Belváros-Lipótváros Egészségügyi Szolgálat

1051 Budapest, Hercegprímás utca 14-16.

Adatvédelmi szabályzat

Aláírás:	Molnár Gábor	L-TENDER Zrt. 3066 Kutasó, Toldi u. 4. Adószám: 27929560-2-12 Cg.szám: 12-10-001700 Bank:10401976-50525970-81661015
Szabályzatot készítette:	L-Tender Zrt.	

Aláírás:	Bacli Ágnes	Dátum:
Jóváhagyta:	Főigazgató	2025.01.01.

BELVÁROS-LIPÓTVÁROS EGÉSZSÉGÜGYI SZOLGÁLAT BLESZ 3 FŐIGAZGATÓ

Aláírás:	Dr Szentkirályi	Dátum: 2025.01.01.
Minőségügyi szempontból ellenőrizte:	Minőségirányítási vezető Dr Szentkirályi	2025.01.01.
Jogi szignó:	dr. Nagy József	

Dr. Nagy József
ügyvéd
1054 Bp. Széchenyi u. 8.
Bp. 1242 Pf. 472.

MÓDOSÍTÁSOK JEGYZÉKE

Változat száma	Módosította: név/dátum	Módosított oldalak/fejezetek száma:
1.		
2.		

Tartalomjegyzék

A Belváros-Lipótváros Egészségügyi Szolgálat (a továbbiakban: Intézet/Adatkezelő) a ***TEVÉKENYSÉG*** részletes szabályait az alábbiakban határozza meg:

Adatkezelő:

neve:	Belváros-Lipótváros Egészségügyi Szolgálat	
PIR szám:	505132	
adószám:	15505130-2-41	
székhelye:	1051 Budapest, Hercegprímás utca 14-16.	
e-elérhetősége:	info@blesz.hu	
képviselője:	Bádi Anikó főigazgató	
az Intézmény telephelyei:		
	1054 Budapest, Akadémia u. 8.	Ifjúság-egészségügyi szolgálat; iskolai védőnői szolgálat; iskolai védőnői ellátás; gyermek háziorvosi ellátás
	1052 Budapest, Semmelweis u. 14.	Felnőtt háziorvosi ellátás
	1053 Budapest, Kecskeméti u. 9.	Fogászati alapellátás (gyermekfogászat); fogászati alapellátás (iskolafogászat)
	1055 Budapest, Markó u. 7.	Fogászati alapellátás (gyermekfogászat); fogászati alapellátás (iskolafogászat)
	1056 Budapest, Váci u. 40.	Felnőtt háziorvosi ellátás
	1054 Budapest, Hold u. 8.	Felnőtt háziorvosi ellátás

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

1. A SZABÁLYZAT CÉLJA

Az Intézmény jelen Szabályzat megalkotásával és elérhetővé tételével biztosítani kívánja a GDPR 12. – 14. cikkében meghatározott megfelelő tájékoztatáson alapuló adatkezelés, valamint az Eütv. 24. §-ában meghatározott betegjogok megvalósulását, illetve hogy megfeleljen az Eüak.-ban meghatározott, az egészségi állapotra vonatkozó különleges személyes adatok és az azokhoz kapcsolódó személyes adatok kezelésének feltételeinek és céljainak.

Jelen Szabályzat célja, hogy az érintettek megfelelő tájékoztatást kaphassanak az Intézmény által kezelt, illetve az általa megbízott adatfeldolgozó által feldolgozott adatokról, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatkezelésbe esetlegesen bevont adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.

Jelen Szabályzattal az Intézmény biztosítani kívánja a nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, meg kívánja akadályozni az adatokhoz való jogosulatlan hozzáférést és azok jogosulatlan megváltoztatását, illetve nyilvánosságra hozatalát.

2. ALKALMAZÁSI TERÜLET

2.1. Szervezeti Hatálya

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

2.2. Személyi Hatálya

A Szabályzat személyi hatálya kiterjed:

- az Intézmény valamennyi egészségügyi és egészségügyben dolgozójára, valamint az Intézménnyel egyéb, munkavégzésre irányuló jogviszonyban álló természetes és jogi személyre,

- az Intézmény adatvédelmi tisztviselőjére,
- az egészségügyi szakemberképzés céljából a betegellátásban résztvevőkre,
- minden olyan, az Intézménnyel szerződéses vagy bármely jogviszonyban álló természetes és jogi személyre, aki a Szabályzat tárgyi hatálya alá tartozó személyes adatot kezel.

A Szabályzat időbeli hatálya 2025. január 1. napjától visszavonásig tart.

3. HIVATKOZÁSOK

3.1. Jogszabályok

Jelen Szabályzatban használt rövidítések:

OKFŐ	Országos Kórházi Főigazgatóság
Eüak.	az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény
Eütv.	az egészségügyről szóló 1997. évi CLIV. törvény
GDPR vagy Rendelet	az Európai Parlament és a Tanács (EU) 2016/679 rendelete
Infotv.	az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
Eszjtv.	az egészségügyi szolgálati jogviszonyról szóló 2020. évi C. törvény
Mt.	a munka törvénykönyvéről szóló 2012. évi I. törvény
Mvt.	a munkavédelemről szóló 1993. évi XCIII. törvény
NAIH vagy Hatóság	Nemzeti Adatvédelmi és Információszabadság Hatóság
NEFMI rendelet	az egészségügyi szakdolgozók továbbképzésének szabályairól szóló 63/2011. (XI. 29.) NEFMI rendelet
NM rendelet	62/1997. (XII. 21.) NM rendelet az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről
Ptk.	a polgári törvénykönyvről szóló 2013. évi V. törvény
Sztv.	a számvitelről szóló 2000. évi C. törvény
Szvtv.	a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény

3.2. Szervezeti és Működési Szabályzat

2025. január 1-jén hatályba lépett a Szervezeti és működési szabályzat (SZMSZ).

4. ILLETÉKESSÉG ÉS FELELŐSSÉG

4.1. A szabályzat kidolgozásáért felelős:

L-Tender Zrt.

4.2. A szabályzatban foglaltak alkalmazásáért felelős:

Az Intézményvezető az Intézmény sajátosságainak figyelembevételével meghatározza az adatvédelem szervezetrendszerét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket és kijelöli az adatkezelés felügyeletét ellátó személyt.

A Szabályzatban előírtak betartatásáért a feladatkörében minden érintett önálló szervezeti egység vezetője felelős, a szervezeti egységek vezetőjének munkáját szervezeti egységi adatvédelmi referens segíti.

4.3. A szabályzatban foglaltak alkalmazásának ellenőrzéséért felelős:

4.3.1. Az Intézményvezető az adatvédelemmel kapcsolatosan ellenőrzi:

- ellenőrzi az adatkezelők és adatfeldolgozók adatkezeléssel, illetve adatfeldolgozással összefüggő tevékenységét,
- ellenőrzi az adatvédelmi tisztviselő és az osztályos adatvédelmi referensek tevékenységét,

4.3.2. Az adatvédelmi tisztviselő ellenőrzi:

- ellenőrzi az adatvédelmi jogszabályoknak, valamint az Intézmény belső szabályzatainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyek tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;

4.3.3. Az Intézményi vezető adatvédelmi referens adatvédelemmel kapcsolatos feladatai során ellenőrzi:

- gondoskodik az adatvédelmi szabályok betartásáról, ellenőrzi az adatkezelést;

4.3.4. A szervezeti egységek osztályos adatvédelmi referense ellenőrzi:

- folyamatosan ellenőrzi a jelen Szabályzat előírásának betartását~~;~~

5. FOGALMAK, DEFINÍCIÓK

E Szabályzat alkalmazásában:

- **Érintett:** azonosított vagy azonosítható természetes személy (GDPR 4. cikk 1.);
  Az Érintett a jelen Szabályzat alkalmazásában az Intézmény által kezelt adatokkal érintett minden természetes személy, különösen az egészségügyi és egészségügyben dolgozó, a munkavállaló (együttesen: dolgozók), a gyermek, hozzátartozó, étkezést igénybe vevő, szerződő fél, kapcsolattartó stb.;
- **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 (GDPR 4. cikk 1.);
- **Személyes adat különleges kategóriái:** 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 (GDPR 9. cikk 1.);
- **Bűnügyi személyes adat:** a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat (Infotv. 3. § 4.);
- **Az érintett hozzájárulása:** az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez (GDPR 4. cikk 11.);
- **Érintett jogai, a Rendelet 12-21. cikkében szabályozott jogok:**
  - tájékoztatás joga,
  - hozzáférési jog,
  - helyesbítéshez való jog,
  - törléshez való jog,
  - adatkezelés korlátozhatóságához való jog,
  - adathordozhatósághoz való jog,
  - tiltakozáshoz való jog;
- **Tiltakozás:** az érintett jogosult arra, hogy saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a GDPR 6. cikk (1) bekezdésének e) vagy f) pontján alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is (GDPR 21. cikk (1) bekezdés);
- **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 (GDPR 4. cikk 7.);
- **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 (GDPR 4. cikk 2.);

- **Adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele (Infotv. 3. § 11.);
- **Nyilvánosságra hozatal:** az adat bárki számára történő hozzáférhetővé tétele (Infotv. 3. § 12.);
- **Adattörlés:** az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges (Infotv. 3. § 13.);
- **Adatkezelés korlátozásához való jog:**
  Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:
  a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;
  b) az adatkezelés jogellenes és az érintett ellenzi az adatok törlését, ehelyett kéri azok felhasználásának korlátozását;
  c) az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
  d) az érintett a 21. cikk (1) bekezdése szerint 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. [GDPR 18. cikk. (1)];

  Adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából (GDPR 4. cikk 3.);
- **Adatmegsemmisítés:** az adatot tartalmazó adathordozó teljes fizikai megsemmisítése (Infotv. 3. § 16.);
- **Adatfeldolgozás:** az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége (Infotv. 3. § 17.);
- **Adatfeldolgozó:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel (GDPR 4. cikk 8.);
- **Adatállomány:** az egy nyilvántartásban kezelt adatok összessége (Infotv. 3. § 21.);
- **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 (GDPR 4. cikk 10.);
- **EGT-állam:** az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez (Infotv. 3. § 23.);
- **Harmadik ország:** minden olyan állam, amely nem EGT-állam (Infotv. 3. § 24.);
- **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 (GDPR 4. cikk 12.);
- **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, technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni (GDPR 4. cikk 5.);
- **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 (GDPR 4. cikk 9.);
- **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 (GDPR 4. cikk 14.);
- **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 (GDPR 4. cikk 15.);
- **Egészségügyi dokumentáció:** a gyógykezelés során a betegellátó tudomására jutott egészségügyi és személyazonosító adatokat tartalmazó feljegyzés, nyilvántartás, vagy bármilyen más módon rögzített adat, függetlenül annak hordozójától vagy formájától [Eüak. 3. § e)];

- **Orvosi titok:** a gyógykezelés során az adatkezelő tudomására jutott egészségügyi és személyazonosító adat, továbbá a szükséges vagy folyamatban levő, illetve befejezett gyógykezelésre vonatkozó, valamint a gyógykezeléssel kapcsolatban megismert egyéb adat [Eüak. 3. § d)];
- **Közeli hozzátartozó:** a házastárs, az egyeneságbeli rokon, az örökbe fogadott, a mostoha- és nevelt gyermek, az örökbe fogadó, a mostoha- és nevelőszülő, valamint a testvér és az élettárs [Eüak. 3. § j)];
- **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 (GDPR 4. cikk 10.);
- **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 (GDPR 4. cikk 13.);
- **Nyilvántartási rendszer:** a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális, vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető (GDPR 4. cikk 6.);
- **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 (GDPR 4. cikk 4.);
- **Releváns és megalapozott kifogás:** a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy 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 (GDPR 4. cikk 24.);
- **Felügyeleti Hatóság:** egy tagállam által a GDPR 51. cikkének megfelelően létrehozott független közhatalmi szerv (GDPR 4. cikk 21.);
- Az Infotv. 38. § (2a) alapján a GDPR-ban a felügyeleti hatóság részére megállapított feladat- és hatásköröket a Magyarország joghatósága alá tartozó jogalanyok tekintetében GDPR-ban, valamint az Infotv-ben meghatározottak szerint a NAIH gyakorolja.
- **Érintett felügyeleti Hatóság:** az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint:
  a) az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság 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

  (GDPR 4. cikk 22.);
- **Az információs társadalommal összefüggő szolgáltatás:** az (EU) 2015/1535 európai parlamenti és tanácsi irányelv 1. cikke (1) bekezdésének b) pontja értelmében vett szolgáltatás (GDPR 4. cikk 25.);
- **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 (GDPR 4. cikk 26.).

Amennyiben a mindenkori hatályos adatvédelmi jogszabályok (jelen Szabályzat megalkotásakor az Infotv. és a GDPR) fogalommagyarázatai eltérnek jelen Szabályzat fogalommagyarázataitól, akkor a jogszabályok, elsősorban a GDPR által meghatározott fogalmak az irányadók.

6. A SZABÁLYZAT LEÍRÁSA

A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
b) 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;
c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

f) 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.

Az Intézmény a faji, vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatokat, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatokat, továbbá egészségügyi adatokat és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatokat (a továbbiakban együtt: a személyes adatok különleges kategóriái) a GDPR tiltása alapján nem kezel, kizárólag abban az esetben, ha a GDPR 9. cikk (2) bekezdésében foglaltak alapján a tilalom alól az alábbiak szerint mentesül.

A személyes adatok különleges kategóriájába eső adatokat az Intézmény az alábbi esetekben kezelheti:
a) az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha az uniós vagy tagállami jog úgy rendelkezik, hogy a fenti tilalom nem oldható fel az érintett hozzájárulásával;
b) 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 uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi;
c) 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;
d) az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára;
e) az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
f) az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el;
g) az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog 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;
h) 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, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, továbbá a GDPR 9. cikk (3) bekezdésben említett feltételekre és garanciákra figyelemmel;
i) az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechnikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan;
j) az adatkezelés a GDPR 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós vagy tagállami jog 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 információs önrendelkezés minden természetes személy Alaptörvényben rögzített alapjoga, így az Intézmény az eljárásai során csak és kizárólag a hatályos jogszabályok rendelkezései alapján végez adatkezelést.

Az Intézmény által kezelt személyes adatok magáncélra való felhasználása tilos.

Az Intézmény az adat felvétele előtt minden esetben közli az érintettel az adatkezelés célját, valamint az adatkezelés jogalapját.

Az Intézménynél adatkezelést végző és az Intézmény megbízásából az adatkezelésben részt vevő, annak valamely műveletét végző szervezet alkalmazottja köteles a megismert személyes adatokat az Eüak. szerinti orvosi titokként megőrizni. A személyes adatokat kezelő és azokhoz hozzáférési lehetőséggel rendelkező személyeket jogszabályban rögzített (Eüak.) titoktartási kötelezettség terheli.

Ha a Szabályzat hatálya alatt álló személy tudomást szerez arról, hogy az Intézmény által kezelt személyes adat hibás, hiányos vagy időszerűtlen, köteles azt helyesbíteni vagy helyesbítését az Intézményvezetőnél kezdeményezni.

Az Intézmény megbízásából adatfeldolgozói tevékenységet végző természetes, vagy jogi személyekre, illetve jogi személyiséggel nem rendelkező szervezetekre vonatkozó adatvédelmi kötelezettségek az adatfeldolgozóval kötött szerződésben érvényesítendők. Az adatfeldolgozóval az Intézmény a GDPR 28. cikk (3) bekezdése által előírt szerződést köthet.

Az Intézmény személyes adatot csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezel, a cél eléréséhez szükséges minimális mértékben és ideig. Az adatkezelés minden szakaszában meg kell felelnie a célnak – és amennyiben az adatkezelés célja megszűnt, vagy az adatok kezelése egyébként jogellenes, az adatok törlésre kerülnek. A törlésről az Intézménynek az adatot ténylegesen kezelő munkavállalója gondoskodik a törlés engedélyezésére jogosult személy jóváhagyását követően. A törlést a munkavállaló felett munkáltatói jogköröket ténylegesen gyakorló személy és – az adatvédelmi tisztviselő ellenőrizheti.

Amennyiben a személyes adat kezelése az egészségügyi dokumentációban történik, úgy a már felvett egészségügyi adatot csak és kizárólag úgy szabad kijavítani vagy törölni, hogy az eredetileg felvett adat megállapítható legyen.

Az Intézmény személyes adatot csak az érintett előzetes – különleges személyes adat esetén írásbeli – hozzájárulása vagy törvény, illetve törvényi felhatalmazás alapján kezel.

Az Intézmény az adat felvétele előtt minden esetben közli az érintettel az adatkezelés célját, valamint az adatkezelés jogalapját.

Az Intézmény szervezeti egységeinél adatkezelést végző foglalkoztatottak és az Intézmény megbízásából az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek alkalmazottjai kötelesek a megismert személyes adatokat bizalmasan kezelni és üzleti titokként megőrizni. A személyes adatokat kezelő és azokhoz hozzáférési lehetőséggel rendelkező személyek kötelesek ***Titoktartási nyilatkozatot*** tenni.

Ha a Szabályzat hatálya alatt álló személy tudomást szerez arról, hogy az Intézmény által kezelt személyes adat hibás, hiányos vagy időszerűtlen, köteles azt helyesbíteni vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.

Az Intézmény megbízásából adatfeldolgozói tevékenységet végző természetes vagy jogi személyekre, illetve jogi személyiséggel nem rendelkező szervezetekre vonatkozó adatvédelmi kötelezettségeket az adatfeldolgozóval kötött megbízási szerződésben érvényesítendőek. Az adatfeldolgozóval az Intézmény az GDPR által előírt ***Adatfeldolgozói szerződést*** köt. Az egyéb szerződésekbe felveendő adatkezelési pontokat jelen Szabályzat 19. sz. melléklete tartalmazza.

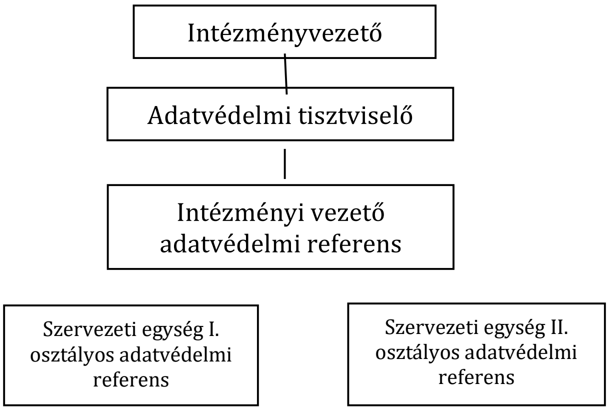
6.1. Az Intézmény adatvédelmi rendszere

Az Intézményvezető az Intézmény sajátosságainak figyelembevételével meghatározza az adatvédelem szervezetrendszerét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket és kijelöli az adatkezelés felügyeletét ellátó személyt.

A Szabályzatban előírtak betartatásáért a feladatkörében minden érintett önálló szervezeti egység vezetője felelős, a szervezeti egységek vezetőjének munkáját szervezeti egységi adatvédelmi referens segíti.

Az Intézmény az alábbi adatvédelmi rendszert alkotja meg:

- az Intézményvezető a 20 főnél több betegellátó személyt alkalmazó szervezeti egységek—élére adatvédelmi referenst jelöl ki,
- a szervezeti egységek adatvédelmi referenseinek munkájának koordinálását az Intézményi vezető adatvédelmi referense végzi,
- a szervezeti egységek adatvédelmi referensei a saját szervezeti egységükön végzett adatkezelési feladatokat felügyelik, az adatvédelmi tisztviselő a szervezeti egységek adatvédelmi referensek munkáját ellenőrzi és fogja össze közvetlenül, vagy az Intézményi vezető adatvédelmi referensen keresztül.



Az Intézményvezető az adatvédelemmel kapcsolatosan:

a) gondoskodik az adatvédelmi szabályok betartásáról, így különösen
   - biztosítja az érintettek GDPR-ban és Eüak-ban meghatározott jogainak gyakorlásához szükséges feltételeket;
   - ellenőrzi az adatkezelők és adatfeldolgozók adatkezeléssel, illetve adatfeldolgozással összefüggő tevékenységét,
b) felelős az Intézmény által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért;
c) felelős az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért;
d) vizsgálatot rendelhet el;
e) kiadja az Intézmény adatvédelemmel kapcsolatos belső szabályait
f) kezdeményezi az adatvédelem, illetve az adatbiztonság területén kifejlesztett új technológiák és eszközök alkalmazását,
g) biztosítja az adatkezeléssel és adatfeldolgozással foglalkozó személyek adatkezelési oktatását,
h) tudományos kutatás esetén engedélyezi az egészségügyi dokumentációba való betekintést, illetőleg az adatgyűjtést,
i) kijelöli az adatvédelmi tisztviselőt, az intézményi vezető adatvédelmi referenst és az osztályos adatvédelmi referenseket,
j) ellenőrzi az adatvédelmi tisztviselő és az osztályos adatvédelmi referensek tevékenységét,
k) gondoskodik az intézmény adatvédelmi szabályzatának elkészítéséről,
l) dönt a kötelező nyilvántartási időt követően a nyilvántartott adatok további tárolásáról vagy megsemmisítéséről.

Az Intézményvezető az alábbi feladatokat a munkajogi előírások által előírt módon az adatvédelmi tisztviselőnek delegálhatja:
a) gondoskodás az adatvédelmi szabályok betartásáról
b) az adatkezelők és adatfeldolgozók adatkezeléssel, illetve adatfeldolgozással összefüggő tevékenységének ellenőrzése,
c) az adatvédelem, illetve az adatbiztonság területén kifejlesztett új technológiák és eszközök alkalmazásának kezdeményezése,
d) az adatkezeléssel és adatfeldolgozással foglalkozó személyek adatkezelési oktatásának biztosítása

6.1.1. Az adatvédelmi tisztviselő

Az adatvédelmi tisztviselő adatvédelemmel kapcsolatos feladatai:
a) ellátja a számára az Intézményvezető által delegált feladatokat,
b) segítséget nyújt az érintettek és betegek személyes adatok védelméhez fűződő jogainak biztosításában;
c) minden év január 15-ig jelentést készít az Intézmény vezetőjének részére az Intézmény adatvédelmi feladatainak végrehajtásáról,
d) jogosult jelen Szabályzat előírásainak betartását Intézményi szinten és egyes szervezeti egységeknél ellenőrizni;
e) vezeti a belső adatkezelési és adattovábbítási nyilvántartást;

f) részt vesz a NAIH által szervezett adatvédelmi tisztviselők konferenciáján;
g) figyelemmel kíséri az adatvédelemmel kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi jelen Szabályzat módosítását;
h) tájékoztatást és szakmai tanácsot ad az Intézmény adatvédelmi jogszabályokban előírt kötelezettségeinek ellátásával kapcsolatban az Intézmény vezetőjének, valamint az Intézmény alkalmazottai részére;
i) ellenőrzi az adatvédelmi jogszabályoknak, valamint az Intézmény belső szabályzatainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyek tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
j) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
k) közreműködik a NAIH-tól az Intézményhez érkezett megkeresések megválaszolásában és a NAIH által kezdeményezett vizsgálat, illetve adatvédelmi hatósági eljárás során;
l) általános állásfoglalás megadása céljából megkeresést fogalmaz meg a NAIH felé, amennyiben egy felmerült adatvédelmi kérdés jogértelmezés útján egyértelműen nem válaszolható meg.
m) Az adatvédelmi tisztviselő a csatlakozott adatkezelőktől és az EESZT felhasználóktól adatot, dokumentumot vagy tájékoztatást kérhet. A kért adatot, dokumentumot vagy tájékoztatást soron kívül, de legkésőbb öt munkanapon belül az adatvédelmi tisztviselő rendelkezésére kell bocsátani.

Az adatvédelmi tisztviselő a b), c)-g) e) pontban meghatározott feladatokat az Intézményi Vezető Adatvédelmi referensen keresztül, az osztályos adatvédelmi referenseinek delegálhatja a saját szervezeti egységük tekintetében.

Az osztályos adatvédelmi referens fentiek meghiúsulása esetén értesíti a fegyelmi jogkör gyakorlóját.

6.1.2. Az Intézményi vezető adatvédelmi referens adatvédelemmel kapcsolatos feladatai:

a) felelős az intézmény adatvédelmi szervezetéért, koordinálja az osztályos adatvédelmi referens tevékenységét;
b) kapcsolatot tart az adatvédelmi tisztviselővel;
c) amennyiben az Intézmény működésében olyan változások történnek, amelyek magánszemélyek adatainak kezelését érintik, az adatvédelmi tisztviselővel közösen gondoskodik az Intézmény adatvédelmi szabályzatának módosításáról;
d) gondoskodik az adatvédelmi szabályok betartásáról, ellenőrzi az adatkezelést;
e) az Intézmény adatvédelmi szabályzatát érintő kérdésekben beszámol az Intézmény vezetőjének;
f) gondoskodik az Intézmény székhelyére érkezett magánszemélyek, hatóságok és bíróságok egészségügyi dokumentáció másolatának kiadására vonatkozó, valamint a fenntartó, hatóságok és bíróságok betegekkel kapcsolatos - az egészségügyi dokumentáció alapján - teljesíthető betegadatok adatkiadásra vonatkozó megkeresései megválaszolásáról;

6.1.3. A szervezeti egységek osztályos adatvédelmi referensei

A szervezeti egység osztályos adatvédelmi referense a saját szervezeti egységében:
a) segítséget nyújt az érintettek és betegek személyes adatok védelméhez fűződő jogainak biztosításában;
b) vezeti a szervezeti egység adatkezelési és adattovábbítási nyilvántartását;
c) folyamatosan ellenőrzi a jelen Szabályzat előírásának betartását~~;~~
d) köteles minden olyan jelzést az intézmény adatvédelmi tisztviselője irányába megtenni, amely az adatvédelmi rendszerben történő jogtalan behatolással, illetőleg az adatvédelmi rendszer tárolási hiányosságaival áll összefüggésben

6.2. Az informatikáért felelős személy

A 2025. január 1-jén hatályba lépett SZMSZ alapján az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Az elektronikus információs rendszer biztonságáért felelős személy feladatait, szerződés alapján külső szolgáltató látja el.

Ennek körében gondoskodik:
a) a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról;
b) elvégzi vagy irányítja tevékenységek tervezését, szervezését, koordinálását és ellenőrzését;

c) előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot;
d) előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását;
e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit;
f) kapcsolatot tart a hatósággal és az eseménykezelő központtal;

6.3. Az Intézmény betegellátó személyeinek és munkatársainak feladata

Az Intézmény betegellátó személyei és munkatársai munkájuk során gondoskodnak arról, hogy jogosulatlan személyek ne tekinthessenek be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

6.4. Adatvédelmi incidens kezelése

6.4.1. Adatvédelmi incidens észlelése és jelentése

Az Intézmény minden munkavállalója – beleértve az egyéb jogviszonyban foglalkoztatott személyeket is – köteles az Intézményen belül történt adatvédelmi incidenst haladéktalanul jelenteni a szervezeti egysége vezetőjének útján az Intézmény főigazgatójának, valamint az adatvédelmi tisztviselőnek. A bejelentés tartalmazza a bejelentő nevét, telefonszámát, beosztását, szervezeti egységének megnevezését, valamint az incidens tárgyát, rövid leírását és azt, hogy az incidens érinti-e az Intézmény informatikai rendszerét.

6.4.2. Adatvédelmi incidens kivizsgálása, értékelése

Az adatvédelmi tisztviselő – informatikai rendszert érintő incidens esetén bevonja az informatikáért felelős személyt – megvizsgálja a bejelentést és amennyiben szükséges, a bejelentőtől további adatokat kér az incidensre vonatkozóan. Az adatvédelmi tisztviselő felhívására a bejelentő köteles megadni: az adatvédelmi incidens bekövetkezésének időpontját és helyét, egyéb körülményeit, az érintett adatok körét, mennyiségét, az érintett személyek körét és számát, várható hatásait, az adatvédelmi incidens megelőzésére, következményeinek enyhítésére megtett intézkedések felsorolását.

A bejelentő az adatszolgáltatást haladéktalanul, de legkésőbb 24 órán belül teljesíti az adatvédelmi tisztviselő részére.

Az Intézet az adatvédelmi incidenseket három kategóriába sorolja:
- 1. kategória: valószínűsíthetően kockázattal nem járó incidens (nem kell NAIH-nak jelenteni)
- 2. kategória: valószínűsíthetően alacsony kockázattal járó incidens (NAIH-nak be kell jelenteni)
- 3. kategória: valószínűsíthetően magas kockázattal járó incidens (az érintettet is tájékoztatni kell)

Az Intézet az adatvédelmi incidenst az alábbi szempontok szerint értékeli:
- az incidens típusa (bizalmassági, integritási vagy elérhetőségi),
- a személyes adatok jellege (személyes adat / különleges kategória),
- a személyes adatok száma,
- az érintett személyek száma,
- az érintett természetes személyek kategóriái,
- az érintett természetes személyek azonosíthatósága,
- a természetes személyre nézve fennálló következmények valószínűsége és súlyossága;
- az érintett adatkezelés jogalapja.

Az Intézet az incidens értékelése során az alábbi konkrét szempontok alapján értékeli:
- az incidensben érintett adatok között találhatóak a személyes adatok különleges kategóriáiba eső adatok,
- az incidensben érintett személyes adatok száma …..
- az incidensben érintett természetes személyek között találhatóak 16. életévüket be nem töltött természetes személyek,
- az incidensben érintett természetes személyek száma….

- az incidensben érintett személyes adatok alkalmasak az érintettel történő közvetlen kapcsolatfelvételre (így különösen lakcím, telefonszám, e-mail cím)
- az incidensben érintett adatkezelés jogalapja 7.2.4. szerinti jogalap,
- az incidensben érintett adatkezelés jogalapja 7.2.5. szerinti jogalap,
- az incidensben érintett adatkezelés jogalapja 7.2.6. szerinti jogalap,
- a személyes adatok alkalmasak az érintett természetes személy személyazonosságának ellopására vagy a személyazonosságával való visszaélésre,
- az incidensben érintett személyes adatok alkalmasak arra, hogy pénzügyi veszteséget, illetve nem vagyoni kárt okozzanak az érintettjüknek.

Amennyiben az Intézet az incidenst a 2. kategóriába vagy a 3. kategóriába tartozónak minősíti, a vezető tisztségviselő legkésőbb 72 órával azután, hogy az adatvédelmi incidens az Intézet tudomására jutott, az incidenst bejelenti a NAIH-nak, a www.naih.hu oldalon elérhető elektronikus bejelentő rendszer vagy a szintén ezen oldalról letölthető formanyomtatvány segítségével.

6.5. Rendszeres tréningek

Az adatvédelmi tisztviselő gondoskodik az adatvédelmi tudatosság növelése céljából az adatvédelmi incidensekkel kapcsolatos oktatásról, mely során a múltban bekövetkezett adatvédelmi incidensek tapasztalatait, vagy a lehetséges adatvédelmi incidensek veszélyeit ismerteti, elemzi, a kockázatok csökkentésével, megelőzésével kapcsolatosan tájékoztatást ad, illetve az ismereteket ellenőrzi.

6.6. Hatásvizsgálat

Amennyiben valamely új adatkezelési folyamat – annak jellegére, hatókörére, körülményeire, céljaira tekintettel - valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelés megkezdését megelőzően az Intézmény hatásvizsgálatot folytat le arra vonatkozóan, hogy az adatkezelési folyamat a személyes adatok védelmét hogyan érinti. Egymáshoz hasonló adatkezelési műveletek, amelyek hasonló kockázatokat jelentenek egyetlenegy hatásvizsgálat keretében is elvégezhetők.

A hatásvizsgálatot főszabály szerint az adatvédelmi tisztviselő végzi. Amennyiben nem ő végzi, úgy az Intézmény köteles kikérni az adatvédelmi tisztviselő szakmai tanácsát.

Az Intézmény jelen Szabályzat 6. sz. mellékletében leírt ***szempontrendszer*** figyelembevételével elvégzi a ***hatásvizsgálatot***.

A hatásvizsgálat elvégzését követően szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén gondoskodik a hatásvizsgálat felülvizsgálatáról, mely során a kockázatok értékelését újra elvégzi. A kockázatok felülvizsgálatát legalább 3 évente el kell végezni.

A személyes adatok kezelésével kapcsolatosan az Adatkezelő kötelezettsége továbbá a kockázatelemzés, amelynek lépései a következők:
- a személyes adatok kezelésével kapcsolatos kockázatok azonosítása,
- kockázati lista felállítása,
- az egyes kockázatok valószínűsíthető fő okainak és várható negatív hatásainak meghatározása és
- ezek alapján a preventív és a korrektív kockázatkezelési folyamatok kidolgozása.

Szükséges a kockázatforrások feltárása, melyen belül meg kell határozni a kockázati preventív és korrektív célkezelés elemeit, az erőforrás-kezelés rendszerét és el kell különíteni az objektív és szubjektív kockázati elemeket.

Az elemzés során el kell jutni a teljes kockázatértékelési rendszer kialakításáig, amelyben teljes kockázatpotenciál és kockázat prioritási sorrend (nem az intézkedési rendszerrel azonos) megállapítása kell megtörténnie. Az elemzés menetét és eredményeit írásba kell foglalni.

A kockázatpotenciálnál meg kell határozni a valószínűség szempontjából
- kicsi
- közepes
- és nagy bekövetkezésű kockázatokat,

illetve horderő szempontjából

- kicsi
- közepes
- és nagy horderejű kockázatokat.

Ez a meghatározás alapozza meg a későbbi kockázatkezelési eljárás módját mind a preventív, mind a korrektív eljárás tekintetében. A kockázatelemzés végrehajtásáért az adatvédelmi tisztviselő felel.

6.6.1. Előzetes konzultáció

Amennyiben az elvégzett hatásvizsgálat azt állapítja meg, hogy az adatkezelési folyamat valószínűsíthetően magas kockázattal jár, akkor az Intézmény az adatkezelési folyamat megkezdését megelőzően konzultációt kezdeményez a Hatósággal.

A konzultáció kezdeményezése során az Intézmény csatolja:

- az elvégzett hatástanulmányt,
- az adatvédelmi tisztviselő nevét, elérhetőségét,
- az adatkezelési folyamatban részt vevő adatkezelő(k), adatfeldolgozó(k) feladatköreinek felsorolását,
- az adatkezelés célját, módját és
- az érintettek jogainak, szabadságainak biztosítása védelmében hozott intézkedéseket, garanciákat.

6.7. Szükségességi teszt

Az Intézmény kizárólag a GDPR 6. cikk (1) bekezdés e) pontja alapján közhatalmi jogkör gyakorlása vagy közfeladat ellátása érdekében végez adatkezelést. Abban az esetben, ha az adatkezelés nem törvényen vagy egyéb jogszabályon, illetve felettes szerv utasításán alapul, az Intézmény minden esetben vizsgálja az adatkezelés megkezdése előtt az érintettek magánszférájának, érdekeinek és alapvető jogainak biztosítása érdekében az adatkezelés szükségességét és arányosságát. Az Intézmény az adatkezelésre vonatkozó döntés előkészítés során vizsgálja a közérdekű feladat ellátásának szükségességét és az érintettek magánszférájába történő beavatkozás arányosságát. Jogszabály által előírt kötelezettség teljesítése során az Intézmény feltételezi, hogy a jogalkotó a szükségességi vizsgálatot elvégezte.

Az adatkezelés jogszerűségének vizsgálatához az Intézmény elvégez egy szükségességi tesztet, mely során az adatkezelés céljának szükségességét, az érintettek jogainak és szabadságainak arányos mértékű korlátozását vizsgálja és megfelelően alátámasztja.

A szükségességi teszt során az Intézmény azonosítja az adatkezelés szükségességét az adatkezeléshez, valamint a súlyozás ellenpontját képező érintetti érdeket és az érintett alapjogot. Az egymással ellentétes jogok és érdekek súlyozásának feltételét mindig az adott eset sajátos körülményeire való tekintettel vizsgálja az Intézmény. Az Intézmény a vizsgálat során figyelembe veszi különösen a kezelt, illetve kezelendő adat természetét és szenzitív jellegét, nyilvánosságának mértékét, az esetlegesen bekövetkező szabályszegés súlyosságát stb.

A kezelhető adatok jellege és mennyisége nem haladhatja meg a jogszerű érdekek érvényesítése céljából szükséges mértéket. Az arányosság vizsgálata a célok és a megválasztott eszközök közötti kapcsolat értékelését foglalja magában. A választott eszközök a szükségesség mértékét nem haladhatják meg, azonban az eszközöknek is alkalmasnak kell lenniük a meghatározott cél elérésére.

A súlyozás elvégzése alapján az Intézmény megállapítja, hogy kezelhető-e a személyes adat.

A teszt eredményéről az érintettek kérés esetén tájékoztatást kapnak, melyből egyértelműen kiderül, hogy az adatkezelés miért tekinthető szükséges és arányos korlátozásnak. Az Intézmény a szükségességi tesztben tájékoztatja az érintetteket a hozzájárulás hiányára tekintettel alkalmazott adatvédelmi garanciákról és az adatkezelés elleni tiltakozás lehetőségeiről.

Az Intézmény mérlegelési jogkörében bevezetett adatkezelések esetén, azok sajátos körülményeire tekintettel minden egyes esetben külön szükségességi tesztet végez el.

6.8. Adatbiztonsági szabályok

Az adatbiztonsági és információbiztonsági szabályok, beleértve a jogosultságkezelést, a hatályos jogszabályokon alapuló központi kezelésű Információbiztonsági Szabályzat, továbbiakban IBSZ határozza meg. Az IBSZ ismerete minden adatkezeléssel elektronikus információs rendszerrel kapcsolatban álló munkakört betöltő munkavállaló részére kötelező.

Az adatbiztonsági szabályokat részletesen az Intézmény információbiztonságról szóló szabályzata tartalmazza.

6.9. Fizikai védelem

A papíralapon kezelt aktív, a gyógyító tevékenység kapcsán használatban lévő és a gyógyító tevékenység tekintetében, folyamatában személyes adatok biztonsága érdekében az Intézmény az alábbi intézkedéseket alkalmazza:

- az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá, más számára fel nem tárhatóak;
- a dokumentumokat jól zárható, száraz, tűz - és vagyonvédelmi berendezéssel ellátott helyiségben helyezi el;
- a folyamatos aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá;
- az adatkezelést végző munkatárs a nap folyamán csak úgy hagyhatja el az olyan helyiséget, ahol adatkezelés folyik, hogy a rá bízott adathordozókat elzárja;
- az adatkezelést végző munkatársa a munkavégzés befejeztével a papíralapú adathordozót elzárja;
- amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat alkalmazza az Intézmény.

A személyes adatok tárolásának helyén az Intézmény az alábbi intézkedéseket és garanciális elemeket alkalmazza:

- az adatkezeléssel érintett helyiségekben található tárolók kulccsal zárhatók, kizárólag csak az arra jogosultak léphetnek be és nyithatják ki,
- a kulccsal rendelkezőkről nyilvántartást vezet az Adatkezelő,
- kizárólag az Intézmény alkalmazottja rendelkezhet ***kulcsfelvételi engedéllyel***
- amennyiben olyan személynek kell tevékenysége ellátása miatt bemenni az adatkezeléssel érintett irodahelyiségbe, aki nem jogosult vagy nem az Intézmény alkalmazottja, akkor minden esetben tartózkodik vele egy olyan személy is, aki ott jogosult tartózkodni.

Amennyiben a papíralapon tárolt személyes adat kezelésének célja megvalósult, úgy az Intézmény intézkedik a papíralapú adathordozó megsemmisítéséről. A ***megsemmisítési jegyzőkönyvmintát*** jelen Szabályzat 7. sz. melléklete tartalmazza.

Amennyiben a személyes adatok adathordozója nem papír, hanem más fizikai eszköz, úgy a fizikai eszköz megsemmisítésére a papíralapú dokumentumokra vonatkozó megsemmisítési szabályok az irányadóak.

6.10. Álnevesítés

Az 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, mivel az Intézmény az ilyen további információt külön tárolja,-technikai és szervezési intézkedések megtételével biztosítja, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.

Az álnéven történő adatkezelést az Intézmény a nagyobb fokú biztonság érdekében, valamint a statisztikai célra gyűjtendő adatok vagy a fejlesztés, tesztelés, karbantartás alatt álló rendszerek esetében a tesztadatok tekintetében végez, mivel a személyes adatok álnevesítése csökkentheti az érintettek számára a kockázatokat, valamint az Intézmény ezáltal könnyebben meg tud felelni az adatvédelmi kötelezettségeinek.
Az álnevesítés személyes adatok kezelése során történő alkalmazásának ösztönzése céljából lehetővé teszi az álnevesítésre irányuló intézkedések és az általános elemzés egyidejű alkalmazását az Intézmény szervezetén belül. Az Intézmény továbbá biztosítja, hogy az ahhoz szükséges további információkat, amelyek által a személyes adatokat egy adott érintetthez lehessen kapcsolni, elkülönítve tárolják. Az Intézménynél az adatvédelmi tisztviselő az, aki ugyanazon a szervezeten belül feljogosított személynek minősül.

A természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli a Rendelet követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát. Ahhoz, hogy az Adatkezelő igazolni tudja a Rendeletnek való megfelelést, olyan belső szabályokat kell alkalmaznia, valamint olyan intézkedéseket kell végrehajtania, amelyek teljesítik különösen a beépített és az alapértelmezett adatvédelem elveit.

Az Intézmény törekszik - a GDPR-nak való megfelelés érdekében - a személyes adatok kezelésének minimálisra csökkentésére, a személyes adatok mihamarabbi álnevesítésére, a személyes adatok funkcióinak és kezelésének átláthatóságára, valamint arra, hogy az érintett nyomon követhesse az adatkezelést, az Intézmény pedig biztonsági elemeket hozhasson létre és továbbfejleszthesse azokat.

6.11. Beépített adatvédelem

Bevezetésre kerül az ún. beépített adatvédelem (privacy by design), melynek következtében az Intézmény már az adatkezelés tényleges megkezdése előtt – például már a projekt előkészítés időszakában – is figyelemmel van a GDPR előírásaira. A beépített adatvédelem az Intézmény saját, olyan belső eljárásainak az összessége, amivel - a külső szabályozásoktól függetlenül is - igyekszik megfelelni annak, hogy az érintett magánszféráját minél jobban védje.

A természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli a GDPR követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát. Az említett intézkedések magukban foglalják a személyes adatok kezelésének minimálisra csökkentését, a személyes adatok mihamarabbi álnevesítését, a személyes adatok funkcióinak és kezelésének átláthatóságát, valamint azt, hogy az érintett nyomon követhesse az adatkezelést, az Intézmény pedig biztonsági elemeket hozzon létre és továbbfejleszthesse azokat. Az adatkezelésnek átláthatónak és felhasználó-központúnak, az adatvédelemnek proaktívnak kell lennie, az adat teljes életciklusát fel kell ölelnie, vagyis a teljes folyamatnak része kell lennie.

Az Intézmény a tudomány és a technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével, mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket - hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt a GDPR-ban foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.
Az Intézmény megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezeknek az intézkedéseknek különösen azt kell biztosítaniuk, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

A GDPR 42. cikke szerinti jóváhagyott tanúsítási mechanizmus felhasználható annak bizonyítása részeként, hogy az Intézmény teljesíti az előbbiekben előírt követelményeket.

Az Intézmény és az adatfeldolgozó intézkedéseket hoz annak biztosítására, hogy az Intézmény vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az Intézmény utasításának megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

A beépített és az alapértelmezett adatvédelem elveit a közbeszerzések során is figyelembe veszi az Intézmény.

Adattovábbítás esetén a megfelelőségi határozat hiányában az Intézmény vagy az adatfeldolgozó a megfelelő garanciák érintett számára való biztosítása útján gondoskodik az adatvédelem harmadik országbeli hiányosságainak ellensúlyozásáról. A garanciák biztosítják az adatvédelmi követelményeknek való megfelelést, az Európai Unión belüli adatkezelés esetén biztosított jogokkal azonos szintű jogokat biztosítanak az érintettek számára, beleértve az érintettek jogainak érvényesíthetőségét és a hatékony jogorvoslat lehetőségét, ezen belül ideértve azt, hogy az érintettek hatékony közigazgatási vagy bírósági jogorvoslatot vehessenek igénybe, valamint kártérítést igényelhessenek az Európai Unióban vagy egy harmadik országban. A garanciák különösen a személyes adatok kezelésére vonatkozó általános elveknek, valamint a beépített és alapértelmezett adatvédelem elveinek való megfelelésre vonatkoznak.

6.12. Oktatás és tréningrendszer

Kiemelt területként kell kezelni a munkavállalók kapcsán a biztonságtudatossági képzést a szervezet informatikai és nem informatikai alkalmazottai részére.

A biztonságtudatos magatartás komoly üzleti károkat okozó hibák és támadások megelőzésében játszhat szerepet.

Nem elegendő a megfelelően kidolgozott IT biztonsági szabályzat, információbiztonsági rendelkezések és adatvédelmi, adatbiztonsági szabályozás megléte a szervezetben, a munkavállalókban rendszeres képzések, tréningek során kell tudatosítani, hogy a kialakított szabályrendszer és az IT eszközök önmagukban nem képesek garantálni a szervezet számára az adat- és információbiztonságot, ehhez a napi munkatevékenységük során felelős magatartásukkal a dolgozóknak is hozzá kell járulniuk.

A munkavállalók megfelelő képzése a képzést követően kimutathatóan kevesebb biztonsági incidenst eredményez, ami a közvetlen adatvesztésből és esetleges adatvédelmi birságból eredő károkon túl a pénzügyi eredményekben is nyilvánvalóan megmutatkozik.
A munkavállalók általános adatvédelmi-információbiztonsági tréning rendje hat havonta (kapcsolható más rendszeres képzésekhez, tréningekhez pl.: tűz- és munkavédelem) egy óra időtartamban történjen. Ez vonatkozik az informatikai és nem informatikai munkavállalókra egyaránt.
Külön tréningrendet kell biztosítani az informatikai, különösen a rendszergazdai feladatokat ellátók részére. Ennek célja, hogy kizökkentse a képzés alatt állókat a megszokott munkamenetükből és feltárja előttük a rosszindulatú támadások, hackerek által folyamatosan fejlesztett aktuális támadási szemléletet, rámutasson az aktuális trendek szerint jellemzően keresett gyenge pontokra és segítse őket abban, hogy érzékelt behatolási kísérlet esetén milyen megoldásokat preferáljanak a támadások elhárítására és a kockázat alacsony szinten tartásának érdekében.

6.13. Az érintettek jogainak érvényesítése

Az érintett tájékoztatást kérhet személyes adatai kezeléséről, valamint kérheti személyes adatainak helyesbítését, illetve – a jogszabályban elrendelt adatkezelések kivételével – törlését, korlátozását az Intézmény feltüntetett elérhetőségein.

Az érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formában megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa.
Az Intézmény a beérkezett kérelmet, illetve tiltakozást köteles a főigazgatóhoz történő beérkezést követően a beérkezéstől számított három munkanapon belül áttenni az Intézményi vezető adatvédelmi referenshez, aki 3 munkanap alatt köteles eljuttatni az adatkezelés szempontjából feladat- és hatáskörrel rendelkező szervezeti egység vezetőjéhez.

A feladat- és hatáskörrel rendelkező szervezeti egység vezetője az érintett személyes adatának kezelésével összefüggő kérelmére, az érkezésétől számított legkésőbb 1 hónapon – tiltakozási jog gyakorlása esetén 15 napon – belül írásban, közérthető formában választ ad az Intézményi vezető adatvédelmi referensnek.

Az érintett kérelmére az Adatkezelő tájékoztatást ad az érintett általa kezelt, illetve az általa vagy rendelkezése szerint megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.

A tájékoztatás főszabály szerint ingyenes, ha a tájékoztatást kérő a folyó évben azonos adatkörre vonatkozóan tájékoztatási kérelmet az Adatkezelőhöz még nem nyújtott be. Egyéb esetekben költségtérítés állapítható meg. A költségtérítés mértékét az Intézmény „66. Szabályzat egyes egészségügyi szolgáltatások térítési díjairól" tartalmazza. A már megfizetett költségtérítést vissza kell téríteni, ha az adatokat jogellenesen kezelték, vagy a tájékoztatás kérése helyesbítéshez vezetett.

A valóságnak nem megfelelő adatot az adatot kezelő szervezeti egység vezetője – amennyiben a szükséges adatok és az azokat bizonyító közokiratok rendelkezésre állnak – helyesbíti, a GDPR. 17. cikkében meghatározott okok fennállása esetén intézkedik a kezelt személyes adat törléséről.
A személyes adatot törölni kell, ha

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását~~,~~ és az adatkezelésnek nincs más jogalapja;
c) az érintett tiltakozik az adatkezelés ellen~~,~~ és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett tiltakozik az adatkezelés ellen;
d) a személyes adatokat jogellenesen kezelték;
e) a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
f) a személyes adatok gyűjtésére a 16 éven aluli gyermekek részére az információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor;
g) ha az Adatkezelő nyilvánosságra hozta a személyes adatot és a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték úgy azt törölni köteles, valamint az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az ésszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

Az érintett tiltakozhat személyes adatának kezelése ellen,

- ha a személyes adatok kezelése vagy továbbítása kizárólag az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez vagy az Adatkezelő, adatátvevő vagy harmadik személy jogos érdekének érvényesítéséhez szükséges, kivéve kötelező adatkezelés esetén;
- ha a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik; valamint
- törvényben meghatározott egyéb esetben.

Az Adatkezelő a tiltakozást a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 napon belül megvizsgálja, annak megalapozottsága kérdésében döntést hoz és döntéséről a kérelmezőt írásban tájékoztatja.

Ha az Adatkezelő az érintett tiltakozásának megalapozottságát megállapítja, az adatkezelést - beleértve a további adatfelvételt és adattovábbítást is – megszünteti, az adatokat korlátozza, valamint a tiltakozásról, továbbá az annak alapján tett intézkedésekről értesíti mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbította és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében.

Ha az érintett az Adatkezelő döntésével nem ért egyet, illetve, ha az Adatkezelő a válaszadási határidőt elmulasztja, az érintett - a döntés közlésétől, illetve a határidő utolsó napjától számított 30 napon belül - bírósághoz fordulhat.
Ha az adatátvevő jogának érvényesítéséhez szükséges adatokat az érintett tiltakozása miatt nem kapja meg, úgy az értesítés közlésétől számított 15 napon belül, az adatokhoz való hozzájutás érdekében bírósághoz fordulhat az Adatkezelő ellen. Az Adatkezelő az érintettet is perbe hívhatja.

Ha az Adatkezelő az értesítést elmulasztja, az adatátvevő felvilágosítást kérhet az adatátadás meghiúsulásával kapcsolatos körülményekről az Adatkezelőtől, amely felvilágosítást az Adatkezelő az adatátvevő erre irányuló kérelmének kézbesítését követő 8 napon belül köteles megadni. Felvilágosítás kérése esetén az adatátvevő a felvilágosítás megadásától, de legkésőbb az arra nyitva álló határidőtől számított 15 napon belül fordulhat bírósághoz az Adatkezelő ellen. Az Adatkezelő az érintettet is perbe hívhatja.

Az Adatkezelő az érintett adatát nem törölheti, ha az adatkezelést törvény rendelte el. Az adat azonban nem továbbítható az adatátvevő részére, ha az adatkezelő egyetértett a tiltakozással, vagy a bíróság a tiltakozás jogosságát megállapította.

Amennyiben az érintett jogainak gyakorlása során az ügy megítélése nem egyértelmű, az adatot kezelő szervezeti egység vezetője az ügy iratainak és az ügyre vonatkozó álláspontjának megküldésével állásfoglalást kérhet az adatvédelmi tisztviselőtől, aki azt három napon belül teljesíti.
Az Intézmény az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak okozott kárt, illetve az általa vagy az általa igénybe vett adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is megtéríti. Az Adatkezelő mentesül az okozott kárért való felelősség és a sérelemdíj megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső, elháríthatatlan ok idézte elő. Ugyanígy nem téríti meg a kárt, amennyiben az a károsult szándékos vagy súlyosan gondatlan magatartásából származott.

Az érintett adatvédelmi ügyekkel kapcsolatos panasszal élhet a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (1055 Budapest, Falk Miksa utca 9-11., postacím: 1363 Budapest, Pf.: 9.), illetve élhet bírósági jogorvoslati jogával a lakóhelye vagy tartózkodási helye szerint illetékes törvényszéknél.

6.14. Az Intézménynél megvalósuló adatkezelések

6.14.1. Az adatkezelések helyei:

Az Intézmény székhelye:

1051 Budapest, Hercegprímás utca 14-16.

6.14.2. Az Intézmény telephelyei:

1054 Budapest, Akadémia u. 8.	Ifjúság-egészségügyi szolgálat; iskolai védőnői szolgálat; iskolai védőnői ellátás; gyermek háziorvosi ellátás
1052 Budapest, Semmelweis u. 14.	Felnőtt háziorvosi ellátás
1053 Budapest, Kecskeméti u. 9.	Fogászati alapellátás (gyermekfogászat); fogászati alapellátás (iskolafogászat)
1055 Budapest, Markó u. 7.	Fogászati alapellátás (gyermekfogászat); fogászati alapellátás (iskolafogászat)
1056 Budapest, Váci u. 40.	Felnőtt háziorvosi ellátás
1054 Budapest, Hold u. 8.	Felnőtt háziorvosi ellátás

7. ZÁRÓ RENDELKEZÉSEK

A Szabályzat személyi, tárgyi és időbeli hatályára a 2. pontban írt rendelkezések az irányadók.