



LUMNICZER SÁNDOR KÓRHÁZ-RENDELŐINTÉZET  
9330. Kapuvár, dr.Lumniczter Sándor u.10. Pf.34.  
Tel.:96/596-500 Fax: 96/242-224  
E-mail: titkarsag@lumniczterkorhaz.hu



„ÉRBETEGEK MEKKÁJA: KAPUVÁR ®”

## ADATVÉDELMI SZABÁLYZAT

Készítette: *Némethné Simacsek-Kun Edina*  
Némethné Simacsek-Kun Edina  
Adatvédelmi tisztviselő  
2020.12.28.

Iktatószám:	SZ35/2021
Változat száma:	1
Állomány név:	
Oldalak száma:	61
Mellékletek száma:	6
Érvénybelépés időpontja:	2021.01.01.

Jóváhagyta: *Dr. Benedek Zoltán*

Dr. Benedek Zoltán  
főigazgató  
2020.12.28.

### MÓDOSÍTÁSOK JEGYZÉKE

Készítette: Módosította:	Dátum, aláírás	Változat	Módosított oldalszám	Jóváhagyta Aláírás	Kibocsátás időpontja

## Tartalom

1.	Célok .....	1
2.	Alkalmazási terület .....	1
2.1.	Tárgyi hatály .....	1
2.2.	Szakterületi és személyi hatály .....	1
2.3.	Időbeli hatály .....	1
2.4.	A szabályzat alkalmazása.....	1
3.	Fogalom meghatározások .....	2
4.	Felelőségek, hatáskörök (figyelemmel a jelen szabályzat 5.3 pontjára) .....	4
5.	Leírás .....	5
5.1.	Az adatok kezelése .....	5
5.1.1.	Adatkezelés - adatfeldolgozás – adattovábbítás .....	5
5.1.1.1.	Alapelvek az adatkezelés során .....	5
5.1.1.2.	Az adatkezelés jogalapja .....	6
5.1.1.3.	Az érintett előzetes tájékoztatása .....	7
5.1.1.4.	Adatfeldolgozó igénybevételének szabályai .....	9
5.1.1.5.	Adattovábbítás, adattovábbítási nyilvántartás .....	9
5.1.2.	Az érintettek jogai és a jogok érvényesítése.....	11
5.1.2.1.	Általános irányelvek.....	11
5.1.2.2.	Az érintettek jogainak érvényesítése .....	11
5.1.2.3.	Az adatok helyesbítéséhez, törléséhez való jog, az adatkezelés korlátozásához való jog .....	12
5.1.2.4.	Az adathordozhatósághoz való jog .....	13
5.1.2.5.	Tiltakozás személyes adat kezelése ellen.....	13
5.1.2.6.	Jogorvoslat, bírósági jogérvényesítés és kártérítés .....	14
5.2.	Az intézmény adatvédelmi rendszere.....	14
5.2.1.	Az adatkezelés folyamatának kialakítása az intézménynél.....	14
5.2.2.	Adatbiztonsági szabályok.....	15
5.2.2.1.	Általános irányelvek.....	15
5.2.2.2.	Fizikai védelem.....	15
5.2.2.3.	Informatikai védelem.....	16
5.2.2.4.	Szerverekbiztonsága.....	16
5.2.2.5.	Jogosultságkezelés.....	17
5.2.2.6.	Jogosultságkezelési folyamat .....	17
5.2.3.	Átnevesítés .....	18
5.2.4.	Beépített adatvédelem .....	18
5.2.5.	Mobil eszköz menedzsment.....	19
5.2.6.	Adatvédelmi incidens kezelése .....	19
5.2.6.1.	Adatvédelmi incidens észlelése és jelentése .....	19
5.2.6.2.	Adatvédelmi incidens kivizsgálása, értékelése .....	19
5.2.6.3.	Az adatvédelmi incidens nyilvántartása.....	20
5.2.6.4.	Az adatvédelmi incidens bejelentése a Hatóság részére.....	20
5.2.6.5.	Az érintettek tájékoztatása az adatvédelmi incidensről.....	20
5.2.7.	Hatásvizsgálat.....	21
5.2.8.	Előzetes konzultáció.....	22
5.2.9.	Érdekmérlegelés .....	22
5.2.10.	Adatvédelmi ismeretek oktatása .....	23
5.3.	Az adatvédelem szervezeti rendszere – az adatkezelésben közreműködők és feladataik.....	23
5.3.1.	A Főigazgató.....	23

5.3.2.	Az adatvédelmi tisztviselő.....	24
5.3.3.	Személyes, egészségügyi adatokkal kapcsolatos adatkezelést ténylegesen végző munkavállaló .....	25
5.4.	Az intézménynél megvalósuló adatkezelések.....	25
5.4.1.	A munkavállalók személyes adatainak kezelése.....	26
5.4.1.1.	Általános irányelvek.....	26
5.4.1.2.	Személyazonosító igazolványok fénymásolása.....	26
5.4.1.3.	Erkölcsei bizonyítványok kezelése.....	27
5.4.1.4.	Egészségügyi alkalmassággal kapcsolatos egészségügyi adatok kezelése ..	28
5.4.1.5.	Megváltozott munkaképességű munkavállalók.....	28
5.4.1.6.	Diákok, szakmai gyakorlatot teljesítő személyek adatainak kezelése.....	29
5.4.1.7.	A munkaviszony fenntartásával és megszűnésével kapcsolatos adatkezelések .....	29
5.4.1.8.	A munkaviszonnyal kapcsolatos adatkezelésekre vonatkozó nyilatkozatok	29
5.4.1.9.	Munkavállalók oktatása .....	29
5.4.1.10.	Béren kívüli juttatások .....	29
5.4.1.11.	Harmadik személyek munkaviszonnyal kapcsolatosan megadott adatai ...	30
5.4.2.	A munkavállalók technikai eszközeinek ellenőrzésével kapcsolatos adatkezelés .....	32
5.4.2.1.	Intézményi informatikai eszközök ellenőrzése .....	32
5.4.2.2.	Intézményi e-mail címek ellenőrzése .....	33
5.4.2.3.	Az internet használatának ellenőrzése .....	33
5.4.2.4.	Intézményi tulajdonú gépjárművek nyomon követése .....	33
5.4.3.	Egészségügyi adatok kezelése.....	33
5.4.4.	Munka- és balesetvédelmi ellenőrzések.....	34
5.4.4.1.	Munkabaleset kivizsgálása .....	35
5.4.4.2.	Tűzesetek kivizsgálása:.....	35
5.4.4.	Munkára alkalmas állapot munkavédelmi vizsgálata .....	36
5.4.5.	Munkára jelentkezők adataival kapcsolatos adatkezelés.....	37
5.4.5.1.	Az intézményhez történő jelentkezés folyamata.....	37
5.4.5.2.	A berepülő önéletrajzokkal és a munkaerő-toborzással kapcsolatos közös szabályok .....	37
5.4.5.3.	A „bepülő önéletrajzok”-ra vonatkozó különös szabályok.....	37
5.4.6.	Ingatlanbérbeadás.....	38
5.4.7.	Kapcsolatfelvétel az intézménnyel .....	38
5.4.8.	Panaszok, észrevételek ügyintézése .....	38
5.4.9.	Kamerás megfigyeléssel kapcsolatos adatkezelés .....	39
5.4.10.	Vagyonvédelemmel kapcsolatos adatkezelés .....	39
5.4.10.1.	Vendégek be- és kiléptetése.....	39
5.4.10.2.	Vagyonvédelmi rendkívüli események .....	39
5.4.11.	Marketing tevékenységgel kapcsolatos adatkezelés .....	39
5.4.12.	Honlap kezelésére vonatkozó adatkezelés .....	40
5.4.13.	Pénzügyi adatkezelés .....	41
5.4.13.1.	Irattározás.....	41
5.4.13.2.	Hátralékkezelés .....	42
5.4.14.	Közérdekű adatok kezelése .....	42
6.	Utalások és megjegyzések.....	42
6.1.	Vonatkozó dokumentáció .....	42
6.2.	Kapcsolódó dokumentumok .....	43
6.3.	Megjegyzések .....	43
7.	Mellékletek.....	44
7.1.	melléklet.....	44
7.2.	melléklet.....	46
7.3.	melléklet.....	47

7.4. melléklet.....	48
7.5. melléklet.....	50
7.6. melléklet.....	60
8. Függelék.....	61

# 1. Célok

A dokumentum a következő célok megvalósításának érdekében kerül kiadásra:

A Szabályzat célja, hogy

- meghatározza az intézménynél vezetett – személyes, egészségügyi, genetikai, biometrikus adatokat tartalmazó - manuális vagy számítógépes nyilvántartások kezelésének rendjét, annak érdekében, hogy az érintettek adatainak védelme biztosított legyen;
- biztosítsa a nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését;
- megakadályozza az adatokhoz való jogosulatlan hozzáférést, az adatok megváltoztatását, jogosulatlan nyilvánosságra hozatalát, továbbá
- mindezek alapján szabályozza az intézmény szervezeti egységeinél történő adatkezelések rendjét;
- 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 nevről, címéről és az adatkezeléssel összefüggő tevékenységéről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.

Az intézmény megnevezése:	Lumniczer Sándor Kórház-Rendelőintézet Kapuvár
Az intézmény törzsszáma:	367307
Az intézmény székhelye:	9330 Kapuvár, Dr. Lumniczer Sándor u.10.
Az intézmény elérhetősége:	<a href="mailto:titkarsag@lumniczerkorhaz.hu">titkarsag@lumniczerkorhaz.hu</a>
Az intézmény képviselője:	Dr. Benedek Zoltán Főigazgató
Adatvédelmi tisztviselő:	Némethné Simacsek-Kun Edina
Adatvédelmi tisztviselő elérhetősége:	<a href="mailto:adatvedelem@lumniczerkorhaz.hu">adatvedelem@lumniczerkorhaz.hu</a>

## 2. Alkalmazási terület

### 2.1. Tárgyi hatály

A szabályzat tárgyi hatálya kiterjed az intézmény bármely szervezeti egységénél és telephelyeinél folytatott valamennyi olyan folyamatra, amely során személyes, egészségügyi, különleges adat kezelése valósul meg.

### 2.2. Szakterületi és személyi hatály

Szakterületi hatály: az intézmény valamennyi szervezeti egysége.

Személyi hatály: kiterjed az intézmény valamennyi, adatok kezelését végző munkavállalójára, továbbá az intézménnyel szerződéses jogviszonyban álló természetes és jogi személyre, jogi személyiséggel nem rendelkező szervezetre, a velük kötött szerződésben rögzített mértékben.

### 2.3. Időbeli hatály

A szabályzat időbeli hatálya 2020. november 01-től visszavonásig tart.

### 2.4. A szabályzat alkalmazása

A szabályzatban előírtak betartásáért és betartatásáért minden, a feladatkörében érintett munkavállaló, illetve egységvezető felelős.

Személyes, egészségügyi, különleges adatot kezelni GDPR 6. cikk alapján - az adatvédelemre vonatkozó alapelvek tiszteletben tartásával lehet.

Az intézmény szervezeti egységeinél adatok kezelését végző, és azokhoz hozzáférési lehetőséggel rendelkező munkavállalók, és az intézmény megbízásából az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek munkavállalói kötelesek a megismert adatokat bizalmasan kezelni, üzleti titokként megőrizni és erről titoktartási nyilatkozatot tenni.

A Lumniczer Sándor Kórház-Rendelőintézetnél megbízási szerződéssel megbízást teljesítő személyek esetében, akik tevékenységük ellátása során az intézmény által kezelt természetes személyekhez

kapcsolódó adatokat megismerik és azokat felhasználják, a területi vezető köteles gondoskodni arról, hogy a megbízottakkal kötött szerződésben kerüljön rögzítésre az adatok titkosságának megőrzésére vonatkozó előírás.

Jelen szabályzat tartalmát az intézményhez való belépéskor - a felvételi eljárás során - minden munkavállalóval meg kell ismertetni. Az intézmény adatvédelmi szabályainak megismertetéséért a felvételt végző szervezeti egység vezetője a felelős.

### 3. Fogalom meghatározások

A szabályzatban hivatkozott jogszabályok jegyzékét, illetve azok rövidítését a 6.1. pontban felsorolt vonatkozó dokumentáció tartalmazza.

A jelen szabályzat fogalmi rendszere megegyezik az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (továbbiakban: az Infotv.) és az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE-ben (GDPR) meghatározott értelmező fogalommagyarázatokkal, így különösen:

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

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

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

**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;

**tiltakozás:** az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri;

**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;

**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;

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

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

**adatkezelés korlátozása:** a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

**adattörlés:** az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges (= anonimizálás, de ≠ megsemmisítés);

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

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

**adatmegsemmisítés:** az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése;

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

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

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

**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;

**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;

**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;

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

**harmadik fél:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adattfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adattfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;

**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;

**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:** 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;

**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 címzettnak; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;

**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;

**közérdekű adat:** egyéb közfeladatot ellátó szerv (állami vagy helyi önkormányzat) vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső adat;

**személyazonosító adat:** a családi és utónév, leánykori név, a nem, a születési hely és idő, az anya leánykori családi és utóneve, a lakóhely, a tartózkodási hely, a társadalombiztosítási azonosító jel (a továbbiakban: TAJ

szám) együttesen vagy ezek közül bármelyik, amennyiben alkalmas vagy alkalmas lehet az érintett azonosítására;

**kötelező erejű intézményi szabályok:** a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező intézmény vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli intézmény vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ;

**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;

**képviselő:** az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és a intézmény vagy adatfeldolgozó által a 27. cikk alapján írásban megjelölt természetes vagy jogi személy, aki, illetve amely az intézményt vagy adatfeldolgozót képviseli az intézményre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában;

**felügyeleti hatóság:** egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv;

**érintett felügyeleti hatóság:** az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint:

a) a intézmény 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 intézmény vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy

b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az intézmény 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;

**nyilvántartási rendszer:** a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

**releváns és megalapozott kifogás:** a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy ezt a rendeletet megsértették-e, illetve, hogy az az intézményre 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.

**szervezeti egység:** az intézmény szervezeti egységei az organogram szerint

**az adatkezelés felelős vezetője:** egy adott adatkezelés koordinálását végző, területi felelős vezető;

#### 4. Felelőségek, hatáskörök (figyelemmel a jelen szabályzat 5.3 pontjára)

A felelőségek, hatáskörök a szövegben kerültek meghatározásra.



## 5. Leírás

### 5.1. Az adatok kezelése

Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy műveletek összessége, így például:

- adatok gyűjtése
- adatok felvétele, rögzítése, rendszerezése és tárolása
- adatok megváltoztatása
- adatok felhasználása, lekérdezése,
- adatok továbbítása, nyilvánosságra hozatala
- adatok összehangolása vagy összekapcsolása
- adatok zárolása, törlése és megsemmisítése
- valamint további felhasználásuk megakadályozása.

Adatkezelésnek számít a fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése is.

#### 5.1.1. Adatkezelés - adatfeldolgozás – adattovábbítás

Azon érintettek esetében, akik gyógykezelésük érdekében maguk jelentkeznek az Intézménybe, a gyógykezeléssel összefüggő adatkezeléshez szükséges felhatalmazás megadottnak tekintendő, a beteg dokumentáció átvételével pedig hozzájárulásukat adják. Erről a gyógykezelt személyt (vagy törvényes képviselőjét) tájékoztatni kell. Ezzel kapcsolatos beteg tájékoztató az Intézmény honlapján is elérhető (7.1. sz. melléklet)

A gyógykezelt személy belátási képességének hiánya esetén, illetőleg sürgős szükség fennforgásánál az önkéntes közlés szándékát vélelmezni kell.

A biometrikus adatok kezelésének jogalapját az érintett hozzájárulása és a létfontosságú érdek védelme valamint az adatkezelő jogos érdeke támasztja alá. Az érintettek biometrikus adatainak kezelésével annak kapcsolatos jogairól és jogorvoslati lehetőségeiről az Intézmény honlapján a Térfigyelő rendszer adatvédelmi és adatbiztonsági szabályzatban tájékozódhat.

A személyes adatok nem egészségügyi célból történő tárolásának jogalapját az érintett hozzájárulása, az érintettel kötött szerződés, és jogi kötelezettség teljesítése támasztja alá.

Ezzel kapcsolatos tájékoztatás az érintettek részére minden esetben (papír alapon/digitálisan) megtörténik. Az adattovábbítás jogalapját a létfontosságú érdek védelme, valamint a jogi kötelezettség teljesítése írja elő.

##### 5.1.1.1. Alapelvek az adatkezelés során

**Célhoz kötöttség és adattakarékosság:** az intézménynél személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében, csak megfelelő tájékoztatáson alapuló beleegyezéssel kezelhető. Kizárólag olyan személyes adat kezelhető - a cél megvalósulásához szükséges mértékben és ideig -, amely az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható, azaz az intézmény rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításához szükségesek.

**Jogszerűség, tisztességes eljárás és átláthatóság, pontosság:** az adatok kezelését tisztességesen és törvényesen, valamint az érintett számára átlátható módon kell végezni. Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és naprakészségét.

A személyes adatok az adatkezelés céljához illeszkedő időtartamig (pl. a hozzájáruló nyilatkozat

visszavonásáig), illetve az ezekhez a műveletekhez kapcsolódó adóügyi, vagyonvédelmi és más előírások szerinti határidőig kezelhetők.

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 törlést a munkavállaló felett munkáltatói jogköröket ténylegesen gyakorló személy és az adatvédelmi tisztviselő ellenőrizheti.

**Szabályszerűség, megfelelés:** a folyamatokra vonatkozó illetve a kapcsolódó törvényeknek, jogszabályoknak és szerződéses kötelezettségeknek való megfeleléshez kapcsolódás.

A személyes adatok megfelelő biztonságát biztosítani kell.

**elszámoltathatóság:** az intézmény vezetője felelős a megfelelésért, továbbá képesnek kell lennie a megfelelés igazolására.

### 5.1.1.2. Az adatkezelés jogalapja

Személyes adat akkor kezelhető, ha (a felsoroltak egyike teljesül)

- a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez:
  - a 16. életévét betöltött kiskorú érintett hozzájárulásának érvényességéhez nem szükséges a törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása)
  - az érintett jogosult arra, hogy a nem egészségügyi ellátáshoz kapcsolódó adatkezelés során hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását;
- 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
  - a szerződésekbe javasolt adatkezelési pontokat a szabályzat szerinti melléklet tartalmazza;
- c) az adatkezelés az intézményre vonatkozó jogi kötelezettség teljesítéséhez szükséges (törvény elrendeli, felhatalmazást ad – kötelező adatkezelés);
- d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
- e) az adatkezelés közérdekű vagy az intézményre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
- f) az adatkezelés az intézmény 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.

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 tilos, kivéve, ha

- 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 tilalom nem oldható fel az érintett hozzájárulásával;
- b) azon személyek esetében, akik gyógykezelésük érdekében maguk jelentkeznek az Intézményben, a gyógykezeléssel összefüggő adatkezeléshez szükséges felhatalmazás megadottnak tekintendő, a beteg dokumentáció átvételével pedig hozzájárulásukat adják.
- c) az adatkezelés az intézménynek 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;
- d) az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképzetlensége folytán nem képes a hozzájárulását megadni;
  - e) 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;
  - f) az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
  - g) az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el;
  - h) 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;
  - i) 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 az alábbi feltételekre és garanciákra figyelemmel:
    - a személyes adatokat abban az esetben lehet a h) pontban említett célokból kezelni, ha ezen adatok kezelése olyan szakember által vagy olyan szakember felelőssége mellett történik, aki uniós vagy tagállami jogban, illetve az arra hatáskörrel rendelkező tagállami szervek által megállapított szabályokban meghatározott szakmai titoktartási kötelezettség hatálya alatt áll, illetve olyan más személy által, aki szintén uniós vagy tagállami jogban, illetve az arra hatáskörrel rendelkező tagállami szervek által megállapított szabályokban meghatározott titoktartási kötelezettség hatálya alatt áll;
  - j) 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;
  - k) az adatkezelés a 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;

Ha a hozzájáruláson alapuló adatkezelés célja az intézménnyel írásban kötött szerződés végrehajtása, a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából az érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbításának tényét, címzettjeit, adatfeldolgozó igénybevételének tényét. A szerződésnek félreérthetetlen módon tartalmaznia kell, hogy az érintett aláírásával hozzájárul adatainak a szerződésben meghatározottak szerinti kezeléséhez. Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulást nem adta meg.

#### 5.1.1.3. Az érintett előzetes tájékoztatása

Az intézmény megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó, a 13. és a 14. cikkben említett valamennyi információt és a 15–22. és 34. cikk

szerinti minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

Az intézmény elősegíti az érintett 15–22. cikk szerinti jogainak a gyakorlását. A 11. cikk (2) bekezdésében említett esetekben az intézmény az érintett 15–22. cikk szerinti jogai gyakorlására irányuló kérelmének a teljesítését nem tagadhatja meg, kivéve, ha bizonyítja, hogy az érintettet nem áll módjában azonosítani.

Az intézmény indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a 15–22. cikk szerinti kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az intézmény a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet. Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri.

Ha az intézmény nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

A 13. és 14. cikk szerinti információkat és a 15–22. és 34. cikk szerinti tájékoztatást és intézkedést díjmentesen kell biztosítani. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, az intézmény, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre:

- g) észszerű összegű díjat számíthat fel, vagy
- h) megtagadhatja a kérelem alapján történő intézkedést.

A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása az intézményt terheli.

Ha az érintetthez vonatkozó személyes adatokat az érintettől gyűjtik, az intézmény a személyes adatok megszerzésének időpontjában az érintett rendelkezésére bocsátja a következő információk mindegyikét:

- a) az intézménynek és – ha van ilyen – a intézmény képviselőjének a kiléte és elérhetőségei;
- b) az adatvédelmi tisztviselő elérhetőségei;
- c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
- d) a 6. cikk (1) bekezdésének f) pontján alapuló adatkezelés esetén, az intézmény vagy harmadik fél jogos érdekei;
- e) adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;

Az intézmény az érintettet a következő kiegészítő információkról tájékoztatja:

- a) a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól;
- b) az érintett azon jogáról, hogy kérelmezheti az intézménytől 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;
- c) a 6. cikk (1) bekezdésének a) pontján vagy a 9. cikk (2) bekezdésének a) pontján alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
- d) a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;
- e) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes

adatokat megadni, továbbá hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása;

- f) a 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

Ha a személyes adatokat nem az érintettől szerezték meg, az intézmény az érintett rendelkezésére bocsátja a következő információkat:

- a) az intézménynek és – ha van ilyen – az intézmény képviselőjének a kiléte és elérhetőségei;
- b) az adatvédelmi tisztviselő elérhetőségei;
- c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
- d) az érintett személyes adatok kategóriái;
- e) a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;

Egy adott adatkezeléssel kapcsolatosan az érintettek előzetes tájékoztatásának megszervezéséről az illetékes szervezeti egység köteles gondoskodni.

A szabályzat 7.1. számú melléklete tartalmazza az adatkezelési tájékoztatót a betegek részére. A dokumentumot elektronikusan közzé kell tenni az intézmény honlapján. Az adatkezelési tájékoztató aktualizálása az adatvédelmi tisztviselő feladata. A tájékoztató a Főigazgató jóváhagyásával - jelen szabályzat véleményeztetése nélkül - aktualizálható.

Az intézmény weboldalán ([www.lumniczerkorhaz.hu](http://www.lumniczerkorhaz.hu)) az adatvédelmi tisztviselő közzéteszi a betegeket érintő, adatvédelemmel kapcsolatos tájékoztatást.

#### 5.1.1.4. Adatfeldolgozó igénybevételeinek szabályai

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

Az adatfeldolgozó az intézmény előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe. Az általános írásbeli felhatalmazás esetén az adatfeldolgozó tájékoztatja az intézményt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőségét az intézménynek arra, hogy ezekkel a változásokkal szemben kifogást emeljen.

Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt.

Az intézmény megbízásából adatfeldolgozói tevékenységet végző természetes vagy jogi személyekre, illetve jogi személyiséggel nem rendelkező szervezetekre vonatkozó adatvédelmi kötelezettségek az adatfeldolgozóval kötött megbízási szerződésben érvényesítendőek. Az adatfeldolgozóval az Intézmény a GDPR. 28. cikk (3) bekezdése által előírt Adatfeldolgozói szerződést/adatfeldolgozói megállapodást köt.

Az adatfeldolgozóval kötött szerződésbe az adatvédelmi incidensre vonatkozó jogszabályi háttérrel be kell építeni (adatvédelmi incidens észlelésével kapcsolatos elvárásokat rögzíteni: értesítési kötelezettség, határidők, információk, csatorna, ...).

#### 5.1.1.5. Adattovábbítás, adattovábbítási nyilvántartás

Az érintett jogosult arra, hogy a rá vonatkozó, általa egy intézmény rendelkezésére bocsátott személyes adatokat, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik intézménynek továbbítsa anélkül, hogy ezt akadályozná az az intézmény, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha:

- i) az adatkezelés hozzájáruláson vagy szerződésen alapul.

Az adattovábbítás történhet kérelemre vagy törvény ilyen tartalmú rendelkezése alapján automatikusan. Az intézmény rendszeres adatszolgáltatást jogszabályban meghatározott szerveknek végez, a jogszabályokban meghatározott időszakonként és tartalommal. A jogszabály által előírt adattovábbítást az intézmény köteles teljesíteni.

Harmadik személy által benyújtott adattovábbítási kérelem elbírálása - a intézmény általi adatkezelésre vonatkozó törvényben kötelezően előírt adattovábbítás esetét kivéve -, az érintett szervezeti egység vezetőjének hatáskörébe tartozik. A szervezeti egység vezetője kikéri a Főigazgató, valamint az adatvédelmi tisztviselő írásbeli állásfoglalását a kérelem teljesíthetősége kérdésében.

Az adatigénylés abban az esetben teljesíthető, ha az tartalmazza:

- a) az adatigénylés célját, jogalapját (az alapul szolgáló törvényi rendelkezés pontos megjelölését);
- b) a kért adatok körének pontos meghatározását;
- c) az érintett személy azonosításához szükséges adatokat.

Törvény eltérő rendelkezése hiányában csak olyan személyes adatok továbbíthatók, amelyeknek az intézmény az adatkezelője. Amennyiben más szerv az intézmény, az adatkérést - törvény eltérő rendelkezése hiányában - el kell utasítani és az adatkérőt tájékoztatni kell arról, hogy a kért adatokat mely szervtől igényelheti.

Az érintett nyilatkozattételétől függetlenül teljesíteni kell a hatóságoktól (rendőrség, bíróság, ügyészség, adóhatóság, NAIH), valamint a nemzetbiztonsági szolgálatoktól érkező megkereséseket. A nemzetbiztonsági szolgálatoktól érkező megkeresésre vonatkozó adat - a minősített adat védelméről szóló mindenkor hatályos törvény alapján - a megkeresésben foglaltak szerinti fokozatú minősített adat. Az adatszolgáltatás csak a Főigazgató jóváhagyásával teljesíthető és erről sem más személy, sem más szerv nem tájékoztatható.

Az intézmény az Európai Parlament és a Tanács (EU) 2016/679. RENDELET 30. cikk. (1) bekezdése szerint belső adatvédelmi és adattovábbítási nyilvántartást vezet, amit az adatvédelmi szabályzatának melléklete tartalmaz. A nyilvántartás papír alapon és elektronikus úton is vezethető.

Az adattovábbítási nyilvántartás adatait a személyes adatok esetében öt évig, különleges adatok esetében húsz évig meg kell őrizni.

Az adattovábbítási nyilvántartásba a következő szervek / személyek tekinthetnek bele:

- a) a társadalombiztosítási szervek, Hatóság, a bíróság, a nyomozó hatóság, valamint a nemzetbiztonsági szolgálat törvényben meghatározott feladatai ellátásához, valamint
- b) az intézmény Főigazgatója, illetve az általa meghatározott személy, és
- c) az intézmény adatkezelésének ellenőrzését végző személy.

Személyes adat nyilvánosságra hozatala:

- a) Törvény közérdekből - az adatok körének kifejezett megjelölésével - elrendelheti a személyes adat nyilvánosságra hozatalát.
- b) Minden egyéb esetben a nyilvánosságra hozatalhoz az érintett hozzájárulása, különleges adat esetében írásbeli hozzájárulása szükséges.

## 5.1.2. Az érintettek jogai és a jogok érvényesítése

### 5.1.2.1. Általános irányelvek

Az érintett:

- tájékoztatást kérhet az intézménytől személyes, egészségügyi adatai kezeléséről az adatfelvételnél jelzett módon, illetve a feltüntetett elérhetőségeken;
- adatváltozás vagy téves adatrögzítés észlelése esetén kérheti az intézmény által kezelt személyes adatainak helyesbítését, valamint személyes adatainak - a kötelező adatkezelés kivételével - törlését az adatfelvételnél jelzett módon, illetve a feltüntetett elérhetőségeken;
- tiltakozhat a személyes adatok kezelése ellen az intézmény feltüntetett elérhetőségein;
- jogosult arra, hogy a személyes adatokhoz és bizonyos információkhoz hozzáférést kapjon;
- kérheti, hogy az intézmény korlátozza az adatkezelést;
- jogosult arra, hogy a rá vonatkozó, általa az intézmény rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formában megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik intézménynek továbbítsa.
- jogorvoslattal, panasszal a Nemzeti Adatvédelmi és Információszabadság Hatóságnál; (1055 Budapest, Falk Miksa utca 9-11. e-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu) telefon: +36 (1) 391-1400) vagy lakóhelye, illetve tartózkodási helye szerint illetékes törvényszéknél élhet.

Az intézményhez beérkezett bejelentés miatt az érintettet nem érheti hátrány.

Amennyiben az alább felsorolt érintetti jogok gyakorlására irányuló kérelem érkezik az intézményhez (az adatkezelési tájékoztatón feltüntetett elérhetőségek ellenére más intézményi elérhetőségre), azt minden esetben azonnal az adatvédelmi tisztviselőhöz kell továbbítani az ügyintézés céljából, aki a beérkezett kérelmet, illetve tiltakozást köteles a beérkezéstől számított három napon belül áttenni az adatkezelés szempontjából feladat- és hatáskörrel rendelkező szervezeti egység vezetőjéhez.

Az intézmény indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az intézmény a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet. Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri.

### 5.1.2.2. Az érintettek jogainak érvényesítése

Az érintett hozzáférési joga - az érintett tájékoztatása személyes, egészségügyi adatainak kezeléséről

- Az érintett jogosult arra, hogy az intézménytől visszajelzést kapjon arra vonatkozóan, hogy személyes, egészségügyi adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy az adatokhoz és a következő információkhoz hozzáférést kapjon:
  - a) az adatkezelés céljai;
  - b) az érintett adatok kategóriái;
  - c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel az adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
  - d) adott esetben az adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
  - e) az érintett azon joga, hogy kérelmezheti az intézménytől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen; kivéve az egészségügyi ellátással kapcsolatos adatkezelés során kezelt adatok

esetében;

- f) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
- g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
- h) az automatizált döntéshozatal ténye, 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.

- Az intézmény indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az intézmény a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet. Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri.

- A tájékoztatás ingyenes, ha a tájékoztatást kérő a folyó évben azonos adatkörre vonatkozóan tájékoztatási kérelmet az intézményhez még nem nyújtott be. Egyéb esetekben az intézmény költségtérítést állapíthat meg. A költségtérítés mértékét a felek között létrejött szerződés is rögzítheti. A már megfizetett költségtérítést vissza kell téríteni, ha az adatokat jogellenesen kezelték, vagy a tájékoztatás kérése helyesbítéshez vezetett.

- A tájékoztatás megtagadása esetén a Főigazgató - az adatvédelmi tisztviselő ügyintézésével - a kérelem kézhezvételét követő 30 napon belül írásban, vagy az érintett hozzájárulásával elektronikus úton közli az érintettel, hogy a felvilágosítás megtagadására mely jogszabályi rendelkezés alapján került sor, és tájékoztatja az érintettet a bírósági jogorvoslat, továbbá a Nemzeti Adatvédelmi és Információszabadság Hatósághoz fordulás lehetőségéről.

- Az elutasított kérelmekről a Főigazgató - az adatvédelmi tisztviselő ügyintézésével - a Hatóságot évente a tárgyévet követő év január 31-éig értesíti.

### 5.1.2.3. Az adatok helyesbítéséhez, törléséhez való jog, az adatkezelés korlátozásához való jog

- 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;
- d) a személyes adatokat jogellenesen kezelték;
- e) a személyes adatok gyűjtésére a 16 éven aluli gyermekek részére az információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor;
- f) a személyes adatokat az intézményre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
- g) ha a intézmény 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 észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő intézményeket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

- Az érintett adata nem törölhető, ha az adatkezelést törvény rendelte el.



Ha az intézmény nyilvánosságra hozta a személyes adatot, és a fentiek értelmében azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő intézményeket, hogy az érintett kérelmezte törlők a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

- Az érintett jogosult arra, hogy kérésére a intézmény 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 intézmény ellenőrizze a személyes adatok pontosságát;
  - b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
  - c) az intézménynek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
  - d) az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az intézmény jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.
- Ha az adatkezelés korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.
- Az adatvédelmi tisztviselő a helyesbítésről, a törlésről és az adatkezelés korlátozásáról az érintettet, továbbá - az adatkezelését felelős vezető megkérdezését követően - mindazokat értesíti, akiknek korábban az adatot adatkezelés céljára az intézmény továbbította, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti. Az érintett kérésére az intézmény tájékoztatja e címzettekről. Az intézmény az érintettet, akinek a kérésére korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

#### 5.1.2.4. Az adathordozhatósághoz való jog

- Az érintett jogosult arra, hogy a rá vonatkozó, általa az intézmény rendelkezésére bocsátott személyes, egészségügyi adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik intézménynek továbbítsa.

#### 5.1.2.5. Tiltakozás személyes adat kezelése ellen

- Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon adatainak kezelése ellen, ideértve a profilalkotást is. Ebben az esetben az intézmény a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.
- Ha a személyes adatok kezelésére tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozhasson a rá vonatkozó személyes adatok kezelése ellen, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.
- Ha az intézmény az érintett tiltakozásának megalapozottságát megállapítja, az adatkezelést - beleértve a további adatfelvételt és adattovábbítást is – megszünteti, az adatokat zárolja, 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.
- 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.

### 5.1.2.6. Jogorvoslat, bírósági jogérvényesítés és kártérítés

- Azt, hogy az adatkezelés a jogszabályban foglaltaknak megfelel, az intézmény, mint adatkezelő köteles bizonyítani.
- Az egyes adatkezelések jogszerűségéért és a jogszabály, illetve jelen szabályzat szerinti megfelelőségéért az illetékes szervezeti egység vezetője a felelős.
- Az érintett jogorvoslati lehetőséggel, panasszal a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (1055 Budapest, Falk Miksa utca 9-11. e-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu) telefon: +36 (1) 391-1400) vagy lakóhelye, vagy tartózkodási helye szerint illetékes törvényszéknél élhet.
- A bírósági jogérvényesítés folyamatáról az Infotv. 22. §-a rendelkezik.
- Az intézmény az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak okozott kárt köteles megtéríteni, illetve az általa vagy az általa igénybe vett adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is megtéríti.
- Az intézmény mentesül az okozott kárért való felelősség és a sérelemdíj megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt az adatkezelés körén kívül eső elháríthatatlan ok idézte elő.
- Az intézmény nem téríti meg a kárt, amennyiben az a károsult szándékos vagy súlyosan gondatlan magatartásából származott.

## 5.2. Az intézmény adatvédelmi rendszere

### 5.2.1. Az adatkezelés folyamatának kialakítása az intézménynél

Az adatvédelmi és adatbiztonsági intézkedések betartásának, valamint jelen szabályzat rendelkezései érvényesülése érdekében egy személyes, egészségügyi adatokat tartalmazó új adatkezelés folyamatának kialakítása során a következő lépéseket kell végrehajtani:

- a) adatkezelés koncepciójának megfogalmazása, adatkezelés megnevezése
- b) az intézmény szervezeti egység kijelölése
- c) az adatkezelés felelős vezetőjének kijelölése
- d) adatvédelmi felelős tájékoztatása
- e) adatvédelmi tisztviselő előzetes tájékoztatása, bevonása
- f) az adatkezelés céljának meghatározása
- g) adatkezelés jogalapjának meghatározása (jogszabályhely kiválasztása, jogos érdek megfogalmazása, érdekmérlegelési teszt elvégzése, ...)
- h) a feldolgozandó adatkör meghatározása
- i) annak vizsgálata, hogy különleges személyes adatok feldolgozására kerül-e sor
- j) az adatkezeléssel érintettek csoportjának leírása, várható mennyiségének behatárolása
- k) adatok forrásának meghatározása
- l) az adatkezelés technológiájának, illetve automatizáltságának kiválasztása,
- m) informatikai feldolgozó rendszer alkalmazása esetén a vonatkozó szabályzat, valamint a rendszerszintű informatikai biztonsági szabályzatok előírásainak érvényesítése
- n) adatfeldolgozó bevonása esetén megállapodás készítése
- o) a tényleges adatkezelés helyének meghatározása
- p) adattovábbítás esetén a továbbítandó adatok körének meghatározása, jogalapjának kiválasztása, a címzett meghatározása
- q) a valószínűsíthetően magas kockázattal járó új adatkezelés esetén hatásvizsgálat lefolytatása, illetve szükség esetén előzetes konzultáció kezdeményezése a Hatósággal
- r) az adattörlés, archiválás megtervezése
- s) hozzájáruláson alapuló adatkezelés esetén a hozzájáruló nyilatkozat kialakítása
- t) az adatkezelési tájékoztató és adatvédelmi nyilatkozat elkészítése
- u) az adatkezeléshez történő hozzájárulások beszerzése
- v) az adatkezelés tervezett megkezdése előtt legalább 20 nappal korábban bejelentés a belső adatvédelmi nyilvántartásba a kitöltött adatkezelési adatlap (a jelen szabályzat mellékletében meghatározott adatkezelési adatlap) jogi és adatvédelmi munkatárs részére történő megküldésével

- (a célonként eltérő adatkezelésekről külön adatkezelési adatlapot kell kitölteni)  
w) a nyilvántartásba vételt követően az adatkezelés megkezdése.

## 5.2.2. Adatbiztonsági szabályok

### 5.2.2.1. Általános irányelvek

Az intézmény az adatok biztonsága és az érintettek magánszférájának védelme érdekében megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek e szabályzat, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az intézmény az adatkezelés során megőrzi

- a titkosságot: megvédi az információt, hogy csak az férhessen hozzá, aki erre jogosult;
- a sértetlenséget: megvédi az információnak és a feldolgozás módszerének pontosságát és teljességét;
- a rendelkezésre állást: gondoskodik arról, hogy amikor a jogosult használónak szüksége van rá, valóban hozzá tudjon férni a kívánt információhoz és rendelkezésre álljanak az ehhez szükséges eszközök.

Az intézmény munkatársai munkájuk során gondoskodnak arról, hogy jogosulatlan személyek ne tekinthessenek be személyes, egészségügyi adatokba, továbbá arról, hogy az adatok tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

Az adatok tárolása és továbbítása során az általános baleset- és tűzvédelmi előírásokat figyelembe kell venni.

Az intézmény által kezelt személyes, egészségügyi, biometrikus adatokhoz:

- a Főigazgató és a Főigazgató által esetleg írásban felhatalmazott személy(ek) teljes körűen férhetnek hozzá, továbbá
- a Belső ellenőrzés a belső ellenőrzési tevékenysége során teljes körűen,
- a Minőségirányítás a minőségügyi auditok során teljes körűen,
- az intézmény megbízott jogi képviselői a jogügylettel érintett személy személyes adatai tekintetében,
- az adminisztratív feladatokat ellátó munkavállalók egyéni jogosultságok alapján,
- a munkáltatói jogkörgyakorlók az érintett munkavállalók személyes adatai tekintetében, illetve
- az adatvédelmi tisztviselő férhet hozzá.

### 5.2.2.2. Fizikai védelem

Papír alapú adathordozón tárolt adatok esetén:

- Az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá, más számára fel nem tárhatóak;
- a személyes, egészségügyi adatokat, keletkezésükkor az adatkezelés céljának megfelelő (formanyomtatvány, stb.) papír alapú adathordozóra kell nyomtatni illetve rögzíteni;
- az adatok olvashatóságáért az azokat felvevő, illetve rögzítő személy felel;
- a személyes, egészségügyi adatokat tartalmazó dokumentumokat az adatkezelés időtartama alatt rendezett formában, jól zárható, száraz, tűzvédelmi és vagyónvédelmi berendezéssel ellátott helyiségben kell tárolni;
- a jogosulatlan hozzáférés megakadályozása érdekében az intézmény adatkezelést végző munkatársa a nap folyamán, illetve a munkavégzés befejeztével csak úgy hagyhatja el az olyan helyiséget, ahol adatkezelés zajlik, hogy a rá bízott adathordozókat elzárja, vagy az irodát bezárja;

Amennyiben a papíralapon tárolt adat kezelésének célja megvalósult, úgy az intézmény intézkedik a dokumentum megsemmisítéséről a Selejtezési Szabályzat szerint.

Ebben az esetben az intézmény kijelöl egy munkavállalót, aki a megsemmisítésért felelős. A megsemmisítésért felelős munkavállaló a megsemmisítéssel érintett szervezeti egység bevonásával állítja össze a megsemmisítendő iratcsomagot. A megsemmisítésen háromtagú megsemmisítési bizottság vesz részt.

Amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat alkalmazza az intézmény.

### 5.2.2.3. Informatikai védelem

Elektronikusan tárolt adatok esetében:

- Az informatikai rendszer üzemeltetőjének a biztonságról szerverszintű és alkalmazásszintű védelmi eljárásokkal kell gondoskodnia. A hálózati rendszer üzemeltetése során biztosítani kell az elektronikusan tárolt adatok maximális védelmét.
- Titkos, illetve bizalmas adatokat, személyes, egészségügyi adatokat, bank-, adótitoknak minősülő adatokat az intézmény a vonatkozó szabályzatokban meghatározott módon védi.
- A személyes, egészségügyi adatok elektronikusan végzett adatfeldolgozása során az Informatika további intézkedésekkel biztosítja
  - a) a jogosulatlan adatbevitel megakadályozását;
  - b) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes, egészségügyi adatokat mely szervereknek továbbították;
  - c) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely adatokat, mikor és ki vitte be az elektronikus adatfeldolgozó rendszerekbe;
  - d) a telepített rendszerek üzemzavara esetén az adatok helyreállíthatóságát és azt, hogy az elektronikus adatfeldolgozás során fellépő hibákról (személyes adatokat nem tartalmazó) jelentés készüljön.
- Szoftverfejlesztés, illetve külső fejlesztőkkel történő együttműködés során a maximális adatbiztonságra kell törekedni.
- A humán kockázat ellen oktatással, a folyamatok megfelelő szabályozásával és ezek betartásának ellenőrzésével, valamint felelősségre vonással kell védekezni.
- A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében az intézmény az alábbi intézkedéseket és garanciális elemeket alkalmazza:
  - az adatkezelés során használt számítógépek az intézmény tulajdonát képezik, vagy azok fölött tulajdonosi jogkörrel megegyező joggal bír az intézmény;
  - a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal - legalább felhasználói névvel és jelszóval – lehet csak hozzáférni, a jelszavak cseréjéről az intézmény rendszeresen, illetve indokolt esetben gondoskodik;
  - lehetőség szerint az adatokkal történő minden számítógépes rekord nyomon követhetően naplózásra kerül;
  - a hálózati kiszolgáló gépen (a továbbiakban: szerver) tárolt adatokhoz csak megfelelő jogosultsággal és csakis az arra kijelölt személyek férhetnek hozzá;
  - amennyiben a nem jogszabályi kötelezettség alá eső adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető;
  - a hálózaton tárolt adatok biztonsága érdekében a szerverek esetén magas rendelkezésre állású infrastruktúrán történő mentésekkel és archiválással kerül el az intézmény az adatvesztést;
  - a személyes adatokat tartalmazó adatbázisok aktív adataiból napi mentést végez, a mentés a központi szerver teljes adatállományára vonatkozik és Network Attached Storage-ra történik;
  - a mentéseket tároló adattár elzárt helyen, a szervertől fizikailag távol, más épületben lett elhelyezve
  - a személyes, egészségügyi adatokat kezelő hálózaton a vírusvédelem folyamatosan biztosított;
  - a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával megakadályozza illetéktelen személyek hálózati hozzáférését.

### 5.2.2.4. Szerverekbiztonsága

Az intézmény az általa kezelt személyes, egészségügyi adatok áramlását elektronikus módon belső hálózaton keresztül, szerverekre történő tárolással valósítja meg. A mentést kiszolgáló NAS-t és a szervereket külön erre a célra kialakított helyiségben kell elhelyezni. Erre a helyiségre vonatkozóan ki kell alakítani egy hozzáférési jogosultsággal rendelkező munkavállalói bázist, akik engedéllyel férhetnek hozzá ezekhez az eszközökhöz és esetlegesen a rajtuk tárolt adatokhoz.

A szerverszobába való belépési jogosultságot a munkavállalónak külön kell igényelnie, amit a Főigazgatónak (az adatvédelmi tisztviselővel, egyetértésben) kell elbírálnia.

A helyiségbe csak a Főigazgató engedélyével rendelkező személy léphet be.

A személyes, egészségügyi adatok tárolásának helyén, a szerverszobákban tárolt szerverek fizikai védelme érdekében az intézmény az alábbi intézkedéseket és garanciális elemeket alkalmazza:

- a szerverszoba klimatizált és tűzjelző berendezéssel ellátott,
- a szerverszobába csak engedéllyel rendelkező személy veheti át a kulcskezelési szabályok alapján a kulcs kezelőjétől a szerverszoba kulcsát,
- a kulcsfelvételtől nyilvántartást vezet az intézmény
- aki nem az intézménnyel szerződött, az nem rendelkezhet kulcsfelvételi engedéllyel,

Kulcsfelvételi engedéllyel nem rendelkező személy csak kulcsfelvételi engedéllyel rendelkező munkavállaló jelenlétében tartózkodhat a szerverszobában.

#### 5.2.2.5. Jogosultságkezelés

A jogosultságkezelés szabályozásának célja, hogy a kiosztott jogosultságok pontosan nyomon követhetők legyenek, dokumentált formában megőrzésre kerüljenek, valamint az egyes jogosultságokkal rendelkező személyek tevékenysége és az általuk felhasznált adatok köre ellenőrizhető legyen. Ezen adatok naprakésztsége nagymértékben hozzásegíti az intézményt a tőle elvárt, illetve általa elérhető biztonsági szint teljesítéséhez, továbbá az informatikai hálózat törvényi és szakmai normák szerinti üzemeltetéséhez.

A szabályozás kiterjed az elektronikus megfigyelőrendszerek informatikai rendszerére és az azokhoz csatlakozó eszközökre.

Az informatikai rendszerben a jogosultságok változásait (új jogosultságok kiosztása, módosítása, megszűnése) dokumentálni kell.

A személyes adatok biztonsága érdekében az intézmény az alábbi jogosultságkezelési előírásokat alkalmazza:

Alapelvek

- Új jogosultság beállítását, illetve jogosultság megváltoztatását a Főigazgató felhatalmazása alapján az adatvédelmi felelős indíttványozza, az adatvédelmi tisztviselő engedélyezi és az ezzel a feladattal megbízott informatikus végzi. (7.6 számú melléklet)
- A jogosultságok megállapítása során kizárólag a munkavégzéshez szükséges és elégséges jogosultságokat kell kiosztani.
- El kell kerülni, hogy teljes hozzáférést, illetve adminisztrátori jogosultságokat kapjanak más munkát végző, illetve a jogosultság birtoklására igényt nem tartó személyek.
- Adminisztrátori jogosultsággal rendelkező nevesített felhasználót kell alkalmazni a rendszer adminisztrálása érdekében minden esetben..

#### 5.2.2.6. Jogosultságkezelési folyamat

A jogosultságkezelési folyamatot az Intézmény a Információ Biztonsági Politikában leírtak szerint végzi.

A jogosultság birtokosa munka vagy jogviszonya megszűnésével közvetlen felettesének kötelessége értesítene az adott szervezeti egység adatvédelmi felelősét a jogosult eddig birtokolt jogosultságai törlésének kezdeményezéséről.

A jogosultság megszűnése esetén az adatvédelmi felelős a megszüntetési kérelmet formanyomtatványon küldi meg az adatvédelmi tisztviselőnek, aki gondoskodik a jogosultság törlésének végrehajtásáról. Áthelyezés esetén a korábbi munkakör feletti munkáltatói jogokat gyakorló felettes és az új munkakör feletti munkáltatói jogokat gyakorló felettes egyetemlegesen kötelesek gondoskodni az adatvédelmi felelős bevonásával a régi jogosultságok törlésének, módosításának vagy új jogosultságok felvételének kezdeményezéséről.

Az informatikai rendszerben a kilépő felhasználók profiljait fel kell függeszteni, használaton kívül kell helyezni. A felhasználói fiókok törlése a rendszerek ellenőrzését követően történhet meg, ha a törlés nem okoz adatvesztést.

### 5.2.3. 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, és technikai és szervezési intézkedések megtételével biztosítja, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.

Az álneven 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 kötelezettségeiknek.

Az álnevesítés személyes, egészségügyi 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 intézmény 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.

### 5.2.4. Beépített adatvédelem

Bevezetésre kerül az ún. beépített adatvédelem, melynek következtében az intézmény már az adatkezelés tényleges megkezdése előtt – például már a projektelőkészítés 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, egészségügyi 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 jogszabályi előírásokat betartva, 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 tovább fejleszthesse azokat.

Az adatkezelésnek átláthatónak és felhasználó-központúnak, az adatvédelemnek proaktívnak kell lennie, és az adat teljes életciklusát fel kell ölelnie, vagyis a teljes folyamatnak része kell, hogy legyen.

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 valószínűsű és súlyosságú kockázat figyelembevételével, mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket –

- a) a személyes, egészségügyi adatok álnevesítését és titkosítását;
- b) az adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy az adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást

- 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 adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy az 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 előbbieken előírt követelményeket.

Az intézmény és az adatfeldolgozó intézkedéseket hoz annak biztosítására, hogy az intézmény vagy az adatfeldolgozó irányítása alatt eljáró, az 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 a intézmény.

#### 5.2.5. Mobil eszköz menedzsment

Az adatvédelmi szabályozás szempontjából a mobil eszköz menedzsment területén az intézmény üzletmenetéhez fontos szolgáltatások, műszaki technikai, informatikai biztosítása mellett adatvédelmi szempontból fontos kötelezettség keletkezik, azaz biztosítani kell az intézmény birtokába kerülő adatok titkosságát, sérthetetlenség és a biztonságot garantáló keretrendszerben való működését.

Az intézmény rendszerében mobilmenedzsment szolgáltatásoknak az alábbi kritériumoknak kell megfelelnie:

- összetett és rendszeresen változó jelszóhasználat kikényszerítése
- használati eszközök automatikus kiléptetése
- titkosítás használata a rendszerben levő eszközökön
- adatok távoli törlésének lehetősége (csak a céges adatokra, vagy az összes adatra vonatkozóan)
- eszköz távoli letiltása

#### 5.2.6. Adatvédelmi incidens kezelése

##### 5.2.6.1. 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 az adatvédelmi felelősöknek vagy az adatvédelmi tisztviselőnek, aki értesítést küld a Főigazgatónak.

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. („Adatvédelmi incidens/rendkívüli esemény jelentő lap” 7.3 számú melléklet)

A bejelentés adatvédelmi tisztviselőhöz érkezését követően az adatvédelmi tisztviselő haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását és értékelését.

##### 5.2.6.2. Adatvédelmi incidens kivizsgálása, értékelése

Az adatvédelmi tisztviselő 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, az adatvédelmi incidens egyéb körülményeit, az adatvédelmi incidens által érintett adatok körét, mennyiségét, az adatvédelmi incidenssel érintett személyek körét és számát, az adatvédelmi incidens 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.

Amennyiben az adatvédelmi incidens értékelése vizsgálatot igényel az adatvédelmi tisztviselő lefolytatja a vizsgálatot. A vizsgálatnak tartalmaznia kell, hogy az adatvédelmi incidens magas kockázattal jár-e az érintettek jogaira és kötelezettségeire, milyen jellegű kockázatról van szó és szükséges-e az érintettek tájékoztatása az incidensről. Amennyiben nem szükséges az érintettek tájékoztatása, a vizsgálatnak tartalmaznia kell ennek indokait is.

A vizsgálat eredményeként az adatvédelmi tisztviselő javaslatot tesz az adatvédelmi incidenssel érintett szervezeti egység vezetőjének az incidens kezeléshez szükséges intézkedések megtételére.

A javaslat alapján a megvalósítandó további intézkedésekről az adatok kezelését vagy feldolgozását végző szakterület vezetője egyetértésével dönt.

A vizsgálatot legkésőbb a bejelentés adatvédelmi tisztviselőhöz érkezésétől számított 72 órán belül be kell fejezni és a vizsgálat eredményéről az intézmény Főigazgatóját az adatvédelmi tisztviselő tájékoztatja.

### 5.2.6.3. Az adatvédelmi incidens nyilvántartása

Az adatvédelmi incidensekről az adatvédelmi tisztviselő nyilvántartást vezet.

Az adatvédelmi incidens-nyilvántartást („Adatvédelmi incidens bejelentő -nyilvántartó lap” melléklet) az adatvédelmi tisztviselő vezeti.

A nyilvántartás tartalmazza:

- az érintett személyes adatok körét,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens időpontját,
- az adatvédelmi incidens körülményeit, hatásait,
- az elhárítására megtett intézkedéseket és
- egyéb jogszabályban előírt adatokat.

Az adatvédelmi incidensnyilvántartás pontos vezetéséről, aktualizálásáról az adatvédelmi tisztviselő gondoskodik.

### 5.2.6.4. Az adatvédelmi incidens bejelentése a Hatóság részére

Az adatvédelmi tisztviselő az adatvédelmi incidenst a tudomásra jutását követően haladéktalanul, de legkésőbb az incidens tudomásra jutásától számított 72 órán belül bejelenti a Hatóság részére, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg határidőben, az adatvédelmi tisztviselő köteles ennek okát igazolni a Hatóság részére.

A Hatósági bejelentésnek tartalmaznia kell:

- az adatvédelmi incidenssel érintett adatok körét és hozzávetőleges számát,
- az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát,
- az adatvédelmi incidens jellegét, körülményeit,
- az adatvédelmi tisztviselő nevét és elérhetőségét,
- az adatvédelmi incidens valószínűsíthető következményeit és
- az adatvédelmi incidens orvoslására és enyhítésére megtett intézkedéseket.

### 5.2.6.5. Az érintettek tájékoztatása az adatvédelmi incidensről

Ha a vizsgálat eredményeként megállapítást nyert, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve és az érintettek tájékoztatása szükséges, az adatvédelmi tisztviselő haladéktalanul értesíti az érintetteket és erről az



intézmény igazgatóját.

Nem kell az érintetteket tájékoztatni:

- ha az intézmény olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét.
- ha az adatvédelmi incidens bekövetkezését követően az intézmény olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg.
- ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton is megtörténhet.

### 5.2.7. 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 új adatkezelésért felelős szervezeti egysége hatásvizsgálatot folytat le arra vonatkozóan, hogy az adatkezelési folyamat a személyes adatok védelmét hogyan érinti. Egymáshoz hasonló adatkezelési műveletek, amelyek hasonló kockázatokat jelentenek egy 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 javaslatát.

Az intézmény a NAIH honlapjáról letöltött PIA program segítségével és szempontrendszerének figyelembevételével elvégzi a hatásvizsgálatot.

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

Az adatok kezelésével kapcsolatosan az intézmény kötelezettsége továbbá a kockázatelemzés, amelynek lépései a következők:

- az 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 kockázatelemzési rendszer kialakításáig, amelyben teljes kockázatpotenciál és kockázat prioritási sorrend (nem az intézkedési rendszerrel azonos) megállapítása kell, hogy megtörténjen. Az elemzés menetét és eredményeit írásba kell foglalni.

A kockázatpotenciálnál meg kell határozni a valószínűség szempontjából

- kicsi
- közepes
- és nagy valószínűséggel bekövetkező kockázatokat,

illetve horderő szempontjából

- kicsi
- közepes
- és nagy horderőjű 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.

### 5.2.8. 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 résztvevő adatkezelő(k), adatfeldokgozó(k) feladatköreinek felsorolását,
- az adatkezelés célját, módját és az érintettek jogai, szabadságai biztosításának védelmében hozott intézkedéseket, garanciákat.

### 5.2.9. Érdekmérlegelés

A GDPR rendelkezései szerint lehetőség van hozzájárulás nélküli adatkezelésre, ha ezt valamilyen jogos érdek lehetővé teszi, feltéve, hogy a intézmény eleget tesz tájékoztatási kötelezettségének. Az adatkezelés jogalapjának vizsgálata során a GDPR 6. cikk (1) bekezdése a)-f) pontjai az irányadók.

Amennyiben a jogalapot a jogos érdek érvényesítése jelenti, az adatkezelési folyamat akkor és annyiban lesz jogszerű, amennyiben az adatkezelés az intézmény 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.

Az adatkezelés jogszerűségének vizsgálatához az adatkezeléssel érintett szervezeti egység elvégzi egy érdekmérlegelési tesztet, mely során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását vizsgálja és megfelelően alátámasztja.

Az érdekmérlegelési teszt során azonosítani kell az intézmény jogos érdekét 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. A mérlegelés során figyelembe kell venni különösen a kezelt, illetve kezelendő adat természetét és szenzitív jellegét, nyilvánosságának mértékét, az esetlegesen bekövetkező szabálysértés súlyosságát, stb.

Az érdekmérlegelési teszt részeként a szükségesség és arányosság vizsgálatát is el kell végezni, amelynek értelmében a személyes adatok védelme alóli kivételeknek és a védelem korlátozásainak a feltétlenül szükséges mérték határain belül kell maradniuk. 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 kell megállapítani, hogy kezelhető-e az adat.

A teszt eredményéről az érintettek tájékoztatást kapnak, melyből egyértelműen kiderül, hogy mely jogos érdek alapján és miért tekinthető arányos korlátozásnak az, hogy az intézmény az érintett beleegyezése nélkül kezeli a személyes adatot, tehát az intézmény adatkezeléséhez fűződő jogos érdeke miért múlja felül az érintett érdekeit, illetve jogait. A hozzájárulás hiányára tekintettel az érintetteket tájékoztatni kell az alkalmazott adatvédelmi garanciákról és az adatkezelés elleni tiltakozás lehetőségeiről.

Nem írható elő az ellentétes érdekek és jogok közötti súlyozás eredménye anélkül, hogy eltérő eredményt tenne lehetővé az intézmény az adott eset sajátos körülményeire tekintettel, ezért az intézmény minden egyes esetben külön érdekmérlegelési tesztet végez el.

Az érdekmérlegelési teszt elvégzésének lehetséges lépései:

1. lépés: az intézmény a tervezett adatkezelés megkezdése előtt áttekinti, hogy a célja elérése érdekében feltétlenül szükséges-e személyes adat kezelése: rendelkezésre állnak-e olyan alternatív

megoldások, amelyek alkalmazásával személyes adatok kezelése nélkül megvalósítható a tervezett cél.

2. lépés: az intézmény a jogos érdekét a lehető legpontosabban meghatározza.
3. lépés: az intézmény meghatározza, hogy mi az adatkezelés célja, milyen személyes adatok, meddig tartó adatkezelését igényli a jogos érdek.
4. lépés: az intézmény felméri és meghatározza, hogy az érintetteknek mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (például azok a szempontok, amelyeket az érintettek felhozhatnának az adatkezeléssel szemben).
5. lépés: az intézmény elvégzi jogos érdekeinek és az érintettek érdekeinek, alapjogainak súlyozását és ez alapján megállapítja, hogy a személyes adat kezelhető-e. Az intézmény meghatározza, hogy miért korlátozza arányosan az intézmény jogos érdeke – és az ennek alapján végzett adatkezelés – a 4. lépésben meghatározott érdekelti jogokat, várakozásokat.
6. lépés: az intézmény meghatározza, mely garanciák biztosíthatják az adatkezelés szükségességét-arányosságát (természetesen más garanciális intézkedések is alkalmazhatók).

Az intézmény az adatvédelmi érdekmérlegelési tesztben leírt szempontrendszer figyelembevételével végzi el az érdekmérlegelést.

#### 5.2.10. Adatvédelmi ismeretek oktatása

Kiemelt területként kell kezelni a munkavállalók kapcsán a biztonságtudatosági 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 munkavállalóknak is hozzá kell járulniuk.

A munkavállalók megfelelő képzése a képzést követően kimutathatóan kevesebb biztonsági incidenst eredményez, ami a közvetlen adatvesztésből és esetleges adatvédelmi bírságból eredő károkon túl a pénzügyi eredményekben is nyilvánvalóan megmutatkozik.

A munkavállalók általános adatvédelmi-információbiztonsági tréning rendje évente (kapcsolható más rendszeres képzésekhez, tréningekhez pl. tűz- és munkavédelem) egy óra időtartamban történjen. Ez vonatkozik az informatikai és nem informatikai munkavállalókra egyaránt.

### 5.3. Az adatvédelem szervezeti rendszere – az adatkezelésben közreműködők és feladataik

#### 5.3.1. A Főigazgató

- a) ellátja az intézmény adatvédelmi rendszerének felügyeletét egy általa megbízott adatvédelmi tisztviselő útján;
- b) felelős az érintettek GDPR-ban meghatározott jogainak gyakorlásához szükséges feltételek biztosításáért;
- c) felelős az intézmény által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért;
- d) felelős az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért;
- e) felügyeli az adatvédelmi tisztviselő tevékenységét;
- f) vizsgálatot rendelhet el;
- g) kiadja az intézmény adatvédelemmel kapcsolatos belső szabályait.

### 5.3.2. Az adatvédelmi tisztviselő

Az adatvédelmi tisztviselő az intézménnyel kötött megbízási szerződés alapján látja el a tevékenységét. Az adatvédelmi tisztviselő független, függetlensége biztosítása érdekében szakmai feladatai ellátása során utasítást nem fogadhat el, szakmai feladatai ellátásával összefüggésben nem bocsájtható el. Jelen szabályzatban foglalt tevékenysége ellátása során autonóm, szakmai ügyekben kizárólag a Főigazgatónak tartozik felelősséggel. A intézmény biztosítja az adatvédelmi tisztviselő részére a feladat ellátásához szükséges forrásokat, valamint biztosítja számára, hogy a feladatai ellátása során utasításokat senkitől ne fogadjon el, ezen feladatai ellátásával összefüggésben nem bocsátható el és szankcióval nem sújtható. Az adatvédelmi tisztviselő esetében a Ptk. megbízásra vonatkozó szabályait kell alkalmazni. Az intézmény az adatvédelmi tisztviselő nevét és elérhetőségét közzéteszi a honlapján, valamint bejelenti ezen adatokat a NAIH részére.

Az adatvédelmi tisztviselő

- a) segítséget nyújt az érintett jogainak biztosításában;
- b) minden év január 15-ig jelentést készít a Főigazgató részére a intézmény adatvédelmi feladatainak végrehajtásáról;
- c) figyelemmel kíséri az adatvédelemmel és információszabadsággal kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi jelen szabályzat módosítását, illetve a jogszabályváltozások esetén jelzést intéz a Főigazgató felé és javaslatot tesz az azokkal kapcsolatos módosítások beillesztésére;
- d) elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot, továbbá a közérdekű adatok kezelésének és közzétételének rendjéről szóló szabályzatot, illetve elkészíti azok szükség szerinti módosítását;
- e) jogosulatlan adatkezelés észlelése esetén jelzést intéz a Főigazgató felé, és javaslatot tesz azok megszüntetésére;
- f) a szervezeti egységekben kijelölt adatvédelmi felelősök vezetőjeként megbeszélést kezdeményezhet az adatvédelemmel kapcsolatos tevékenységekkel, azok felülvizsgálatával kapcsolatban;
- g) kivizsgálja a hozzá érkezett bejelentéseket;
- h) intézi a hozzá beérkező, érintetti jogokkal kapcsolatos megkeresések megválaszolását
- i) közreműködik a NAIH-tól az intézményhez érkezett megkeresések megválaszolásában és a NAIH által kezdeményezett vizsgálat, illetve adatvédelmi hatósági eljárás során;
- j) általános állásfoglalás megadása céljából megkeresést fogalmaz meg a NAIH felé, amennyiben egy felmerült adatvédelmi kérdés jogértelmezés útján egyértelműen nem válaszolható meg;
- k) évente január 31-ig a Hatóság részére tájékoztatást küld a megelőző évben elutasított tájékoztatási kérelmekről;
- l) tájékoztatást és szakmai tanácsot ad a intézmény adatvédelmi jogszabályokban előírt kötelezettségeinek ellátásával kapcsolatban;
- m) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
- n) segítséget nyújt a belső adatvédelmi nyilvántartás vezetéséhez;
- o) nyilvántartást vezet az adatvédelmi incidensekről;
- p) az intézmény adatkezelési folyamatai során érvényt szerez az adatkezelés érintettjeinek adatkezelési aspektusból felmerülő jogos érdekeinek;
- q) véleményezi a részére megküldött, adatvédelmi kérdéseket érintő szabályzattervezeteket;
- r) ellenőrzi a GDPR és az adatkezelésre vonatkozó nemzeti szabályozás elemeinek érvényesülését a intézmény adatkezelési folyamataival kapcsolatban;
- s) 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;
- t) munkája során együttműködik az érintett szakterületek munkavállalóival;
- u) gondoskodik az adatvédelmi ismeretek oktatásáról, illetve 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 kapcsolatban tájékoztatást ad, illetve az ismereteket ellenőrzi,
- v) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon

- követi a hatásvizsgálat elvégzését;
- w) együttműködik a NAIH-val;
  - x) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a NAIH felé, valamint bármely egyéb kérdésben konzultációt folytat le.
  - y) Új adatkezelő belépésekor, illetve a felhasználóhoz rendelt hozzáférés kérés szükségessége esetén az erre rendszeresített űrlapon a kérést jóváhagyja, megszüntetés/passzíválás esetén tudomásul veszi (7. sz. melléklet), az Informatikai részleget haladéktalanul értesíti
  - z) Rendszeres időközönként az információ-technológiai (IT) fejlesztési igények megbeszélése különös tekintettel a biztonsági kérdésekre.
  - aa) Adatbiztonsággal érintő beruházási témák megbeszélése, javaslattétel, különös tekintettel a biztonsági kérdésekre.

Feladatai ellátása során jogosult teljes mélységben betekinteni az intézménynél végzett összes adatkezelés és adatfeldolgozás anyagaiba, és jogosult teljes körű tájékoztatást kapni a vizsgált adatkezelésekről. Minden olyan adatkezelést megismerhet, amely személyes, egészségügyi adatokkal összefüggő, és minden helyiségbe beléphet, ahol adatkezelés folyik.

Az adatvédelmi felelős:

- a. Az általa felügyelt egység adatkezelőivel az Adatvédelmi és Adatkezelési Szabályzat és Felhasználói Biztonsági Kézikönyv megismertetése és betartatása, az adatkezelők adatvédelmi oktatása, illetve az adatbiztonsági adatvédelmi feladatok folyamatos belső ismertetése.
- b. Az intézmény Adatvédelmi és adatkezelési Szabályzatában meghatározott és az adatvédelemmel kapcsolatos egyes dokumentumok kezelése, naprakészen tartása.
- c. Engedélyeztetési, jóváhagyási eljárások kezdeményezése és megszervezése.
- d. A különböző munkakörökben folytatandó adatvédelmi tevékenység koordinálása.
- e. Az általa felügyelt egységben keletkezett és manuálisan kezelt egészségügyi dokumentáció tárolására, archiválására vonatkozó helyi szabályozás kialakítása, az adatkezelőkkel való megismertetése, valamint a szabályozási rend betartásának ellenőrzése.
- f. A hatáskörébe tartozó számítástechnikai védelmi tevékenység folyamatos és tervszerű ellenőrzése.
- g. Az adatvédelemmel kapcsolatos problémákat írásban jelzi az Adatvédelmi Tisztviselőnek
- h. Új adatkezelő belépésekor, illetve a felhasználóhoz rendelt hozzáférés kérés (jogosultsági szint meghatározásával) ill. törlés/passzíválás szükségessége esetén az erre rendszeresített űrlapon jóváhagyásra, tudomásul vételre elküldi az Adatvédelmi Tisztviselőnek (7.6 sz. melléklet)
- i. Nyilvántartja az általa felügyelt egységben lévő adatkezelőket a 7.5. sz. mellékletben szereplő nyomtatvány felhasználásával
- j. Az Adatvédelmi és adatkezelési Szabályzat módosítására tett és hozzá érkezett javaslatot az Adatvédelmi Tisztviselőnek továbbítja.
- k. Haladéktalanul jelentést tesz az Adatvédelmi Tisztviselőnek az adatvédelemmel kapcsolatos rendkívüli eseményről a 3. sz. mellékletben szereplő formanyomtatvány felhasználásával.
- l. Az elveszett, eltulajdonított, megsemmisült dokumentumokról és az eset körülményeiről készített jegyzőkönyv egy példányát haladéktalanul eljuttatja az Adatvédelmi Tisztviselőnek.

### 5.3.3. Személyes, egészségügyi adatokkal kapcsolatos adatkezelést ténylegesen végző munkavállaló

- a) köteles gondoskodni arról, hogy munkája során jelen szabályzat előírásai érvényesüljenek, biztosítva, hogy az adatot tartalmazó dokumentum, adathordozó előírászerűen legyen kezelve, tárolva, megsemmisítésre előkészítve;
- b) gondoskodik az érintett részére, adatainak kezeléséről szóló előzetes tájékoztatás megadásáról;
- c) Nem szükséges külön adattovábbítási nyilvántartás készítése, amennyiben az adattovábbítások a rendszerből egyértelműen kimutathatók.
- d) az adatkezelést a Felhasználói Biztonsági Kézikönyvben leírtak szerint végzi.

### 5.4. Az intézménynél megvalósuló adatkezelések

Az intézmény tevékenység ellátása kapcsán magánszemélyekkel kapcsolatba kerül.

Az adatkezelés helye: 9330 Kapuvár, Dr. Lunniczter Sándor utca 10. Lunniczter Sándor Kórház-Rendelőintézet és telephelyei

Az adatvédelmi tisztviselő által vezetett belső adatvédelmi nyilvántartás, adattérkép az intézménynél végzett adatkezelések részleteit tartalmazza.

#### 5.4.1. A munkavállalók személyes adatainak kezelése

##### 5.4.1.1. Általános irányelvek

A munkavállalótól csak olyan nyilatkozat megtétele vagy adat közlése kérhető, amely személyiségi jogát nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges. A munkavállalóval szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet munkaviszonyra vonatkozó szabály ír elő, vagy amely munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.

Törvényi felhatalmazás hiányában az adatkezelés alapjául kizárólag a munkavállaló megfelelő tájékoztatáson alapuló, önkéntes és határozott - különleges adat esetén írásbeli – hozzájárulása szolgálhat, amelyben félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok meghatározott célból és körben történő kezeléséhez.

A munkáltató köteles a munkavállalót tájékoztatni személyes adatainak kezeléséről, az adatkezelések részleteiről. A felvétel során, kifejezetten a intézmény munkavállalói részére összeállított, egyedi adatkezelési tájékoztatót kell a munkavállalónak dokumentáltan átadni.

A munkáltató a munkavállalóra vonatkozó tény, adatot, véleményt harmadik személlyel csak törvényben meghatározott esetben vagy a munkavállaló hozzájárulásával közölhet.

A munkaviszonyból származó kötelezettségek teljesítése céljából a munkáltató a munkavállaló személyes adatait - az adatszolgáltatás céljának megjelölésével, törvényben meghatározottak szerint - adatfeldolgozó számára átadhatja. Erről a munkavállalót előzetesen tájékoztatni kell.

A munkavállalóra vonatkozó adatok statisztikai célra felhasználhatók és statisztikai célú felhasználásra - hozzájárulása nélkül, személyazonosításra alkalmatlan módon - átadhatók.

Az intézmény köteles biztosítani, hogy a munkavállaló a róla kezelt adatokat megismerhesse, a kezelt adatokat tartalmazó iratokról másolatot vagy kivonatot kaphasson. Ugyanakkor gondoskodni kell a munkavállalók akár papír alapon, akár elektronikusan tárolt személyes adataihoz történő, intézményen belüli jogosulatlan hozzáférés megakadályozásáról.

A munkáltató a munkavállalót csak a munkaviszonnyal összefüggő magatartása körében ellenőrizheti. A munkáltató ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkavállaló magánélete nem ellenőrizhető. A munkáltató előzetesen tájékoztatja a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak. Amennyiben a bevezetésre kerülő technikai ellenőrzés a munkavállalók nagyobb csoportját érinti, abban az esetben a szakszervezetet tájékoztatni kell.

A munkaviszony létesítésének bármely okból történő meghiúsulása esetén, a felvételi eljárás során rögzített személyes adatokat 8 munkanapon belül törölni kell, kivéve, ha azok további kezeléséhez az érintett kifejezett hozzájárulását adta, illetve amennyiben arra jogszabályi előírás teljesítése érdekében van szükség.

A munkaviszonnyal kapcsolatos adatkezelés célja a munkaviszony létesítése, fenntartása és megszüntetése.

##### 5.4.1.2. Személyazonosító igazolványok fénymásolása

A kórházban a munkavállalók végzettségét igazoló iskolai bizonyítványainak, erkölcsi bizonyítványának és okmányainak másolásának kérdéskörével a NAIH/2018/3654/2/V. ügyszámú állásfoglalás foglalkozik, mely szerint ezek másolása nem szükséges (adattakarékosság elve alapján), tekintettel arra, hogy a munkáltató szempontjából elegendő a végzettség tényének rögzítése, továbbá a másolatok hitelesnek sem tekinthetők. Alkalmazható a "négy szem elve" is, amikor két ügyintéző tekinti meg a bemutatott iratot.

### 5.4.1.3. Erkölcsei bizonyítványok kezelése

Az intézmény jogszabályi előírás vagy egyéb jogviszony teljesítésének okán fenntartja magának a jogot, hogy olyan munkavállalót alkalmazzon, aki erkölcsileg megfelel az elvárásainak, ezért az intézmény a munkaerő-felvételt tiszta erkölcsi bizonyítvány meglétéhez kötheti.

A tiszta erkölcsi bizonyítvány ellenőrzését a munkaügyi előadó végzi, ellenőrzi az erkölcsi bizonyítvány:

- érvényességét (bárki számára elérhető módon), illetve
- annak tartalmát.

Az intézmény bűnügyi személyes adatot csak az érintett írásbeli hozzájárulásával kezel. Az intézmény előzetesen tájékoztatja az érintettet, hogy a bűnügyi személyes adat kezelésének célja az adott munkakörre való érdemesség eldöntése, így ezen adatot csak a cél megvalósulásáig, a döntésig kezeli.

Az intézmény csak az adott, konkrét munkakör feltételeként köti ki a büntetlen előéletet. Egyes méltányolható esetekben azonban az intézmény Főigazgatója, egyedi elbírálás során dönthet a munkakörre való alkalmasság megítélése mellett akkor is, ha olyan bejegyzés található az erkölcsi bizonyítványban, amely

- az elkövetett cselekmény fajtájától és súlyától függően a betöltendő munkakörben elvártakkal nem összeegyeztethetetlen,
- a bírósági mentesítési időszakában tart,
- a törvényi mentesítési idő beálltához közel van,
- egyéb méltányolható indoknál fogva nem veszélyezteti az intézmény céljait és elveit.

A munkára való jelentkezés során az adatok az alábbiak alapján a döntési jogkörrel rendelkező személyhez kerülnek. A munkakörre való alkalmasság elbírálása a szakmai vezetők és a munkaügyi előadó jogköre. A munkára jelentkezés során megadott adatokat így csak a szakmai vezetők, a Humánpolitikai előadó és a fent ismertetett különleges esetekben az intézmény Főigazgatója ismerhetik meg.

Az adatokhoz az itt megjelöltekén kívül senki sem férhet hozzá, így az Intézmény más munkavállalója vagy egyéb, az intézménnyel más jogviszonyban álló személy azokat semmilyen módon és formában nem ismerheti meg.

Az érintett a meghatározott munkakörre vonatkozó munkaviszony létesítése során benyújtja érvényes erkölcsi bizonyítványát is. Mivel a munkakörre való alkalmasságról a szakmai vezetők és a Humánpolitikai előadó dönt, ezért hozzájuk az összes adatnak el kell jutnia. Az intézmény azonban minden esetben keresi a lehető legjobb módszert arra, hogy ne korlátozza az érintett magánszféráját, s mivel egy érvényes erkölcsi bizonyítvány a kiállításától számított 90 napon belül felhasználható az intézményhez történő jelentkezésen kívüli más célokra is, ezért az intézmény papír alapon nem iktatja be az érintett erkölcsi bizonyítványt.

Amennyiben különleges méltányolást igénylő esetben a munkaviszony létesítésével kapcsolatos eljárás során az érintett nem tud erkölcsi bizonyítványt bemutatni, úgy azt postán is megküldheti hiánypótlásként a intézménynek. Ebben az esetben 30 napos határidőn belül

- a szakmai vezető dönt a munkaviszonyról,
- a dokumentum a döntési eljárás zárultával postai úton, utólag is nyomon követhető módon visszaküldésre kerül az érintettnek.

Annak érdekében, hogy a intézmény bizonyítani tudja, hogy

- a felvételi eljárás során megvizsgálta az erkölcsi bizonyítvány érvényességét,
- a felvételi eljárás során milyen elérhető adatok alapján ítélte meg a leendő munkavállalót,

az alábbi adatokat a munkaviszony fenntartásához szükséges adatokkal együtt, azonos tárolási módon és tárolási határidővel rögzíti:

- erkölcsi bizonyítvány kiállításának dátuma
- erkölcsi bizonyítvány okmányszáma
- erkölcsi bizonyítvány kérelem azonosítója

Ezen adatok a GDPR szerint azonban nem számítanak különleges személyes adatnak, mert nem bűnügyi személyes adatok. Ezen adatok alapján a BM Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság rendszerében utólag minden, 2013. január 1-je után kiállított erkölcsi bizonyítvány

valódisága és tartalma ellenőrizhető.

Az intézmény így sem a felvételi eljárás során, sem a munkaviszony kapcsán nem tárol erkölcsi bizonyítványt, sem az erkölcsi bizonyítványról készült másolatot.

Abban az esetben, ha a munkára jelentkező érintett nem kerül kiválasztásra, úgy az ő adatait, azaz az erkölcsi bizonyítvánnyal kapcsolatos adatait az intézmény haladéktalanul törli a kiválasztási folyamat végeztével.

Amennyiben a jövőben olyan munkakörre történő jelentkezéshez használja fel intézmény az érintett adatait, ahol az érintettnek tiszta erkölcsi bizonyítványra van szüksége, úgy az érintettet ismét egy érvényes erkölcsi bizonyítvány bemutatására kérheti fel.

#### 5.4.1.4. Egészségügyi alkalmassággal kapcsolatos egészségügyi adatok kezelése

Az egészségügyi alkalmassággal kapcsolatos adatokat az intézmény nem ismeri meg, és nem kezeli egyetlen érintett adatát a célon túlterjeszkedő mértékben. Az intézmény az egészségügyi alkalmasság eldöntése céljából egészségügyi szolgáltatótól származó alkalmassági eredmény alapján dönt az adott (leendő) munkavállaló egészségügyi alkalmasságáról. Az intézmény csak az egészségügyi alkalmasság tényét bizonyító adatot kezeli.

Amennyiben a munkaszerződés megkötésének folyamata során derül ki, hogy az adott érintett alkalmatlan a munkakör betöltésére, ezért a munkaviszony nem jön létre vagy ennek hatására szűnik meg, úgy az adatkezelés határideje és módja is ehhez igazodik.

A munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről szóló 33/1998. (VI. 24.) NM rendelet hatálya kiterjed az intézményre, mint a munkavédelemről szóló 1993. évi XCIII. törvény 87. § 9. pontja szerinti szervezett munkavégzés (a továbbiakban: szervezett munkavégzés) keretében munkavállalót foglalkoztató munkáltatóra.

A rendelet 4. §-ában meghatározott esetekben előzetes munkaköri alkalmassági vizsgálatot kell végezni.

A rendelet 6. §-ában meghatározott esetekben időszakos munkaköri alkalmassági vizsgálatot kell végezni.

A rendelet 7. §-ában meghatározott esetekben soron kívüli munkaköri vagy szakmai alkalmassági vizsgálatot kell végezni.

Az intézmény a rendelet alapján köteles továbbítani a vizsgálatban érintett személy (leendő munkavállaló, munkavállaló) adatait, ezt a kötelezettségét a rendelet írja elő: a 15. § (6) szerint az intézmény, mint munkáltató a munkaköri alkalmasságot vizsgáló és véleményező szerv kérésére mindazokat a munkaköri és munkahelyi adatokat közli, amelyeket a véleményezéshez szükségesnek tart, illetve amit a véleményező kér. Az egészségügyi szerv a tudomására jutott nem egészségügyi adatokat nem hozhatja nyilvánosságra.

Az intézmény azonban ebben az esetben nem válik a GDPR 4. cikk 15. szerinti különleges (egészségügyi) személyes adat kezelőjévé, mert a rendelet 13. § (4) szerint a vizsgálatokat a foglalkozás-egészségügyi alapszolgáltatás nyújtására jogosult orvos végzi, aki a véleményt és a korlátozásokat, a munkaköri, illetve szakmai alkalmasságot véleményező szerv a rendelet 12. számú melléklet szerinti, az „Elsőfokú munkaköri orvosi alkalmassági vélemény” elnevezésű nyomtatványon közli az intézménnyel, mint a munkáltatóval. A nyomtatványon csak a munkavállaló neve, születési ideje, munkaköre és az alkalmasság ténye szerepel.

Bár a rendelet 13. § (5) felhatalmazást ad a munkaköri alkalmasság vizsgálatát végző számára, hogy az alkalmatlanság okát a vizsgált személy írásbeli hozzájárulásával közölje munkáltatóval, de az intézmény még a vizsgált személy írásbeli hozzájárulásával sem kezeli semmilyen esetben sem a különleges személyes adatokat.

#### 5.4.1.5. Megváltozott munkaképességű munkavállalók

A megváltozott munkaképességű munkavállalókra adatkezelési szempontból azonos szabályok vonatkoznak, mint az intézmény saját alkalmazottjaira, rájuk vonatkozóan azonban bővebb a kezelt adatok köre: lásd a kezelt adatok körében. (Az intézmény törvényi előírás alapján kezeli a megváltozott munkaképességű munkavállalók egészségi állapotára vonatkozó adatokat.)

Megváltozott munkaképességű munkavállalók esetében a megváltozott munkaképességű személyek



ellátásairól és egyes törvények módosításáról szóló 2011. évi CXCI. törvény 21. §, 21/A. §, 21/B. § alapján a munkavállalókról kötelezően kezelendő adatkör kiegészül az alábbiakkal:  
szakértői bizottság szakvéleménye /ORSZI - Országos Rehabilitációs és Szociális Szakértői Intézet/,  
határozat a megváltozott munkaképességről.

#### 5.4.1.6. Diákok, szakmai gyakorlatot teljesítő személyek adatainak kezelése

Jelenleg diákok/szakmai gyakorlatot, nyári munkát teljesítők bevonása is történik időszakosan az intézmény tevékenységébe, amennyiben sor kerül rá, úgy együttműködési megállapodás, illetve a tanuló/hallgatói szerződések keretében történhet a foglalkoztatás.

Az adatkezelés célja: a diákokra vonatkozó munkaviszony létesítése, teljesítése vagy megszüntetése, az ezekkel kapcsolatos jogosultságok elismerése és kötelezettségek tanúsítása

Az adatkezelés jogalapja: törvényi felhatalmazás, a munka törvénykönyvéről szóló 2012.évi I. törvény 10.§.(1) és (3), és az érintett hozzájárulása {a GDPR.6.cikk. (1)a}

A kezelt adatok köre: név, anyja neve, születési helye és ideje, lakcíme, adószáma + törzsszám, munkavégzés helye, beosztás, TAJ szám, folyószámlaszám, telefonszám, e-mail cím, oktatási azonosító, iskolai végzettséget igazoló dokumentumok, kiskorú tanuló esetén: törvényes képviselő neve, lakcíme, telefonszáma

Az adatkezelés határideje: az adatkezelés céljának megvalósulásáig, főszabály szerint

- munkaviszonnal kapcsolatos jogosultságokkal és kötelezettségekkel kapcsolatosan a munkaviszony megszűnéséig
- munkaviszonyból fakadó jogosultságokkal kapcsolatosan a nyugdíjfolyósításról szóló jogszabályokban meghatározott határideig

#### 5.4.1.7. A munkaviszony fenntartásával és megszűnésével kapcsolatos adatkezelések

Az intézmény munkavállalóiról személyzeti, illetve bér- és munkaügyi nyilvántartást vezet.

A személyzeti nyilvántartás a munkaviszonyra, illetve foglalkoztatásra irányuló egyéb jogviszonyra (pl. önálló tevékenységként végzett megbízás, vállalkozás stb.) vonatkozó tények dokumentálására szolgáló adatkezelés. A személyzeti nyilvántartás adatai a munkavállaló munkaviszonyával kapcsolatos tények megállapítására és statisztikai adatszolgáltatásra használhatók fel. A személyzeti nyilvántartás az intézmény valamennyi munkavállalójának adatait tartalmazza.

A munkavállalók adatkezelésének jogalapja a törvényi felhatalmazás (munka törvénykönyvéről szóló 2012. évi I. törvény) a GDPR. 6. cikk (1) a) szerinti érintetti hozzájárulás.

A munkavállalói adatok kezelésére vonatkozóan a szabályzat „Tájékoztató a munkavállalók részére személyes adataik kezelésével kapcsolatban” mellékleteként szereplő munkavállalói tájékoztató készült, amelynek célja a munkavállalók előzetes tájékoztatása az adatkezelésről.

#### 5.4.1.8. A munkaviszonnal kapcsolatos adatkezelésekre vonatkozó nyilatkozatok

Amennyiben a munkaviszony létesítéséhez, fenntartásához, megszüntetéséhez, az ezekkel kapcsolatos jogosultságok bizonyításához vagy kötelezettségek elismeréséhez nyilatkozat beszerzése szükséges a munkavállalótól, úgy a nyilatkozat beszerzése során az intézmény minden esetben felhívja a munkavállaló figyelmét a nyilatkozaton megadott adatokkal kapcsolatosan az adatkezelés tényére, jogalapjára, céljára.

#### 5.4.1.9. Munkavállalók oktatása

Az intézmény fenntartja a jogot, hogy munkavállalók oktatására harmadik féllel szerződjön. Amennyiben az oktatás a munkaviszony ellátásához jogszabályban előírt, úgy a harmadik fél az intézmény adatfeldolgozójaként dolgozza fel az adatokat, minden más oktatás esetén a munkavállaló hozzájárulásával kerül a harmadik félhez továbbításra a személyes adat.

#### 5.4.1.10. Béren kívüli juttatások

Az intézmény fenntartja a jogot, hogy béren kívüli juttatásokat biztosítson a munkavállalók részére és

erre harmadik féllel szerződjön. Amennyiben a munkavállaló a béren kívüli juttatási elemek közül kiválasztja azon szolgáltatásokat, amelyeket igénybe kíván venni, úgy azon szolgáltatók részére a szolgáltatás igénybevételéhez szükséges adatokat az intézmény továbbítja az érintett szolgáltató felé. A béren kívüli juttatások rendszeréről az intézmény Cafeteria szabályzata rendelkezik.

#### 5.4.1.11. Harmadik személyek munkaviszonnyal kapcsolatosan megadott adatai

A munkaviszony kapcsán beszerzett harmadik személy adatai (például pótszabadság, családi adókedvezmény kapcsán vagy baleset esetén értesítendő személy megjelölésekor) a szükséges adattartalom meg nem haladóan vehetők fel és kezelhetők.

##### AMUNKAVÁLLALÓK SZEMÉLYES ADATAINAK KEZELÉSE

Az adatkezelés célja: munkaviszony létesítése, teljesítése vagy megszüntetése, az ezekkel kapcsolatos jogosultságok elismerése és kötelezettségek teljesítése

A kezelt adatok köre:

- neve,
- születési neve,
- születési helye és ideje,
- állampolgársága,
- anyja születési neve,
- lakóhelyének címe,
- tartózkodási helye (amennyiben eltérő a lakóhelytől),
- adóazonosító jele,
- társadalombiztosítási azonosító jele (TAJ szám),
- személyi igazolvány száma
- törzsszám/ nyugdíjas törzsszám (nyugdíjas munkavállaló esetén)
- vállalkozói igazolvány száma
- munkakönyv másolat (ha van)
- nyilatkozat tartozásról,
- nyilatkozat adatbiztonság megtartásáról,
- folyószámla száma, pénzügyi neve
- munkaviszony kezdő napja,
- biztosítási jogviszony típusa,
- munkavégzéssel kapcsolatos időadatok, távollétek,
- munkavégzéssel kapcsolatos szervezeti, költséghely besorolások, adatok,
- telefonszáma,
- email címe,
- végzettséget igazoló dokumentum,
- nyelvtudás és a fokozat megjelölése, nyelvtudást igazoló dokumentum száma, másolat
- munkaköre, statisztikai besorolások
- béradatok
- munkaidő fajtája: teljes/ részmunkaidő
- munkaszerződés határozott, határozatlan, próbaidő,
- munkavégzés helye,
- foglalkozás-egészségügyi alkalmassági vizsgálat eredménye (alkalmasság ténye), érvényesség vége,
- szakszervezeti tagság ténye
- önkéntes, illetve magán-nyugdíjpénztári tagság ténye, belépés ideje (év, hó, nap), bank neve és kódja, belépési nyilatkozat
- önkéntes egészségpénztári tagságra vonatkozó adatok, belépési nyilatkozat,
- erkölcsi bizonyítványának kiállításának dátuma, okmányszáma, kérelem azonosítója,
- a csökkent munkaképességű munkavállaló csökkent munkaképességét megalapozó szakértői határozat száma, másolat

gépkocsivezetők esetében továbbá:

- vezetői engedély száma, érvényessége,

a pótszabadság igénybevételével kapcsolatosan

A kezelt adatok köre:

- a rehabilitációs szakértői szerv legalább 40 százalékos mértékű egészségkárosodását megállapítását igazoló okmány fénymásolata,
- fogyatékosági támogatásra jogosultságot igazoló okmány fénymásolata,
- vakok személyi járadékára jogosultságot igazoló okmány fénymásolata
- gyermekek után járó pótszabadság esetében: gyermek neve, születési ideje, gyermek fogyatékoságának ténye;
- apanap esetében: gyermek TAJ száma, születési anyakönyvi kivonatának száma, anyja neve;

Az adatkezelés jogalapja: az Mt. 118 § és 120.§

az adóelőleg – kedvezmény megállapítása céljából:

A kezelt adatok köre:

- munkavállaló: név, adóazonosító jel; házastárs/élettárs: név, adóazonosító jel, anyja neve, lakcím; eltartottak: név, adóazonosító jel;
- családi kedvezményénél még: jogosultság jogcíme; eltartotti minőség,
- első házások kedvezményénél még: házasságkötés ideje;
- személyi kedvezményénél: fogyatékos állapot jellemzői (orvosi igazolás alapján kezdő nap, végső nap, véglegesség, rokkantsági járadékot, illetve fogyatékosági támogatást megállapító határozat száma)

Az adatkezelés jogalapja: a személyi jövedelemadóról szóló 1995. évi CXVII. tv. 48. §

egyéb kedvezmények igénybevétele céljából:

- hozzátartozó halotti anyakönyvi kivonatának száma: munkavégzési kötelezettség teljesítése alóli mentesülés igénybevétele céljából;
  - gyermek születési anyakönyvi kivonatának száma: gyermekszületés esetén járó munkaidő-kedvezmény igénybevétele céljából;
- kegyeleti költségtérítés esetén:
- az érintett elhunyt hozzátartozó neve, rokonsági foka, temetető neve, rokonsági foka, folyószámla száma, pénztintézet neve, elhunyt halotti anyakönyvi kivonatának száma

élet- és balesetbiztosítás kötése alkalmával kedvezményezett kijelölése:

- biztosított: neve, születési ideje, helye, anyja neve, lakcíme, adóazonosító jele, személyazonosító igazolvány típusa, száma, állampolgársága, tartózkodási helye, közszereplői nyilatkozata,
- kedvezményezett: neve, születési helye és ideje, anyja neve, lakcíme,
- tanúk: neve, címe, személyi igazolvány száma

cafeteria nyilatkozatok és ehhez kapcsolódó igénylőlapok nyilvántartása egyéb személyi jellegű juttatások kezelése céljából:

- név, anyja neve, születési helye és ideje, személyi igazolvány száma, lakcíme, adószáma, törzsszám, szolgálati hely és beosztás,
- adómentes lakáscélú támogatáshoz: telefonszám, bankszámla száma, típusa, hitelt nyújtó pénztintézet neve, célhitel azonosítója (szerződésszám), hitellel érintett ingatlan címe, helyrajzi száma, korábbi munkáltató neve, adószáma, korábban igényelt lakástámogatások összege, tanúk neve, lakcíme, e-mail címe,
- bölcsődei, óvodai szolgáltatáshoz: gyermek neve, anyja neve, születési helye, ideje, adóazonosító jele, lakcíme, a szolgáltatás igénybevételéről szóló számla
- SZÉP kártya, Erzsébet kártya igénylőlap adatai,
- önkéntes nyugdíjpénztári, önkéntes egészségpénztári tagság ténye, belépés ideje (év, hó, nap), bank neve és kódja, belépési nyilatkozat

a jóléti és szociális, valamint az üdülő létesítmények igénybevételével kapcsolatos

dokumentáció kezelése céljából:

- igénylő: név, lakcím, telefonszám, munkavállaló esetén törzsszám is, üdülő létesítmény esetén még: szolgálati hely, beosztás, munkaviszony kezdete; hozzátartozók, egyéb –
- igénybevevők: név, születési idő, rokonsági fok, e-mailen történő jelentkezés esetén e-mailcím is  
törzsszám, szervezeti egység/költséghely, munkakör, jogviszony kezdete, jogcíme; hozzátartozók neve, születési ideje, személyi igazolvány száma, maszkolt másolata, lakcíme; lakcímkártya maszkolt másolata,
- a kedvezményre jogosult családtagoknál még: a rokonsági fok;
- tanulók esetében még: nappali tagozat, rendszeres jövedelemmel rendelkezik-e;
- az elhunyt jogán alapuló igénylésnél még: a volt munkavállaló neve, születési dátuma, igénylő neve, születési dátuma, személyi igazolvány száma, elhunyt munkavállaló jogviszonyának kezdete, vége, elhalálozás dátuma; volt munkaköre,
- gyerekek esetében még: a diákigazolvány száma, iskola/óvoda látogatási igazolás;
- előző jogviszony elismerése esetén: az előző munkáltató igazolása a jogviszony kezdetéről, a munkavállaló nyilatkozata a két munkaviszony közötti kieső időben történt foglalkoztatásról

Megváltozott munkaképességű munkavállalók esetében a megváltozott munkaképességű személyek ellátásairól és egyes törvények módosításáról szóló 2011. évi CXCI. törvény 21. §, 21/A. §, 21/B. § alapján a fenti adatkör kiegészül az alábbiakkal:

- szakértői bizottság szakvéleménye /ORSZI - Országos Rehabilitációs és Szociális Szakértői Intézet/,
- határozat a megváltozott munkaképességről

Az adatkezelés jogalapja: GDPR 6. cikk (1) a) szerinti érintetti hozzájárulás, a munka törvénykönyvéről szóló 2012. évi I. törvény 10. § (1) és (3)] valamint az adó és TB, nyugdíj biztosítási jogszabályok vonatkozó rendelkezései

Az adattárolás határideje: az adatkezelés céljának megvalósulásáig, főszabály szerint,

#### 5.4.2. A munkavállalók technikai eszközeinek ellenőrzésével kapcsolatos adatkezelés

A munkáltató a munkaviszonnnyal összefüggő magatartása körében ellenőrizheti a munkavállalót. Az ellenőrzésre az Mt. 11. § (1)-(2) bekezdése ad jogalapot.

Az intézmény az Mt.-ben meghatározott jogalappal ellenőrzi munkavállalóit. Az intézmény előzetesen tájékoztatja a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak. E tájékoztató részét képezi a 7.4. számú mellékletnek.

Az intézmény a tulajdonában álló eszközöket a fokozatosság elvének betartása mellett ellenőrizheti.

##### 5.4.2.1. Intézményi informatikai eszközök ellenőrzése

Az intézmény a munkavállalóknak indokolt esetben, munkavégzés céljára biztosít számítógépet, e-mail címet és internet-hozzáférést. A használat szabályairól és az ellenőrzés lehetőségéről a munkavállalókat a intézmény előzetesen írásban tájékoztatja a IT rendszerére vonatkozó felhasználási szabályok, alapelvek kapcsán vonatkozó szabályzatában, valamint jelen szabályzat 7.4. számú mellékletét képező munkavállalói tájékoztató megismertetésével.

Mivel az intézmény tulajdonát képező személyi számítógépeket és laptopokat, céges e-mail címet a intézmény munkavégzés céljából biztosítja, azokon személyes adatot tárolni tilos. Amennyiben a munkavállaló a tiltás ellenére ezen eszközökön magáncélú személyes adatait (pl.: családi fotók, telefonkönyvek, saját adatbázisok stb.) tárolja, úgy intézmény a számítógép ellenőrzése során ezeket az adatokat is megismerheti.

Erről a munkavállalókat az eszközök használata előtt írásban tájékoztatja az Intézmény.

#### 5.4.2.2. Intézményi e-mail címek ellenőrzése

Az intézmény munkavállalói tudomásul veszik, hogy mindazon e-mail címek, amelyekben az intézmény neve kiterjesztésként szerepel (...@lumniczerkorhaz.hu), az intézmény tulajdonát képezik és az ezen a címeiken folytatott levelezés munkacélú levelezésnek minősül. A fogadott és küldött e-mailek tartalma az intézmény tulajdonát képezik!

Az ilyen címeiken folytatott levelezésbe az intézmény megfelelő jogalap esetén jogosult betekinteni. Az intézmény jogosult a fent nevezett címeiken folytatott levelezések meghatározott időközönkénti biztonsági mentésére, az elektronikus levelező rendszer folyamatosságának és stabilitásának érdekében.

A céges e-mail címeiken nem munkavégzési célú (magán vagy bármilyen egyéb) levelezést tilos folytatni. Amennyiben a munkavállaló (...@lumniczerkorhaz.hu) céges e-mail címén található leveleiben magán- vagy bármilyen egyéb célú levelezést folytat, ezzel egy időben a postafiókban magáncélú személyes adatait tárolja, úgy a intézmény az e-mail cím ellenőrzése során ezeket az adatokat is megismerheti. Mindemellett főszabály szerint a magáncélú levelek tartalmát a munkáltató munkaviszonyból fakadó jogosultság érvényesítése során sem jogosult megismerni.

#### 5.4.2.3. Az internet használatának ellenőrzése

A fenti szabályok érvényesek az internethasználatra is: az internet használata munkaidőben csak intézményi célokra engedélyezett. Emiatt az internetezési adatok céges adatoknak minősülnek.

#### 5.4.2.4. Intézményi tulajdonú gépjárművek nyomon követése

Az intézmény fenntartja a jogot, hogy a tulajdonában lévő gépjárművekbe nyomkövető rendszert telepítsen. A gépjármű csak az intézmény céljaival összefüggésben használható, aminek során a nyomkövető rendszer folyamatosan jelzést ad a gépjármű aktuális pozíciójáról. Mivel a gépjármű használója minden esetben összeköthető a gépjármű aktuális pozíciójával, így ez személyes adattá válik – erről az intézmény minden esetben tájékoztatja a gépjárművet használó munkavállalót.

Az intézmény tulajdonában lévő gépjárművek magáncélra nem használhatók, ha vannak olyan munkavállalók, akik magánhasználatra is igénybe vehetik a gépjárművet, az intézménynek biztosítania kell a GPS kikapcsolását vagy magánkapcsolóra történő átállítását.

Az adatkezelés célja: az intézmény jogos üzleti érdekeinek megfelelően a munkavállalók Mt. 11. § (1) szerinti ellenőrzése, így különösen a munkavállalónak biztosított gépjárművek útvonalának ellenőrzése

A kezelt adatok köre: gépjárművet igénylő neve, feladatköre, igénylés időpontja, gépjármű GPS adatai

Az adatkezelés jogalapja: GDPR 6. cikk (1) f) szerinti jogos érdek és az Mt. 10§ (1) és a 11. § (1)

Az adattárolás határideje: az adatkezelési cél megvalósulásáig, az ellenőrzéssel kapcsolatos igény elévüléséig, maximálisan az adatfelvételtől számított 5 évig

Az adatkezelés módja: papíralapon és elektronikusan

#### 5.4.3. Egészségügyi adatok kezelése

Az egészségügyi és személyazonosító adatok szoftveres felvétele a gyógykezelés része.

Az egészségügyi és személyazonosító adatok kezelését - a Szabályzat követelményeinek eleget tevő - Integrált Egészségügyi Rendszer (HIS) biztosítja. Az Intézményben kezelt egészségügyi és személyazonosító adatok védelme alap követelmény. A HIS-ben történő adatkezelést csak az adatkezelésre jogosult személyek végezhetnek. Ennek biztosítása és ellenőrzése céljából a HIS-ben az adatkezelőknek hozzáférési szintek és megfelelő jogosultságok kiosztása történik az Informatikai biztonsági szabályzat és az Információbiztonsági Politikában leírtak alapján. Az egyéni jelszó a HIS-ből a kórházi adatvédelmi tisztviselő és az informatikus szakemberek (rendszeradminisztrátorok) által lesz kiolvasható. Az egyéni jelszavakról osztályos nyilvántartás nem vezethető. Az egyéni jelszó titokban tartására minden adatkezelő köteles. Az adatkezelőket a HIS-ben történő jelszavas adatkezelésért személyes felelősség terheli. A HIS egyes moduljaiban az adat-hozzáférési jogosultság menürendszer segítségével állítandó be. A legmagasabb szintű hozzáférési jog csak az Adatvédelmi Tisztviselőt, valamint a

rendszeradminisztrátorokat illeti meg. Az alsóbb szintű hozzáférési jogosultság az Osztályos Adatvédelmi Felelősökre, adatkezelőkre, statisztikusokra vonatkozik. Az Osztályos Adatvédelmi Felelősök a hozzáférés igénylésekor központilag meghatározott irányelv alapján járnak el. Az irányelv rögzíti az egyes munkakörökhöz javasolt belépési szinteket. Az irányelvektől eltérni csak a kórházi adatvédelmi tisztviselő kifejezett hozzájárulásával lehet. Az egyes osztályokon a hozzáférési joggal rendelkező munkatársakról az Osztályos Adatvédelmi Felelősök nyilvántartást vezetnek. Az általuk közölt adatok figyelembe vételével egységes központi nyilvántartás is készül, amelynek karbantartásáról az Adatvédelmi Tisztviselő gondoskodik. Az osztályos hozzáférési regiszterekbe más osztályok adatkezelői csak meghatározott időre és csak a kórházi adatvédelmi felelős írásbeli engedélyével vehetők fel. Mind az osztályos, mind a központi listáról ki kell vezetni azt a munkavállalót, aki az osztályon adatkezelést nem folytat, illetőleg akinek munkajogi viszonya az Intézményben megszűnik. Az egyes modulokba a hozzáférési lajstromban szereplő dolgozók mellett, kizárólag a rendszeradminisztrátorok léphetnek be. A HIS az adatbevitelt úgy fogadja, hogy egyben regisztrálja az adatkezelő kódját, az adatlétrehozás helyét és idejét, illetőleg a bevételre használt munkaállomást. A HIS-be már bevitt adatok módosítása rendszerint tilos. A leletek, zárójelentések - a főszabálytól eltérően - a gyógykezelt személynek az adott vizsgálatot, illetve kezelést végző osztályról való távozásig módosíthatók. Ezt követően - pl. véglegesítés céljából - hozzájuk már csak kiegészítés fűzhető. A kiegészítésben az eredeti lelet nem változtatható meg. Korrigálhatók (távoztatásig) a tévesen felvett, avagy a rendszerben szereplőkhöz képest módosult személyazonosító adatok is. A korrekció előtti adatot, továbbá az adatcserét eszközölő személy azonosítóját a rendszer automatikusan elmenti. Az átírás előtti adatok a HIS munkaállomásairól a későbbiekben nem érhetők el. A gyógykezelt személy távoztatásakor a kezelőorvos a finanszírozáshoz kellő adatokat a HIS-be felviszi. Ezek hozzáférhetősége időben nem korlátozott. A HIS alkalmas, hogy jegyezze a rendszerbe való belépéseket és az adatkezelők által működtetett informatikai modulok használatát, megállapítható minden adatrögzítés és - módosítás időpontja és a kezdeményező kiléte. A belépések ellenőrzését - a jogosulatlan használat gyanúja esetén - az adatkezelő, a Főigazgató, az adatvédelmi tisztviselő az Osztályos Adatvédelmi Felelős kezdeményezheti. Elektronikus adatátviteli berendezéseken (fax, e-mail) tilos egészségügyi vagy azzal összekapcsolt személyes adatokat, és különleges adatokat továbbítani.

Az adatkezelés célja:

- a) az egészség megőrzésének, javításának, fenntartásának előmozdítása,
- b) a betegellátó eredményes gyógykezelési tevékenységének elősegítése, ideértve a szakfelügyeleti tevékenységet is,
- c) az érintett egészségi állapotának nyomon követése,
- d) a népegészségügyi [16. §], közegészségügyi és járványügyi érdekből szükségessé váló intézkedések megtétele,
- e) a betegjogok érvényesítése.

A kezelt adatok köre: Név, Születési név. Anyja neve, Taj száma, Születési adatok, Lakcím. Az egészségügyi ellátás során keletkező mindennemű az ellátással összefüggő különleges adat (34iagnosis, beavatkozás, lelet, zárójelentés, kórtörténet stb)

Az adatkezelés jogalapja: Az érintett egészségéhez fűződő létfontosságú érdeke  
A közérdek (pl. közegészségügyi járványügyi adatkezelés, orvosok szakképzése)  
jogi kötelezettség teljesítése (pl. egészségbiztosítás terhére igénybe vehető ellátásokhoz kapcsolódó adatkezelés, társadalombiztosítási ellátások megállapításához kapcsolódó adatkezelés-az Egészségügyi Adatkezelésről szóló 1997. XLVII. törvény, valamint az 1997. LXXXIII. a Kötelező egészségbiztosításról szóló törvény).

Az adattárolás határideje: jogszabályban előírt ideig

Az adatkezelés módja: papíralapon és elektronikusan

#### 5.4.4. Munka- és balesetvédelmi ellenőrzések

Alkalmazandó szabályzat: Munkavédelmi szabályzat

A munkavédelmi ellenőrzéseknek két fajtája van:

- rendszeres felülvizsgálatok,
- soron kívüli ellenőrzések.

Az ellenőrzésekről jegyzőkönyv készül. A jegyzőkönyvekben a jelenlevők neve szerepel.

Az Intézmény munkavédelmi felelőse tartja a munkavállalók részére a munkavédelemmel kapcsolatos oktatásokat.

Az oktatásoknak három csoportja van:

- előzetes,
- időszakos és
- rendkívüli.

Az oktatásokon résztvevők egy jelenléti ív aláírásával tanúsítják, hogy az oktatást megkapták.

A munkavédelmi felelős az oktatásokról oktatási naplót vezet. Az oktatási naplóban az alábbi adatok szerepelnek:

Szervezeti egység megnevezése: .....

Munkahely megnevezése: .....

Oktatás időpontja: ..... év ..... hó ..... nap

Oktatás jellege: - ismétlődő - pótktatás - rendkívüli -\*

Oktatott dolgozók létszáma: ..... fő

Oktatáson jelen levő személyek neve

#### 5.4.4.1. Munkabaleset kivizsgálása

A munkabalesetek kivizsgálását a hatályos jogszabályok szerint a Munkavédelmi szabályzatban foglaltak alapján végzi az intézmény, attól jogszerűen nem is térhet el.

Jogszabály írja elő, hogy a munkabalesettel kapcsolatban milyen adatokat kell a munkáltatónak nyilvántartani. Alkalmazandó jogszabályok: Mvt., 5/1993. (XII. 26.) MüM rendelet (jelen pont esetében rendelet).

A munkáltató a munkabaleset súlyosságától és a sérült munkavégző képességének változásától függetlenül köteles a fenti adatokat nyilvántartani. A munkabaleset nyilvántartásának alapja a munkabaleseti jegyzőkönyv. A jegyzőkönyvet köteles a munkáltató az irattárban öt évig megőrizni. A munkabaleset kivizsgálása során nyert adatokat a munkáltatónak munkabaleseti jegyzőkönyvben [az 5/1993. (XII.26.) MüM rendelet mellékletében meghatározott formanyomtatvány] rögzítenie kell. A jegyzőkönyvet minden sérültről külön-külön ki kell állítani meg akkor is, ha egyidejűleg több személy sérült meg.

A munkabalesetet kivizsgáló munkavédelmi felelős eljárására vonatkozó jogszabályi kötelezettségeket és kezelendő adatokat a rendelet 3. számú melléklete sorolja fel.

A munkabalesetről a rendelet 4 a. számú mellékletében meghatározott munkabaleseti jegyzőkönyvet kell kitölteni, az abban meghatározott adattartalommal. A tárolási határidő a rendelet szerint 5 év.

„Jelen adatokat a Lumniczer Sándor Kórház-Rendelőintézet a munkavédelemről szóló 1993. évi XCIII. törvény egyes rendelkezéseinek végrehajtásáról szóló 5/1993. (XII. 26.) MüM rendelet 3. számú és 4a. számú melléklete alapján köteles kezelni.”

Az adatkezelés célja: munka- és balesetvédelmi ellenőrzések elvégzése és dokumentálása, a törvényi előírás betartása

A kezelt adatok köre: 5/1993. (XII. 26.) MüM rendelet 3. és 4a. melléklete alapján: a sérült munkavállaló adatai: neve, születési neve, TAJ száma, anyja neve, születési helye, neme, állampolgársága, születési ideje, lakcíme, foglalkozása, telefonszáma, foglalkoztatási jogviszonya, foglalkoztatás jellege, munkabaleset adatai, munkabaleset részletes leírása

Az adatkezelés jogalapja: 5/1993. (XII. 26.) MüM rendelet 3. és 4a. számú melléklete Az adattárolás határideje: a munkabaleseti jegyzőkönyv felvételétől számított 5 év

Az adattárolás módja: elektronikusan és papíralapon

#### 5.4.4.2. Tüzesetek kivizsgálása:

Aki tüzet vagy annak közvetlen veszélyét észleli, köteles azt haladéktalanul jelezni a hívásfogadó központnak, a katasztrófavédelmi igazgatóság műveletirányító ügyeletének vagy a tűzoltóságnak.

A tűzjelzés fogadásakor a tűzoltási, műszaki mentési, hatósági feladat végrehajtása érdekében, a jelzést fogadó a tudomására jutott vagy a bejelentő által közölt alábbi adatokat rögzíti:

a) a bejelentő nevét,

- b) a bejelentő telefonszámát, ennek hiányában lakcímét,
- c) a bejelentéskor használt telefonszámhoz tartozó előfizető nevét, címét,
- d) a bejelentő által használt telefonállomás azonosított adatait,
- e) a hívások rögzített tartalmát, a tűzoltási, műszaki mentési feladatot indokoló esemény helyét és jellegét, a személyi sérülés, haláleset adatait,
- f) a műveletirányítás által szükségesnek tartott további, személyes adatnak nem minősülő információt.

A tűzoltóság a kárhelyszínen tartózkodó, a káresemény tekintetében érdemi információval szolgálni tudó személyek alábbi adatait rögzítheti:

- a) név,
- b) lakcím,
- c) egyéb elérhetőség.
- d) A személyes adatokat és a bejelentést rögzítő hangfelvételeket a tűzoltóság 5 évig kezeli.

#### 5.4.4. Munkára alkalmas állapot munkavédelmi vizsgálata

Az Mt. 52. § (1) a) kimondja, hogy a munkavállaló köteles a munkáltató által előírt helyen és időben munkára képes állapotban megjelenni.

Az Mvt. 2. § (3)-ban kapott felhatalmazás alapján az alábbiak szerint határozza meg az alkoholos befolyásoltságra vonatkozóan az egészséget nem veszélyeztető és biztonságos munkavégzés követelményeinek megvalósítását.

Az Mvt. 60. § (1) alapján a munkavállaló csak biztonságos munkavégzésre alkalmas állapotban, a munkavédelemre vonatkozó szabályok, utasítások megtartásával, a munkavédelmi oktatásnak megfelelően végezhet munkát. A munkavállaló köteles munkatársaival együttműködni, és munkáját úgy végezni, hogy ez saját vagy más egészségét és testi épségét ne veszélyeztesse.

Az intézmény minden munkakörre vonatkozóan tiltja, hogy a munkavállalói alkoholos befolyásoltság alatt valamint tudatmódosító szer hatása alatt tartózkodjanak a munkavégzés területén – ez vonatkozik arra az esetre is, ha a munkavállaló munkaidején túl, már/még nem munkavégzési céllal tartózkodik a területen, lévén az alkoholos befolyásoltság alatt álló személy veszélyezteti mások biztonságos munkavégzését. Tilos a intézmény területére vagy amennyiben az nem azonos vele, úgy a munkavégzés területén alkoholos befolyásoltság alatt tartózkodni, ott alkoholt fogyasztani, alkoholos befolyásoltság alatt munkát végezni.

A biztonságos munkavégzés feltételeit veszélyeztetheti a munkára képes állapot hiánya, így az alkoholos befolyásoltság. Emiatt a munkavállalónak nem csak a munkavégzésre történő megjelenéskor kell munkára képes állapotban lennie, hanem ezt az állapotát egészen a munkaideje lejártáig köteles megőrizni.

A munkavállaló munkája ellátása során nem veszélyeztetheti sem a maga, sem pedig más egészségét és testi épségét.

Az intézmény a biztonságos munkavégzés követelményeit kialakítandó kötelezettségénél fogva köteles rendszeresen meggyőződni arról, hogy a munkavállalók megtartják-e a rájuk vonatkozó rendelkezéseket. A munkajogi előírások betartásának ellenőrzésére vonatkozó szabályokat mind az Mt., mind az Mvt. pontosítja.

Mt. 11. § (1) A munkáltató a munkavállalót csak a munkaviszonnyal összefüggő magatartása körében ellenőrizheti. A munkáltató ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkavállaló magánélete nem ellenőrizhető.

Mvt. 54. § (7) b) Az egészséget nem veszélyeztető és biztonságos munkavégzés érdekében a munkáltató köteles rendszeresen meggyőződni arról, hogy a munkakörülmények megfelelnek-e a követelményeknek, a munkavállalók ismerik, illetve megtartják-e a rájuk vonatkozó rendelkezéseket.

Az Intézmény jelen adatkezelésre vonatkozóan rendelkezik külön szabállyal (Munkavédelmi szabályzat), jelen szabályzatban nem meghatározott kérdésekben a megjelölt szabályzat az irányadó.

Az adatkezelés célja: munkára alkalmas állapot ellenőrzése munkavédelmi célból

A kezelt adatok köre: az ellenőrzés eredménye, időpontja, munkára alkalmas állapot ténye, ellenőrzést végző személy adatai, ellenőrzés alá fogott munkavállaló adatai. Ha az ellenőrzött személy vitatja az eredményt, akkor annak ténye is, illetve pozitív minta esetén, ha lemond a vérvizsgálat jogáról, ennek ténye is.



Az adatkezelés jogalapja: GDPR 6. cikk (1) f) szerinti jogos érdek, a munkavédelemről szóló 193. évi XCIII. törvény 60. § (1), valamint a munka törvénykönyvéről szóló 2012. évi I. törvény 11.

§ (1) és (2) bekezdés

Az adattárolás határideje: az ellenőrzésből fakadó jogok és kötelezettségek által megalapozott igények érvényesítésére nyitva álló határidő

Az adatkezelés módja: papíralapon

#### 5.4.5. Munkára jelentkezők adataival kapcsolatos adatkezelés

##### 5.4.5.1. Az intézményhez történő jelentkezés folyamata

A meghirdetett álláshelyekre, ajánlással és jelentkezéssel keresztül keres megfelelő személyt az intézmény, berepülő önéletrajzok pedig postai és elektronikus úton, valamint személyesen is érkeznek.

Az önéletrajzok tárolása elektronikus adatbázisban történik, egy évig.

Az adott álláshelyre megfelelő munkavállaló kiválasztásáért az intézmény HR munkatársa és a mindenkori munkáltatói jogkörgyakorló a felelős, így a jelen adatkezeléssel összefüggő feladatok ellátása során az adatvédelmi tisztviselővel együttműködve kötelesek az érintettek jogait biztosítani.

##### 5.4.5.2. A berepülő önéletrajzokkal és a munkaerő-toborzással kapcsolatos közös szabályok

Az intézmény a munkára jelentkezés céljából érkezett személyes adatokat tartalmazó önéletrajzok esetén nem tesz különbséget azok érkezésének módja között: azonos elbírálás alá esik a papíralapon és az elektronikus módon érkezett önéletrajz.

Főszabály szerint az önéletrajzokat későbbi felhasználás céljából tárolja az intézmény, a később megüresedő vagy betöltendővé váló pozíciók miatt. Az adatbázisba kerülő adatokat egy év elteltével semmisíti meg, lévén ennyi idő elteltével már vélhetően nem relevánsak a munkakeresés szempontjából az adatok.

Minden, az intézmény előtt feltárt önéletrajz esetében az adatkezelésre az GDPR 6. cikk (1) a) pontja szerinti érintetti hozzájárulás ad jogalapot.

Az adatkezeléshez adott hozzájárulás megdönthető, így az érintett jelen szabályzat szerint meghatározottak alapján visszavonhatja hozzájárulását.

##### 5.4.5.3. A „bepülő önéletrajzok”-ra vonatkozó különös szabályok

A nem meghirdetett álláshelyre való jelentkezés esetén az intézmény válaszelevelet küld a jelentkezőnek, amelyben tájékoztatja az adatkezelés tényéről, jogalapjáról és az adatkezelés elleni tiltakozás formáiról. Az „Önkéntes hozzájárulás személyes/egészségügyi adataim kezeléséhez” című nyilatkozat a szabályzat 7.2. számú mellékletét képezi.

Az önéletrajz alapján kiválasztott érintett adatainak további kezelése (úgy mint: alkalmasság eldöntése) már a munkaviszony létesítése céljából történik, így az azzal kapcsolatos adatkezelést az 5.4.1. pont taglalja.

## MUNKÁRA JELENTKEZŐK ADATAIVAL KAPCSOLATOS ADATKEZELÉS

Az adatkezelés célja: a megüresedő álláshelyek betöltésére a munkaviszony későbbi létesítése céljából, megfelelő leendő munkavállaló kiválasztása

A kezelt adatok köre: név, születési dátum, anyja neve, lakcím, képzési adatok, fénykép, az érintett által megadott egyéb adatok, ajánló személyazonosító adatai, háttérellenőrzés sikerességének ténye Az adatkezelés jogalapja: a GDPR 6. cikk (1) a) szerinti érintetti hozzájárulás

Az adattárolás határideje: az érintett törlési kérelméig, maximum 1 évig  
Az adattárolás módja: papíralapon és elektronikusan

#### 5.4.6. Ingatlanbérbeadás

Ingyatlanbérbeadás esetén az intézmény eshetőlegesen kezel csak személyes adatot, amennyiben a polgári jogviszony másik érintettje egyéni vállalkozó vagy természetes személy. Ebben az esetben az adatok kezelése a szerződéses jogviszonyokra irányadó szabályok szerint és a számviteli törvényben meghatározott időtartamig történik az érintett hozzájárulásával (a szerződéskötési szabadság miatt csak az érintett hozzájárulásával tud intézményünk szerződést kötni partnereivel).

Az adatkezelés célja: ingatlanbérbeadásával kapcsolatos számlázás

Az adatkezelés jogalapja: a GDPR 6. cikk (1) b) szerinti szerződéses kötelezettség teljesítése

A kezelt adatok köre: név, születési hely, idő, személyi azonosító igazolványok számai, telefonszám, lakcím, e-mail cím.

Az adattárolás határideje: Szvt. szerinti 8 év

#### 5.4.7. Kapcsolatfelvétel az intézménnyel

Az intézmény lehetőséget biztosít arra, hogy az érdeklődő felvegye az intézménnyel a kapcsolatot. A megkereséseket az intézmény rögzíti, a megadott személyes adatokat a megkeresés céljával összefüggő határideig tárolja.

Az adatkezelés célja: az intézménnyel történő kapcsolatfelvétel elősegítése

A kezelt adatok köre: név, e-mail cím, telefonszám, kapcsolatfelvétel tárgya, üzenet szövege

Az adatkezelés jogalapja: a GDPR 6. cikk (1) a) szerint az érintett hozzájárulása

Az adattárolás határideje: a kapcsolatfelvételi ügy elintézéséig (a cél megvalósulásáig) Az adattárolás módja: elektronikusan

#### 5.4.8. Panaszok, észrevételek ügyintézése

A panaszok felvételének módja történhet személyesen, telefonon, panaszlevél formájában, vagy e-mailen keresztül. A telefonon, illetve személyesen tett panaszok rögzítése az intézmény Panaszvizsgálási szabályzata alapján, az abban szereplő adattartalommal történik. Az elektronikusan, illetve postai úton érkező panaszokról külön feljegyzés nem készül.

Az ügyfelek által igénybe vehető panaszbejelentés módjai:

- személyesen (szóban és írásban),
- telefonon
- postai úton,
- az intézmény honlapján feltüntetett e-mail címre
- 

A panaszról felvett jegyzőkönyv a következőket tartalmazza:

- a) az ügyfél neve;
- b) az ügyfél lakcíme, székhelye, illetve amennyiben szükséges, levelezési címe;
- c) a panasz előterjesztésének helye, ideje, módja;
- d) az ügyfél panaszának részletes leírása, a panasszal érintett kifogások elkülönítetten történő rögzítésével, annak érdekében, hogy a vendég panaszában foglalt valamennyi kifogás teljes körűen kivizsgálásra kerüljön;
- e) az ügyfél által bemutatott iratok, dokumentumok és egyéb bizonyítékok jegyzéke;
- f) a jegyzőkönyvet felvevő személy és az ügyfél aláírása (utóbbi formai elem személyesen közölt szóbeli panasz esetén elvárt);
- g) a jegyzőkönyv felvételének helye, ideje. (1997. évi CLV. törvény 17/A § (5) bekezdés)

Az intézmény a hatályos panaszkezelési szabályzatában meghatározottak szerint rögzíti a panaszokat. A panasz megtételére lehetőséget biztosító helyszínen az intézmény jelen szabályzat „Általános adatkezelési tájékoztató” mellékletét képező tájékoztatást helyez el.

Az adatkezelés célja: panaszok, észrevételek ügyintézés

Az adatkezelés jogalapja: a GDPR 6. cikk (1) a) szerinti érintetti hozzájárulás, a fogyasztóvédelemről szóló 1997. évi CLV. törvény 17/A § (7) bekezdése

A kezelt adatok köre: név, lakcím, telefonszám, e-mailcím

Az adattárolás határideje: az Intézmény a panaszról felvett jegyzőkönyvet és a válasz másolati példányát öt évig megőrzi [Fgytv. 17/A. § (7) és 17/B. § (3)]

#### 5.4.9. Kamerás megfigyeléssel kapcsolatos adatkezelés

Az intézmény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvényben rögzítettek (a továbbiakban: az Szvmt.) szerint elektronikus megfigyelőrendszert üzemeltet. Az intézmény által üzemeltetett elektronikus kamerarendszerek pontos felsorolásáról és a telepítésre vonatkozó szabályokról a "Térfigyelő rendszer működésének szabályzata" rendelkezik.

A rögzített adatok vonatkozásában a felhasználás és az információk továbbítása csak az Szvmt. és az GDPR szabályainak figyelembe vételével történhet.

#### 5.4.10. Vagyonvédelemmel kapcsolatos adatkezelés

##### 5.4.10.1. Vendégek be- és kiléptetése

Az intézmény saját tulajdonú területeire a belépés mindenki számára engedélyezett. Személyes adat rögzítésére nem kerül sor.

Az intézmény területére járművekkel is behajthatnak. Az intézmény területére érkező, vagy onnan távozó minden járműnek a portaszolgáltatónál meg kell állnia, személyes adat rögzítésére nem kerül sor.

Az intézmény vagyonvédelmi tevékenységét vállalkozási szerződéssel a Kéfkény Security Vagyonvédelmi Kft látja el.

##### 5.4.10.2. Vagyonvédelmi rendkívüli események

Rendkívüli esemény minden olyan, az átlagostól jelentősen eltérő esemény, körülmény, amely az objektumban tartózkodó személyek életét, testi épségét vagy az ott található anyagi javakat tekintve súlyos következményekre vezethet vagy reális esélye van annak, hogy vezetni fog és ezzel az objektum működésében komoly zavart okoz.

adatkezelés célja: vagyonvédelmi rendkívüli események kivizsgálása

kezelt adatok köre: a jegyzőkönyv kitöltésének dátuma, biztonsági szolgálat munkatársának neve, aláírása, vizsgált személy neve, aláírása, vizsgált személy születési neve, születési helye, ideje, anyja neve, lakcíme, tartózkodási helye és a cselekmény leírása

adatkezelés jogalapja: GDPR 6. cikk (1) f) szerinti jogos érdek, valamint a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló törvény végrehajtásáról szóló 22/2006. BM rendelet (IV. 25.) 8. § (1) bekezdése

adattárolás határideje: az esemény kivizsgálása, az abból fakadó jogokkal és kötelezettségekkel kapcsolatos igényérvényesítésre nyitva álló határidő

adattárolás módja: papíralapon

##### 5.4.11. Marketing tevékenységgel kapcsolatos adatkezelés

Az intézmény hivatalos közleményeit kizárólag a [www.lumniczerkorhaz.hu](http://www.lumniczerkorhaz.hu) oldalon teszi közzé az interneten, a közösségi oldalakon nem regisztrált, nem hozott létre nyilvános profilt az intézmény nevével. Ezekon az oldalakon megjelenő információk, üzenetek, válaszok, vélemények nem az intézmény hivatalos közleményei, így az ezekkel kapcsolatos adatkezelés során sem az intézmény az adatok kezelője.

Az intézmény eseti jelleggel rendezvényeket szervez. A marketing tevékenység részeként az intézmény évente Lumniczer napot, Mikulás ünnepséget és karácsonyi ünnepséget szervez. A rendezvényen az intézmény munkavállalói és családtagjai vehetnek részt. A rendezvényeken fényképek, videók készülhetnek. Az így készült fényképeket, videókat az intézmény publikálhatja.

A rendezvényre látogatókat az intézmény előzetesen tájékoztatja az őket érintő adatkezelési szabályokról.

Az adatkezelés célja: a rendezvényeken video- és fényképfelvételek készítése és felhasználása

Az adatkezelés jogalapja: a GDPR 6. cikk (1) a) szerinti érintetti hozzájárulás és a Polgári Törvénykönyvről szóló 2013. évi V. törvény 2:48 § (1) bekezdése

A kezelt adatok köre: az érintett hang- és képmása, az érintettel kapcsolatba hozható egyéb adatok

Az adattárolás határideje: az adott marketingtevékenységgel elérendő cél megvalósulásáig

Az adatok kezelésének jogszerűvé tételéhez az intézmény e tevékenységéhez kapcsolódó pályázati felhíváson adatvédelmi tájékoztatót jelentet meg, amelynek szövege jelen szabályzat „Adatvédelmi tájékoztató céges rendezvényen való részvételhez” mellékletét képezi.

Bizonyos rendezvények előzetes regisztrációhoz kötöttek.

A regisztráció során felvett adatokat az alábbiak szerint kezeli az intézmény.

#### REGISZTRÁCIÓ SORÁN FELVETT ADATOK

Az adatkezelés célja: a rendezvényen résztvevő beazonosítása

Az adatkezelés jogalapja: a GDPR 6. cikk (1) a) szerinti érintetti hozzájárulás

A kezelt adatok köre: a jelentkező neve, e-mail címe, telefonszáma, 16 év alatti regisztráció esetén törvényes képviselő neve

Az adattárolás határideje: a rendezvény lebonyolításáig

A regisztrációhoz kötött rendezvények során rögzített adatok kezeléséről az érintetteket tájékoztatni kell, illetve a 16 év alatti résztvevők esetében hozzájáruló nyilatkozat beszerzése szükséges amely jelen szabályzat „Hozzájáruló nyilatkozat a regisztrációhoz” és „Hozzájáruló nyilatkozat a szülők részéről” melléklete.

Az intézmény tevékenysége során sajtóközleményt adhat ki vagy a honlapján ([www.lumniczerkorhaz.hu](http://www.lumniczerkorhaz.hu)) információkat tüntet fel. Amennyiben a sajtóközlemény harmadik fél személyes adatát tartalmazza (így különösen az érintett neve, tevékenységével kapcsolatos adatok, képmása), úgy az intézmény minden esetben előzetesen megszerzi az érintett hozzájárulását az adatkezeléshez.

Amennyiben a intézmény sajtónyilvános eseményt szervez, úgy az azon készülő kép- és hangfelvételek kezelője minden esetben az azt készítő médium, így az azzal kapcsolatos adatkezeléssel összefüggően az adott médium felelős az érintetti jogok biztosítására. Az intézmény akarata ellenére nem kötelez senkit a sajtónyilvános eseményen való részvételre, ahol róla így felvétel készülhet, az intézmény nem él vissza különösen munkáltatói jogaival és csorbítja ezzel az érintett önkéntes hozzájárulásának alapját.

#### 5.4.12. Honlap kezelésére vonatkozó adatkezelés

Az intézmény saját honlappal rendelkezik, mely az alábbi címen érhető el:

<http://www.lumniczerkorhaz.hu>

A honlap az intézmény saját tulajdonú oldala.

A [www.lumniczerkorhaz.hu](http://www.lumniczerkorhaz.hu) domain név és honlap az intézmény saját tulajdona. A honlap üzemeltetését külsős cég végzi. A szervert és az alaprendszert külső szolgáltató biztosítja, az információtartalom feltöltését az intézmény informatikusai végzik.

A honlap cookiekat használ, amelyről figyelmeztető üzenet jelenik meg a honlap alján, melyhez a felhasználó hozzájárulása kell. A cookie (websüti) a böngészőprogramok által a honlap megbízásából tárolt adatsomag. A sütitet maga a honlap hozza létre a böngésző segítségével a felhasználó számítógépén, vagy eszközén, ahol azok egy elkülönített könyvtárban kerülnek tárolásra. Többek között információt tárolhatnak a böngészésre használt eszköz paramétereiről, a felhasználó esetleges egyéni beállításairól, korábbi látogatásairól, hogy ezáltal is jobb böngészési élményben részesüljön: a tárolt adatok révén az Önnek megfelelő beállítású lap töltődik be.

Az intézmény honlapjának böngészése során az intézmény az alábbi cookie-kat alkalmazza.

- Munkamenet cookie (session cookie): ezek a cookie-k ideiglenesen aktiválódnak, amíg a böngészés folyik (azaz attól a pillanattól, amikor a felhasználó megnyitja a böngésző ablakot, addig a pillanatig, amíg be nem zárja azt), amint bezárul a böngésző, minden munkamenet cookie automatikusan törlődik.
- Állandó cookie: ezek a cookie-k a felhasználó eszközén maradnak a cookie-ban meghatározott ideig. Minden alkalommal aktiválódnak, amikor a felhasználó meglátogatja az adott weboldalt.

A cookie-k használatára vonatkozó jogi feltételeket megállapító rendelkezéseket az elektronikus hírközlésről szóló 2003. évi C. törvény rögzíti. A hírközlési törvény egyértelműen kimondja, hogy cookie-t elhelyezni, a cookie által gyűjtött személyes adatokat felhasználni csak az érintett felhasználó világos és teljes körű, az adatkezelés céljára is kiterjedően, a tájékoztatását követő hozzájárulása alapján lehet.

## A HONLAP KEZELÉSÉRE VONATKOZÓ ADATKEZELÉS

Az adatkezelés célja: az intézmény honlapjának interaktív módon való működése, a weboldal használhatóságának és folyamatainak megkönnyítése, illetve a felhasználók számának meghatározása, akik a honlapra látogatnak

Az adatkezelés jogalapja: a GDPR 6. cikk (1) a) szerinti érintetti hozzájárulás

A kezelt adatok köre: név, cím, e-mail cím, üzenet szövege, a látogatás kezdő és befejező időpontja, IP-címe, a böngésző, az operációs rendszer típusa, nyelve, az eszköz paramétere, a weboldalon megadott beállítások, a meglátogatott oldalak és az azokon eltöltött idő.

Az adattárolás határideje: a cél megvalósulásáig

Az adattárolás módja: elektronikus

### 5.4.13. Pénzügyi adatkezelés

Az intézmény által kiállított számlák a személyes adatok tekintetében – a magánszemélyek és az egyéni vállalkozók esetén - az általános forgalmi adóról szóló 2007. évi CXXVII. törvény 169. § szerinti kötelező elemeket tartalmazzák: a vevő neve, címe, valamint a vevő adószáma (külföldi vevő esetén: közösségi adószám) és bankszámla száma.

#### 5.4.13.1. Irattározás

Az intézmény fenntartja a jogot, hogy a pénzügyi adatkezelése során kiállított számlák kezelését (így különösen azok kategorizálásával, tárolásával, selejtezésével) saját maga végezze. A számlák tárolása az intézmény saját irattárában történik.

## PÉNZÜGYIADATKEZELÉS

Az adatkezelés célja: számlázás, jogok és kötelezettségek nyilvántartása

A kezelt adatok köre: magánszemély esetén név, cím, számlázással kapcsolatos adatok, egyéni vállalkozó beszállító esetén neve, címe, adószáma, számlavezető pénzügyintézet neve, bankszámlaszáma

Az adatkezelés jogalapja: a 2000.: C. tv. 169. § (1)-(2)-ben szereplő törvényi rendelkezés

Az adattárolás határideje: az adatfelvételtől számított 8 év [Sztv. 169. § (1)-(2)]

#### 5.4.13.2. Hátralékkezelés

Az intézmény tevékenysége során hátralékkal rendelkező magánszemélyek adatait hátralékkezelés céljából is kezeli. A szerződéses viszonyból fakadó hátralékok kezelését az intézmény saját munkavállalói végzik, így a fizetési meghagyással kapcsolatos nem peres eljárást, illetve a végrehajtással kapcsolatos ügyintézését. A saját munkavállalókkal szembeni követelések kezelését az intézmény saját alkalmazottai végzik. A jogi úton történő vevő és egyéb követelésbehajtást a intézmény által megbízott jogi képviselő végzi.

#### HÁTRALÉKKEZELÉS

Az adatkezelés célja: a követelés behajtása céljából

A kezelt adatok köre: név, lakcím, születési idő és hely, anyja neve, a számlázásra és a díjfizetésre vonatkozó adatok, telefonszám, e-mail cím

Az adatkezelés jogalapja: a GDPR 6. cikk (1) f) szerinti jogos érdek érvényesítése

Az adattárolás határideje: a hátralék kiegyenlítését követő 5 évig, de legfeljebb a hátralékkal kapcsolatos polgári jogi igények elévüléséig

Adattovábbítás a jogi képviselő részére

#### 5.4.14. Közérdekű adatok kezelése

A közérdekű adatok kezeléséről "Közérdekű adatok megismerésének szabályzata" rendelkezik.

#### KÖZÉRDEKŰ ADATKEZELÉS

Az adatkezelés célja: közérdekű adatigénylések teljesítése, illetve az azzal kapcsolatos számlázás

Az adatkezelés jogalapja: 2011. évi CXII. tv. (Infotv.) 26. § - 31. §

A kezelt adatok köre: név, lakcím, telefonszám, e-mail cím, egészségügyi ellátáshoz kapcsolódó adatok

Az adattárolás határideje: 1 évig

## 6. Utalások és megjegyzések

### 6.1. Vonatkozó dokumentáció

- Az 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.);
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet – GDPR)
- 305/2005. (XII.25.) Kormányrendelet a közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról
- Alaptörvény
- A Munka Törvénykönyvéről szóló 2012. évi I. törvény
- A mindenkor hatályos Polgári Törvénykönyv
- 2003. évi XCII. törvény az adózás rendjéről
- 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (Szvmt.)
- 2003. évi C. törvény az elektronikus hírközlésről
- 33/1998 NM rendelet a munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről
- 1993. évi XCIII. törvény a munkavédelemről

- 5/1993. MüM. rendelet a munkavédelemről szóló 1993. évi XCIII. törvény egyes rendelkezéseinek végrehajtásáról
- 2000. évi C. törvény a számvitelről
- a fogyasztóvédelemről szóló 1997. évi CLV. törvény
- 2007. évi CXXVII. törvény az általános forgalmi adóról
- 1997. évi CLIV. tv. az egészségügyről (a továbbiakban: Eütv.)
- 1997. évi XLVII. tv. az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről (a továbbiakban: Eüak.)
- 1998. évi VI. tv. az egyének védelméről a személyes adatok gépi feldolgozása során Strasbourgban 1981. január 28. napján kelt Egyezmény kihirdetéséről
- 62/1997. (XII. 21.) NM rendelet az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről
- 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről

Amennyiben a vonatkozó dokumentáció tartalma változik (hatályát veszti, módosul, új lép hatályba, stb...) úgy a jelen szabályzat módosítása hiányában is értelemszerűen a megváltozott dokumentációkat kell alkalmazni.

## 6.2. Kapcsolódó dokumentumok

- NEAK szerződésben meghatározott adatközlések
- Informatikai Biztonsági szabályzat
- Információ Biztonsági Politika
- Térfigyelő rendszer adatvédelmi és adatbiztonsági szabályzata
- Beléptető rendszer adatvédelmi szabályzata
- Iratkezelési és irattározási Szabályzat
- szakmai jogszabályokban elrendelt kötelező egészségügyi adatszolgáltatások
- munkavédelmi szabályzat
- tűzvédelmi szabályzat
- közérdekű adatok megismerésének szabályzata
- térítési szabályzat
- érdekmérlegelési tesztek
- hatásvizsgálatok

## 6.3. Megjegyzések

A szabályzat által nem érintett, közérdekű adatkezeléssel, a közérdekű adatok közzétételével, az informatikai adatvédelmi, illetve iratkezelési, és titokvédelmi előírásokkal kapcsolatosan a hatályos vonatkozó Főigazgatói szabályzatok szerint kell eljárni.

## Melléletek

### 7.1. melléklet

#### Tájékoztató az egészségügyi és személyazonosító adatok kezeléséről a kapuvári Lumniczer Sándor Kórház-Rendelőintézetben és Telephelyein (továbbiakban Intézmény)

Az adatkezelés célja:	Az gyógyulása és kezelése érdekében szükségünk van arra, hogy az Ön adatait Intézményünkben felvegyük és az adatokat előírás szerint kezeljük.
Az adatkezelés jogalapja:	Az intézmény jogszerű adatkezelésének jogalapja az érintett hozzájárulása. Hivatkozva az 1997. évi XLVII. tv. az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló törvény 12. § (2) bekezdésére: Abban az esetben, ha az érintett önként fordul az egészségügyi ellátóhálózathoz, a gyógykezeléssel összefüggő egészségügyi és személyazonosító adatainak kezelésére szolgáló hozzájárulását - ellenkező nyilatkozat hiányában - megadottnak kell tekinteni, és erről az érintettet (törvényes képviselőjét) tájékoztatni kell.
Az érintettek kategóriái:	<p>Az adatokhoz csak szabályozott esetekben, a hatályos törvények által felhatalmazott egyes hivatalos szervek és hatóságok férhetnek hozzá. Az intézmény minden dolgozóját köti az orvosi titok megtartásának kötelezettsége.</p> <p>Az Intézményben, például a kórteremben vagy vizsgálatok, kezeléseik során más betegek is jelen lehetnek, mindent el fogunk követni az emberi jogok és a személyes méltóság tiszteletben tartására.</p> <p>Az Intézményben kijelölés alapján, leendő orvosok és más egészségügyi szakemberek felkészítése is folyik. Az ilyen szakember jelöltek éppúgy kötelesek az orvosi titkot megőrizni, mint az Intézmény más dolgozói. A kezeléseik egyes szakaszaiban ilyen szakember jelöltek is jelen lehetnek az Intézmény orvosain és más betegellátó személyzetén kívül.</p> <p>A vizsgálaton való részvétellel, a kezeléseik elfogadásával hozzájárul, hogy a személyes, egészségügyi adatait a gyógykezeléshez szükséges mértékben az Intézmény az irányadó adatvédelmi szabályoknak megfelelően, jogszerűen és célhoz kötötten kezelje.</p> <p>Tájékoztatjuk, hogy EESZT lakossági portálon</p>



	keresztül leilthatja egészségügyi, betegséggel kapcsolatos adatainak megtekinthetőségét.
Személyes adatok kategóriái:	A természetes személy (beteg) neve, lakcíme, telefonos elérhetősége, anyja neve, TAJ száma, betegségei, kórelőzménye, hozzátartozó (k) neve és elérhetősége
Tárolás időtartama:	Magyarországon az 1997. évi XLVII. törvény szabályozza az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelését és védelmét. E jogszabály kimondja, hogy az egészségügyi dokumentációt legalább <b>30 évig</b> , a zárójelentést legalább <b>50 évig</b> , a képalkotó diagnosztikai eljárással készült felvételt <b>10 évig</b> , a felvételtől készített leletet pedig <b>30 évig</b> kell megőrizni. Az egészségügyi dokumentációval kapcsolatban a GDPR szerinti törléshez való jog tehát korlátozottan érvényesül.
Címzettek kategóriái:	Nincsen.
Harmadik országba történő adattovábbítás:	Nincsen.
Köteles-e megadni személyes adatot?	Az Intézményben személyes és egészségügyi adatokat a gyógykezelés érdekében fogják kezelni.

7.2. melléklet

**Önkéntes hozzájárulás  
személyes/egészségügyi adataim kezeléséhez**

Alulírott érintett egyértelműen és kifejezetten hozzájárulok, hogy a jelen nyilatkozattól formailag különálló dokumentumokban, így önéletrajzomban és motivációs levelemben megtalálható adataimat a Lumniczer Sándor Kórház-Rendelőintézet, mint adatkezelő adatállományában megtarthassa abban az esetben is, ha álláspályázatomban/önéletrajzomban nem kerül kiválasztásra, a jelentkezésemtől/önéletrajzom leadásától számított 1 évig azzal a céllal, hogy az adatkezelő számomra megfelelő pozíció megnyílásakor velem a kapcsolatot felvehesse. Az aláírt hozzájárulást postai/(scannelt formában) elektronikus úton/személyesen eljuttatom az Intézmény Titkárságára 5 munkanapon belül.

Tudomásul veszem, amennyiben hozzájárulásomat nem adom, önéletrajzom/pályázatomban törlésre kerül.

Adataim kezelésével kapcsolatban tudomásul veszem a következőket:  
az adatkezelés módja: elektronikusan és papír alapon, manuálisan történik  
az adatok forrása: közvetlenül az érintettől  
adatközlés: harmadik fél számára nem kerül közlésre

Tudomásul veszem, hogy adataimmal kapcsolatban jogaim a következők: a tájékoztatás és hozzáférés joga, a helyesbítés joga, a törléshez és az „elfeledtetéshez való” jog, az adatok zároláshoz/korlátozáshoz való jog, adathordozhatóság joga.

Tudomásul veszem, hogy bármely hozzájárulásomat bármikor visszavonhatom, és jogaimmal a következő elérhetőségekre küldött nyilatkozattal élhetek:

- a. postai úton: Lumniczer Sándor Kórház-Rendelőintézet Titkárság, 9330 Kapuvár, dr. Lumniczer Sándor u. 10.
- b. e-mail-en keresztül: [titkarsag@lumniczerkorhaz.hu](mailto:titkarsag@lumniczerkorhaz.hu)
- c. vagy jelezhetem telefonon a 06/96-596504 számon.

Önrendelkezési jog megsértése esetén panasszal a NAIH-hoz (Nemzeti Adatvédelmi és Információszabadság Hatóság, 1055 Budapest, Falk Miksa utca 9-11, tel.: +36 (1) 391-1400, E-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu); [www.naih.hu](http://www.naih.hu)) vagy bírósághoz fordulhatok.

Kelt: 201\_\_ . \_\_\_\_\_ hó \_\_\_\_ napján

Érintett olvasható neve: \_\_\_\_\_

Érintett aláírása: \_\_\_\_\_

7.3. melléklet

**Adatvédelmi incidens/rendkívüli esemény jelentő lap**

Sorszám	Incidens ideje	Incidens megnevezése	Érintettek köre	Érintett személyes adatok	Incidens hatása/következményei	Intézkedések

Dátum:

A jelentőlap átvételének dátuma:

.....  
Bejelentő / Belső adatvédelmi felelős

.....  
Adatvédelmi Tisztviselő

#### 7.4. melléklet

### TÁJÉKOZTATÓ A MUNKAVÁLLALÓK RÉSZÉRE SZEMÉLYES ADATAIK KEZELÉSÉVEL KAPCSOLATBAN

#### I. Adatkezelő és az adatvédelmi tisztviselő adatai

##### I.1. Az adatkezelő

Lumniczer Sándor Kórház-Rendelőintézet

Elérhetőségei:

E-mail: titkarsag@lumniczerkorhaz.hu

Postacím: 9330 Kapuvár, dr. Lumniczer Sándor u. 10.

Telefon: 06/96-596-500

##### I.2. Adatvédelmi tisztviselő

Az adatvédelmi tisztviselő neve: Némethné Simacsek-Kun Edina

Elérhetőségei:

E-mail: adatvedelem@lumniczerkorhaz.hu

Postacím: 9330 Kapuvár, dr. Lumniczer Sándor u. 10.

Telefon: 06/96-596-541 (hétfő: 7-15 óra között)

#### II. A személyes adatok kezelésének célja, jogalapja és időtartama

Az adatkezelő jogosult kezelni a munkavállalóknak a munkaviszonnyal és a munkavégzéssel összefüggő személyes adatait. A személyes adatok kezelése a táblázatban szereplő célok 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, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendeletben (a továbbiakban: GDPR) meghatározott alábbi jogalapok szerint történik.

A munkavállalók személyes adatai kezelésének	
célja	jogalapja
a munkavállalók társadalombiztosításával, bérével és béren kívüli juttatásaival kapcsolatos ügyintézés	az adatkezelő jogi kötelezettségének teljesítése [GDPR 6. cikk (1) bek. c) pont]
a munkaviszonnyal összefüggő magatartás ellenőrzése	az adatkezelő jogos érdeke (a káresemények, illetve az adatkezelő érdekét sértő események megelőzése) [GDPR 6. cikk (1) bek. f) pont]
elektronikus megfigyelőrendszer (kamerák) által mozgókép rögzítése	az adatkezelő jogos érdeke (vagyonvédelem, biztonság) [GDPR 6. cikk (1) bek. f) pont]
foglalkozás-egészségügyi orvosi vizsgálat alapján alkalmassági vizsgálat eredményének beszerzése	szerződés teljesítése, amelyben a munkavállaló az egyik fél [GDPR 6. cikk (1) bek. b) pont]
munkajogi felelősség	az adatkezelő jogos érdeke (kártérítés, leltárhiányért való felelősség) [GDPR 6. cikk (1) bek. f) pont]
a munkahelyen belüli kapcsolattartás biztosítása	szerződés teljesítése, amelyben a munkavállaló az egyik fél [GDPR 6. cikk (1) bek. b) pont]
munkaszerződések nyilvántartása és a kapcsolódó tájékoztatók	szerződés teljesítése, amelyben a munkavállaló az egyik fél [GDPR 6. cikk (1) bek. b) pont]
tűz- és munkavédelmi oktatás	szerződés teljesítése, amelyben a munkavállaló az egyik fél [GDPR 6. cikk (1) bek. b) pont], az adatkezelő jogi kötelezettségének teljesítése

	[GDPR 6. cikk (1) bek. c) pont]
új munkavállaló beléptetése	szerződés megkötését megelőző lépés megtételéhez szükséges [GDPR 6. cikk (1) bek. b) pont]
beléptető rendszerrel történő munkaidő nyilvántartás	az adatkezelő jogos érdeke (az adatkezelő érdekét sértő események megelőzése) [GDPR 6. cikk (1) bek. f) pont]

Az adatkezelő által a munkavállalók tekintetében kezelt személyes adatok körét az adatkezelési nyilvántartása tartalmazza, amelynek tartalmáról a munkavállaló a munkáltatójától, illetve az adatvédelmi tisztviselőtől kérhet felvilágosítást.

A munkavállalók személyes adatait az adatkezelő a vonatkozó jogszabályban, kifejezett jogszabályi rendelkezés hiányában pedig az Iratkezelési és irattározási szabályzat 1. számú mellékletében meghatározott ideig kezeli.

Amennyiben a személyes adat szolgáltatása jogszabályi kötelezettségen alapul, és az érintett ennek nem tesz eleget, az a munkaviszony megszüntetését eredményezheti.

Jogszabály által előírt esetekben az adatkezelő jogosult kezelni munkavállalói hozzátartozóinak személyes adatait.

A munkavállalók részére biztosított hivatali mobiltelefon, hivatali laptop és személyi számítógép, valamint a hivatali e-mail postafiók munkavégzés céljára használható. Amennyiben a munkavállaló a hivatali mobiltelefonon, hivatali laptopon, illetve személyi számítógépen saját személyes adatait tárolja, a személyes adatainak az eszközön való elhelyezésével tudomásul veszi, hogy azokhoz az adatkezelő hozzáférhet. A munkavállaló a hivatali e-mail postafiókról saját személyes adatait magáncélból nem küldheti el, más személy által magáncélból megküldött bármely személyes adatot pedig köteles haladéktalanul törölni a hivatali e-mail postafiókból. E rendelkezések megsértése esetén adatkezelőnek a munkavállaló minősül, az adatkezelő vonatkozásában megállapított kötelezettségek, valamint az ezzel kapcsolatos felelősség őt terhelik.

A munkavállalók munkaviszonnal összefüggő magatartásának ellenőrzése érdekében az adatkezelő minden munkavállaló tekintetében jogosult betekinteni az alábbi technikai eszközök által rögzített személyes adatokba:

- az adatkezelő által a munkavállaló részére biztosított hivatali mobiltelefon, hivatali laptop, személyi számítógép.

Az ellenőrzésre – összhangban a munka törvénykönyvről szóló 2012. évi I. törvény 11. § (1) bekezdésével – minden esetben a munkaviszonnal összefüggő magatartás körében kerül sor. Az alkalmazott eszközök nem járnak az emberi méltóság megsértésével, valamint nem irányulnak a munkavállaló magánéletének ellenőrzésére.

Ellenőrzésre büncselekmény, szabálysértés elkövetésének vagy munkaviszonyból származó kötelezettség megszegésének gyanúja esetében kerülhet sor.

Az ellenőrzés tényéről, elvégzésének körülményeiről, az ezzel összefüggő adatkezelés céljáról, időtartamáról, az adatkezeléssel kapcsolatos jogairól a munkavállalót előzetesen szóban, távolléte esetén írásban tájékoztatni kell. A szóbeli tájékoztatás megtörténtét a munkavállaló aláírásával tanúsítja. Az aláírás megtagadása esetében a tájékoztatást két tanú jelenlétében meg kell ismételni. Az előzetes tájékoztatás az ellenőrzésre okot adó körülmény figyelembevételével mellőzhető.

Az ellenőrzést a fokozatosság elvének betartásával kell végezni. Az ellenőrzésnél – ha erre mód van – biztosítani kell a munkavállaló jelenlétét.

## **II.1. Tájékoztató elektronikus megfigyelőrendszer (videokamerák) alkalmazásáról**

Az elektronikus megfigyelőrendszer által rögzített személyes adatok kezelése az adatkezelő jogos érdekeinek érvényesítéséhez, biztonsági és vagyónvédelmi okból szükséges [GDPR 6. cikk (1) bek. f) pont].

Az adatkezelő a kamerarendszer telepítésekor mérlegelte annak a munkavállalókra gyakorolt hatását, és megállapította, hogy a felvételek készítése nem jár az érintettek érdekeire, alapvető jogaira és szabadságaira nézve aránytalan és szükségtelen mértékű korlátozással.

A kamerák kihelyezésére kizárólag biztonsági és vagyónvédelmi okból kerül sor, a rendszer nem irányul a munkavállalók tevékenységének és munkavégzésének megfigyelésére és ellenőrzésére. Egyetlen kamera sem

figyel meg közterületet, munkavállalók munkaközi pihenőjének eltöltése céljára kijelölt területet, öltözőt és mosdót. A kamerák kizárólag képfelvételt (vagy: kép- és hangfelvételt) rögzítenek.

Szabálysértés vagy bűncselekmény gyanúja miatt indult eljárás esetén a felvétel továbbításra kerül az illetékes hatóságok részére.

A kamerák felvételeit az adatkezelő a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény 31. § (2) és (5) bekezdése alapján felhasználás hiányában legfeljebb a rögzítéstől számított három munkanapig őrzi meg, ezt követően törli. Ha a felvétel bírósági vagy más hatósági eljárásban bizonyítékként kerül felhasználásra, az eljárás jogerős befejezését követően kerül törlésre.

Akinek jogát vagy jogos érdekét a képfelvétel, illetve más személyes adatának rögzítése érinti, a képfelvétel, illetve más személyes adat rögzítésétől számított három munkanapon belül jogának vagy jogos érdekének igazolásával kérheti, hogy az adatot annak kezelője ne semmisítse meg, illetve ne törölje. Bíróság vagy más hatóság megkeresésére a rögzített képfelvételeket, valamint más személyes adatot a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni. Amennyiben a megkeresésre attól számított harminc napon belül, hogy a megsemmisítés mellőzését kérték, nem kerül sor, a rögzített képfelvételeket, valamint más személyes adatot meg kell semmisíteni, illetve törölni kell.

## **II. 2. Tájékoztató beléptető rendszer alkalmazásáról**

A munkahelyi adatkezelések esetén az adatkezelés jogalapja az adatkezelő jogos érdeke, valamint törvényen (a Munka Törvénykönyvében) alapul. A munkaidő nyilvántartást illetően a Munka Törvénykönyve azt írja elő, hogy a munkáltató "kötelessége nyilvántartani a rendes és rendkívüli munkaidőt, a készenlét és a szabadság tartamát". Ennek megfelelően a munkaidőre vonatkozó adatokat a munkáltató jogszerűen vezeti, saját törvényi kötelezettségének teljesítése érdekében, a törvény alapján. A nyilvántartásra ennek megfelelően párhuzamosan vonatkoznak a munkajogi és az adatvédelmi előírások: a nyilvántartást naprakészen és pontosan kell vezetni, úgy, hogy abból megállapítható legyen a teljesített rendes és rendkívüli munkaidő.

Az első kártyát az Intézmény ingyenesen biztosítja a munkavállalónak, ugyanakkor a jogviszony megszűnéskor a kártyát a kilépési folyamat során le kell adni ..... az irodában, a kártya leadásával a beléptető rendszerből törlésre kerülnek a személyes, valamint a hozzá kapcsolt kártya adatok. A kártya le nem adása esetében eljárási díjat kell fizetni. Az eljárási díj aktuális összegét az évenként felülvizsgált Térítési Szabályzat tartalmazza, melynek befizetése a kilépő munkavállalónak az Intézmény pénztárában történik.

A kártya elvesztését 3 munkanapon belül jelezni kell a HR-nek, ezzel egyúttal megtörténik az új kártya igénylése is. A kártya elkészültéről a HR értesíti az igénylőt, akinek az új kártya felvételekor a Térítési Szabályzatban rögzített összeg kifizetésével jogosult annak birtoklására és használatára.

A beléptetőrendszerben csak a kiadott kártyák használhatóak a belépési jogosultság megállapítására. Minden személy a saját kártyáját használhatja, a kártya átadása más személynek nem megengedett, következménye a munkavállaló munkaviszonyának azonnali hatályú megszüntetése.

## **III. A személyes adatok továbbítása és adatfeldolgozó igénybevétele**

A munkavállalók személyes adatainak továbbítása a vonatkozó jogszabályi előírások alapján, elektronikusan dokumentált és visszakövethető módon történik.

Szerződéses partnerekkel és ügyfelekkel történő kapcsolattartásra kijelölt munkavállalóknak a kapcsolattartáshoz szükséges személyes adatait az adatkezelő jogosult megküldeni a partner részére.

A munkavállalók személyes adatait az adatkezelő az Európai Unió kívüli országba vagy nemzetközi szervezet részére a GDPR vonatkozó rendelkezéseinek megfelelően továbbítja.

A munkaviszonyból származó jogok gyakorlásának és kötelezettségek teljesítésének elősegítése érdekében az adatkezelő a munkavállalók személyes adatait az Államkincstár Központi rendszerén kívül a Nexon rendszerben is kezeli. A Nexon rendszerben kezelt személyes adatokhoz csak az érintett munkavállaló, a munkáltató, továbbá – ügyfél-támogatási feladatainak ellátása érdekében, az adatkezelő eseti engedélyével – a Nexon Kft. Ügyfélszolgálatára férhet hozzá. A Nexon rendszerben tárolt személyes adatok tekintetében a Nexon Kft. az adatkezelő adatfeldolgozójaként jár el.

## **IV. A személyes adatok védelmét biztosító garanciák**

A munkavállalók személyes adatai biztonságának megőrzését az adatkezelőnél a következő technikai és

szervezési intézkedések garantálják:

- a) az elektronikusan tárolt személyes adatokhoz csak a munkáltató férhet hozzá;
- b) külső és belső tűzfalak, behatolást jelző és megakadályozó (IDS/IPS) csomagszűrő eszközök, vírusvédelmi szoftverek;
- c) rendszeres (általában naponta történő) mentés, oly módon, hogy adatsérülés esetében az adott napon belüli változások is visszaállíthatók;
- d) a munkaviszonnyal, munkavégzéssel összefüggő személyes adatokat tartalmazó papíralapú iratok zárt szekrényben történő tárolása.

## **V. Az adatkezeléssel érintettek jogai**

A munkavállaló jogosult személyes adatai kezelését illetően az adatkezelőtől

- tájékoztatást kapni az adatkezeléssel kapcsolatos körülményekről;
- a személyes adatok helyesbítését vagy – a GDPR szerint meghatározott esetekben – törlését kérni;
- az adatkezelés korlátozását kérni;
- tájékoztatást kapni azon címzettekről, akikkel helyesbítéssel, törléssel vagy az adatkezelés korlátozásával érintett személyes adatát közölték;
- hozzáférni személyes adataihoz;
- tiltakozni a jogos érdek nélküli adatkezelés ellen.

Tekintettel arra, hogy az adatkezelőnél nem történik automatizált módon adatkezelés, így az adathordozhatósághoz, valamint az automatizált döntéshozatal elleni tiltakozáshoz való jog nem illeti meg a munkavállalókat.

A munkavállaló a fenti jogaival kapcsolatos kérelmét írásban vagy elektronikus úton, a munkáltatónak címezve terjesztheti elő a tájékoztató I.1. pontjában szereplő elérhetőségek bármelyikén.

Az adatkezelő a kérelemről indokolatlan késedelem nélkül, legkésőbb a beérkezésétől számított egy hónapon belül dönt, és tájékoztatja a munkavállalót a kérelem nyomán hozott intézkedésekről, vagy amennyiben intézkedés nem történik, ennek okáról, a felügyeleti hatósághoz panasz, illetve a bírósághoz jogorvoslat benyújtásának lehetőségéről.

Az intézkedés határideje szükség esetén, a kérelem összetettségére és a kérelmek számára figyelemmel további két hónappal meghosszabbítható. A határidő meghosszabbításáról okainak megjelölésével a kérelem beérkezésétől számított egy hónapon belül az adatkezelő tájékoztatja a kérelmezőt.

Amennyiben az érintett kérelme egyértelműen megalapozatlan vagy túlzó, az adatkezelő díjat számíthat fel vagy megtagadhatja az intézkedést.

### **V.1. Az érintett tájékoztatáshoz való joga**

Az adatkezelő e tájékoztatás közzétételével intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó, a GDPR 13. cikke által meghatározott minden információ a rendelkezésére álljon.

Abban az esetben, ha a rendelkezésre bocsátott adatokat az adatkezelő nem az érintettől szerezte meg, az adat megszerzését minden esetben az adatkezelőre alkalmazandó uniós vagy tagállami jog írja elő.

### **V.2. Az érintett hozzáférési joga**

Az érintett személyazonosságának igazolását követően jogosult arra, hogy az adatkezelőtől visszajelzést kapjon a személyes adatainak kezeléséről. A hozzáférési jog gyakorlásával összefüggő tájékoztatást az adatkezelő írásban, postai vagy elektronikus úton adja meg.

### **V.3. A helyesbítéshez és törléshez való jog**

Az érintett kérheti, hogy az adatkezelő helyesbítse a rá vonatkozó pontatlan adatot.

Az érintett jogosult arra, hogy indokolt kérelmére az adatkezelő késedelem nélkül törölje a rá vonatkozó személyes adatot. Az adatkezelő köteles törölni a személyes adatot, amennyiben:

- a személyes adatokra már nincs szükség abból a célból, amelyből azokat kezelték;
- az érintett visszavonja a hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;

- a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell.

Az érintett nem gyakorolhatja a törléshez való jogát többek között abban az esetben, ha az adatkezelés

- a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése céljából,
- jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges.

#### **V.4. Az adatkezelés korlátozásához való jog**

Az érintett jogosult arra, hogy indokolt kérelmére az adatkezelő korlátozza az adatkezelést, ha:

- az érintett vitatja a személyes adatok pontosságát (amíg az adatkezelő ellenőrzi az adatok pontosságát);
- az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését;
- 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 (amíg az adatkezelő el nem bírálja a tiltakozás iránti kérelmet).

A korlátozás ideje alatt a személyes adatokat tárolás kivételével többek között csak az érintett hozzájárulásával vagy jogi igények érvényesítéséhez kapcsolódó adatkezelés esetén lehet tovább kezelni.

#### **V.5. A tiltakozáshoz való jog**

Az érintett abban az esetben tiltakozhat az adatkezelés ellen, amennyiben annak jogalapja az adatkezelő jogos érdekeinek érvényesítése. Ebben az esetben az adatkezelő csak akkor kezelheti tovább az adatokat, ha igazolja, hogy az adatkezelést elsőbbséget élvező jogos okok indokolják vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

### **VI. Jogorvoslatok rendje**

#### **VI. 1. Panasz benyújtása az adatvédelmi tisztviselőhöz**

Amennyiben személyes adatainak kezelésével összefüggésben panasszal kíván élni, forduljon az adatkezelő adatvédelmi tisztviselőjéhez az alábbi elérhetőségek valamelyikén:

Az adatvédelmi tisztviselő neve: Némethné Simacsek-Kun Edina

E-mail címe: [adatvedelem@lumniczerkorhaz.hu](mailto:adatvedelem@lumniczerkorhaz.hu)

Telefonszáma: 06/96-596-541

Postacíme: 9330 Kapuvár, dr. Lumniczer Sándor u. 10.

#### **VI. 2. Bírósági eljárás indítása**

Ha Önt érintetti jogainak gyakorlásával összefüggésben vagy a személyes adatai kezelése során jogsértés éri, polgári pert kezdeményezhet az adatkezelő ellen. A per elbírálása törvényszék hatáskörébe tartozik. Az eljárás megindítható az érintett lakóhelye vagy tartózkodási helye szerinti törvényszék előtt. A bíróság az ügyben soron kívül jár el. A jogsértés megállapítása esetén Ön kártérítésre és sérelemdíjra tarthat igényt, valamint a bíróság kötelezheti az adatkezelőt az érintetti jogok gyakorlásának teljesítésére.

További információt és a törvényszékek elérhetőségét az alábbi linken tekintheti meg:

<http://birosag.hu/torvenyszekek>

#### **VI. 3. Panasz benyújtása a felügyeleti hatósághoz**

Amennyiben Önt a személyes adatok kezelésével kapcsolatban sérelem éri, panaszával a Nemzeti Adatvédelmi és Információszabadság Hatósághoz fordulhat.

A hatóság elérhetősége: 1055 Budapest, Falk Miksa utca 9-11.

E-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

Telefon: +3613911400

Postacím: 1530 Budapest, Pf.: 5.

Honlap: [www.naih.hu](http://www.naih.hu)

A tájékoztatóban foglaltakat megismertem.

Kelt: Kapuvár, .....

---

munkavállaló aláírása



## ADATKEZELŐK NYILVÁNTARTÁSI LAPJA

..... OSZTÁLY/EGYSÉG

Felhasználó neve	Felhasználó típusa	Munkahelyek	Megjegyzés	Megszűnés
	<input type="checkbox"/> orvos <input type="checkbox"/> egészségügyi adminisztrátor <input type="checkbox"/> egyéb adminisztrátor			
	<input type="checkbox"/> orvos <input type="checkbox"/> egészségügyi adminisztrátor <input type="checkbox"/> egyéb adminisztrátor			
	<input type="checkbox"/> orvos <input type="checkbox"/> egészségügyi adminisztrátor <input type="checkbox"/> egyéb adminisztrátor			
	<input type="checkbox"/> orvos <input type="checkbox"/> egészségügyi adminisztrátor <input type="checkbox"/> egyéb adminisztrátor			

7.6. melléklet

Szoftver felhasználói hozzáférési űrlap

.....OSZTÁLY/EGYSÉG

Felhasználó neve (pecsész. is, ha orvos)	Adatkezelő Felvétel/törlés	Felhasználó típusa	Megadandó munkahelyek megnevezése	Szoftver neve - moduljai	Jogviszonyra vonatkozó adatok
	<input type="checkbox"/> Felvétel  <input type="checkbox"/>  Törlés/passzivalás	<input type="checkbox"/> orvos  <input type="checkbox"/> egészségügyi adminisztrátor  <input type="checkbox"/> egyéb adminisztrátor			Kezdetre: Szervezeti egység: Munkakör: Jogv. vége esetén: Megszűnés dátuma:
	<input type="checkbox"/> Felvétel  <input type="checkbox"/>  Törlés/passzivalás	<input type="checkbox"/> orvos  <input type="checkbox"/> egészségügyi adminisztrátor  <input type="checkbox"/> egyéb adminisztrátor			Kezdetre: Szervezeti egység: Munkakör: Jogv. vége esetén: Megszűnés dátuma:

\* Engedélyezve/ Végrehajtás időpontja:

\* Nem engedélyezve,

mert.....

\*Törlést/Passzivalást tudomásul vettem

.....

Osztályos Adatvédelmi Felelős

Adatvédelmi Tisztviselő

Kapuvár, .....év ..... hó ..... nap

\* Adatvédelmi Tisztviselő által megfelelő aláírandó!

## 8. Függetlenség