikus formában is.

XII.1.1 A közérdekű adat megismerésére irányuló igények benyújtásának módja

- írásban: Útkeresés Segítő Szolgálat 2400 Dunaújváros, Bartók Béla út 6/b.
- elektronikusan: utkereses.vezeto@gmail.com

Ha az adatigénylés nem egyértelmű, az intézmény felhívja az igénylőt az igénylés pontosítására. A szóbeli egyedi, azonnali teljesítéssel nem teljesíthető adatigénylést az átvevő munkatársnak írásba kell foglalnia. Az adatigénylésnek közérthetően és az adatigénylő által megjelölt módon kell eleget tenni.

Az írásbeli adatigényléseket a kézhezvétel után a lehető legrövidebb időn belül továbbítani kell az illetékes szervezeti egység vezetőjének véleményezésre. A megkeresett szervezeti egység vezetője az előkészített választ az intézményvezetőnek jóváhagyásra eljuttatja. A közérdekű adatigényléseknek a lehető legrövidebb idő alatt, legfeljebb 15 napon belül eleget kell tenni. Nagy terjedelmű, illetve nagyszámú adatigénylés esetén a határidő egy alkalommal legfeljebb 15 nappal meghosszabbítható, melyről az adatigénylőt a kérelem kézhezvételétől számított 8 napon belül tájékoztatni kell.

Amennyiben az adatigénylés olyan adat igénylésére vonatkozik, mely adatot nem az intézmény kezel, az adatigénylést haladéktalanul át kell tenni az adatot kezelő, közfeladatot ellátó, illetékes szerv vezetőjéhez. Abban az esetben, ha az illetékes szerv nem állapítható meg, az igénylőt erről az intézmény értesíti.

Az igény teljesítésének megtagadásáról és annak indokairól 8 napon belül a Intézmény levélben, vagy amennyiben az igény elektronikus úton érkezett, vagy ha – az igényben az elektronikus levelezési cím is fel van tüntetve – elektronikusan tájékoztatást küld az igénylőnek. Az igényelt adatokat tartalmazó dokumentumról vagy dokumentumrészről, annak tárolási módjától függetlenül az igénylő másolatot kap.
A másolat készítéséért költségtérítés állapítható meg, amelynek összegéről az igénylőt a teljesítést megelőzően az Intézmény tájékoztatja. A költségtérítés mértékét a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Korm. rendeletben előírtaknak megfelelően kell kiszámolni.
Ha jelentős terjedelmű a dokumentum vagy dokumentumrész iránt nyújtottak be igényt, a Szolgálat a másolatkérést a költségtérítés megfizetését követő 15 napon belül teljesíti. Az adatigénylést nem lehet elutasítani arra való hivatkozással, hogy annak közérthető formában nem lehet eleget tenni.

XII.2. Közérdekű adatok közzétételére vonatkozó szabályok

A kötelezően közzéteendő közérdekű adatokat a Szolgálat a közadatkereső rendszer (www.kozadat.hu) digitális formában, bárki számára, személyazonosítás nélkül, korlátozástól mentesen, kinyomtatható, és részleteiben is adatvesztés és –torzulás nélkül kimásolható módon, a betekintés, a letöltés, a nyomtatás, a kimásolás és a hálózati adatátvitel szempontjából is díjmentesen kell, hogy hozzáférhetővé tegye (a továbbiakban: elektronikus közzététel).
A közzétett adatok megismerése személyes adatok közléséhez nem köthető.

A Szolgálat saját honlapon közzé teszi, hogy az intézmény közérdekű adatai hol érhetők el.

Az intézményben foglalkoztatottak létszámára és személyi juttatásaira vonatkozó összesített adatokat minden negyedévet követő hó 15-ig, az elemi költségvetést és a költségvetési beszámolót pedig az irányító szerv általi jóváhagyást követően haladéktalanul meg kell küldeni az adatközlő felé, hogy az Intézmény az Info. Törvény előírásainak megfelelően közzé tudja tenni azokat.

XII.2.1. A közérdekű adatok közzétételének rendje

Az Info. törvény 37. § szerinti közzétételi listákon meghatározott adatait a Szolgálat a közadatkereső rendszerben – ha a törvény másként nem rendelkezik – a tv. 1. melléklete szerint (közzétételi lista) közzéteszi. A közzétételi listákon szereplő adatok pontos, naprakész és folyamatos közzétételéről az intézményvezető gondoskodik. Az intézményvezető, mint adatfelelős a közzéteendő adatokat adatközlőnek továbbítja.
Az Info. törvény. 35. § (4) bekezdése alapján az elektronikusan közzétett adatok – ha a tv. vagy más jogszabály eltérően nem rendelkezik – a honlapról nem távolíthatók el. A szerv megszűnése esetén a közzététel kötelezettsége a szerv jogutódját terheli. A közzéteendő közérdekű adatokat az adatfelelős elektronikus úton vagy elektronikus adathordozón juttatja el az adatközlőhöz. Az adatfelelősi feladatokat az intézményvezető, az adatközlő feladatokat az intézményvezető-helyettes látja el.
Az adatközlő az adatfelelőstől kapott adatokat az adatfelelős és a közzététel idejének megjelölésével közzéteszi. Az adatfelelős köteles az eljuttatott és a közzétett adatok egyezőségét ellenőrizni.

A Szolgálat gazdálkodásával összefüggő adatokat a GESZ gazdasági vezetője az Info. Törvény 1. sz. mellékletében szabályozottak szerint megküldi a Szolgálat vezetőjének, aki gondoskodik az adatok továbbításáról az adatközlőhöz.
Az irányító szerv 15/2015. (V. 22.) önkormányzati rendelet 4. melléklete szerinti egyedi közzétételi listában rögzítettekről a GESZ nyilvántartást vezet (gazdasági koordinátor feladata). A koordinátor a listát folyamatosan aktualizálja, a döntést követő hatvanadik napig frissíti és átadja a Szolgálat vezetőjének, aki gondoskodik a közzétételről.

A közzétett közérdekű adatok pontatlanná, tévessé vagy időszerűtlenné válása esetén, illetve ilyen közérdekű adatok feltárása esetén az adatfelelős állítja elő a helyesbített vagy frissített közérdekű adatokat tartalmazó, külön jogszabályban meghatározott közzétételi egységeket, és azokat közzététel végett átadja az adatközlőnek.

Az adatközlő köteles a közzétételre átadott közérdekű adatokat megvizsgálni. A közzététel végett átadott közérdekű adatok szükségessé való helyesbítése esetén az adatközlő erről értesítheti az adatfelelőst, de az átadott közérdekű adatokat ilyen szempont szerint nem köteles vizsgálni.

A frissített adat új állapota mellett fel kell tüntetni a frissítés tényét és idejét, illetve az adat előző állapotának archív állományban való elérhetőségét.
Az Info. Törvény végrehajtásával összefüggő kötelezettségek teljesítését évenkénti gyakorisággal vizsgálni szükséges, és arról átfogó jelentést kell készíteni.

A Szolgálat tevékenységéhez kapcsolódóan az Info. törvény 1. számú melléklete szerinti közzétételi listában meghatározott adatokat a szabályzat *12. sz. mellékletében* foglaltak szerint közzéteszi.

XIII. A szabályzat nyilvánossága

A szabályzat és a kapcsolódó mellékletek, nyilvántartások és egyéb dokumentumok nyilvánosságát a személyes adatok védelmi szempontok szem előtt tartásával kell biztosítani.
Az intézményvezető, illetve az adatvédelmi tisztviselő, a szabályzat egyes mellékletei, illetve egyes kapcsolódó dokumentumok és nyilvántartások tartalmának megismerését különböző feltételekhez kötheti.

A szabályzat érintettekkel való megismertetését megismerési záradékkal kell igazolni, mely tartalmazza azt, hogy a megismertetés a szabályzat mellékleteinek és csatolt dokumentumainak mely körére terjedt ki.

A szabályzat mindenki számára megismerhető részét közzé kell tenni, ennek keretében egy példányát ki kell függeszteni az intézmény hirdetőtáblájára.

Az intézményvezető és az adatvédelmi tisztviselő kiemelt feladata, hogy biztosítsa a szabályzat védelmét olyan információk tekintetében, melyek ismerete, nyilvánossága sértené, vagy veszélyeztetné a személyes adatok védelmének biztonságát.

XIV. A belső együttműködés szabályai

A személyes adatok védelmének biztosítása, valamint a jelen szabályzatban meghatározott elvek, jogok biztosítása, valamint a meghatározott intézkedések hatékonysága érdekében köteles együttműködni:

- az intézményvezető és az adatvédelmi tisztviselő,
- az adatvédelmi tisztviselő és az intézmény dolgozói.

Kiemelt szakmai együttműködés szükséges:
- az adatvédelmi tisztviselő, és az
- információbiztonsággal összefüggő feladatkört ellátók, így
- a biztonsági eseményt kivizsgáló személy között.

A biztonsági eseményt kivizsgáló személy: intézményvezető

Az adatvédelemmel érintett munkakört ellátóknak a tevékenységük során folyamatos:

- tájékoztatási,
- együttműködési,
- és tevékenység harmonizációs

kötelezettségük van.

Az együttműködésének jellemző formái:

- vezetői szóbeli vagy írásbeli utasítás,
- tájékoztatás,
- beszámoltatás,
- közös tevékenység.

XV. A szabályzat felülvizsgálata

A szabályzat teljes felülvizsgálatát legalább évenként el kell végezni. A szabályzat egyes részterületeit a szabályzatban meghatározott időnként, az általános felülvizsgálati időtől függetlenül el kell végezni.

Az adatvédelmi tisztviselő a szabályzat teljes, illetve egyes részeinek felülvizsgálatát köteles kezdeményezni és a felülvizsgálatot előkészíteni, ha azt a körülmények indokolják. A módosítást az intézményvezető írásban hagyja jóvá.

A jóváhagyást követően ismét gondoskodni kell a szabályzat megismertetéséről, illetve a szabályzat védendő adatainak védelméről.

XVI. Záró rendelkezések

A szabályzat annak elfogadása napján lép hatályba, és rendelkezéseit a szabályzat hatályon kívül helyezéséig kell alkalmazni.

Dunaújváros 2026. július 01.

Mészárosné Libor Ágnes
intézményvezető