Ikt.szám: FOIG/281-1/2024.

BALATONFÜREDI ÁLLAMI SZÍVKÓRHÁZ

Adatvédelmi és Adatbiztonsági Szabályzat

Készítette:

Simon Csaba
informatikai vezető

Jóváhagyta:

Dátum:

Balatonfüred,
2011. 06. 22.

Prof. Dr. Veress Gábor
főigazgató

A dokumentáció kódja:	**AASZ**
Változat száma:	**1**
Oldalak száma:	**42**
Mellékletek száma:	**6**
Érvénybelépés időpontja:	**2011. 06.22.**

módosítások jegyzéke

Módosította Aláírás/dátum	Változat száma	Módosított oldalszám	Jóváhagyta Aláírás/dátum	Ellenőrizte Aláírás/ dátum	Kibocsátás időpontja
2016.01.01. Simon Csaba	2	GIG/387-1/2016.	Prof. Dr. Veress Gábor 2016.01.01.	2016.01.01.	2016.01.01.
2019.01.02.	3	GIG/18-1/2019.	Prof. Dr. Veress Gábor 2019.01.02.	2019.01.02.	2019.01.02.
2021.09.01. Varga Róbert	4	FOIG/100-1/2021.	Prof. Dr. Veress Gábor 2021.09.01.	2021.09.01.	2021.09.01.
2024.09.01. Varga Róbert Csendes Judit	5	Oldalszám: 95	Dr. Simon Attila 2024.09.01.	Dr. Simon Attila 2024.09.01.	2024.09.01.

A Balatonfüredi Állami Szívkórház (a továbbiakban: Intézet) főigazgatója az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.), az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (a továbbiakban: Eüak.), valamint az Európai Parlament és a Tanács 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 2016/679. számú Rendelete (a továbbiakban: Rendelet) alapján az alábbiak szerint állapítja meg az Intézetben történő adatkezelés rendjét.

1.rész
Általános adatvédelmi szabályok

I. fejezet
A szabályzat célja és hatálya

1. § (1) Ezen rész célja, hogy meghatározza az Intézet, mint adatkezelő által végzett adatkezelési tevékenység törvényes rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését.

(2) Ezen rész tárgyi hatálya kiterjed az Intézet szervezeti egységeinél folytatott valamennyi személyes adatokat tartalmazó adatkezelésre. Az egészségügyi adatokra vonatkozó különös szabályokat az jelen szabályzat egészségügyi adatvédelmi fejezete tartalmazza; e szabályzat rendelkezéseit az egészségügyi adatok tekintetében ezen fejezetben foglalt eltérésekkel kell alkalmazni.

(3) Ezen rész személyi hatálya az Intézettel egészségügyi szolgálati jogviszonyban, valamint munkavégzésre irányuló egyéb jogviszonyban álló személyekre, továbbá az intézeti adatkezeléssel érintett bármely természetes és jogi személyre terjed ki.

II. fejezet
Értelmező rendelkezések és alapelvek

2. § E szabályzat alkalmazásában

a) személyes adat: azonosított vagy azonosítható természetes személyre (továbbiakban: érintett) vonatkozó bármely információ, amely alapján az érintett 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;

b) különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adat, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok;

c) 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

d) személyazonosító adat: az egészségügyi adat érintettjének azonosítására szolgáló személyes adat, amelyet az adatkezelő az egészségügyi adattal együtt, az egészségügyi adat kezelésével azonos vagy attól elválaszthatatlan céllal az egészségügyi dokumentáció részeként kezel.

e) 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;

f) adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége.

3. § (1) Az Intézet az adatkezelési tevékenységét a Rendelet 5. cikk (1) bekezdésében megfogalmazott alapelvek, a jogszerűség, tisztességes eljárás és átláthatóság elve, a célhoz kötöttség, az adattakarékosság és a korlátozott tárolhatóság elve, a pontosság elve és az integritás és bizalmas jelleg biztosításának elve alapján végzi.
(2) Az Intézet – a Rendelet 25. cikkében foglalt beépített és alapértelmezett adatvédelem elvével összhangban – megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása céljából, hogy az Intézet adatkezelése a vonatkozó szabályokkal összhangban történjen.
(3) Az Intézet valamennyi szervezeti egysége gondoskodik arról, hogy az Intézet képes legyen az alapelveknek és az adatkezelés szabályainak való megfelelés igazolására (elszámoltathatóság elve).

III. fejezet
Az adatkezelés és az adatfeldolgozás

4. § (1) Az Intézetben folyatott adatkezelések adatkezelője az Intézet, amely az adatkezeléseket erre felhatalmazott szervezeti egységei (továbbiakban: adatkezelő szervezeti egység) útján végzi. Az egyes adatkezelések adatkezelő szervezeti egységét az adatkezelések nyilvántartása tartalmazza.
(2) A fentiektől eltérően amennyiben az adatkezelés különleges célja azt indokolja, és az adatkezelés célját az Intézet valamely szervezeti egysége önállóan határozza meg, vagy törvény az adatkezelő személyét kifejezetten nevesíti, az Intézet valamely szervezeti egysége adatkezelőnek minősülhet. Az adatkezelések nyilvántartásában ezt a tényt egyértelműen fel kell tüntetni.
(3) Az Intézet egyes adatkezelési műveletek tekintetében adatfeldolgozót vehet igénybe. Az adatfeldolgozó az adatkezelő nevében, annak megbízásából és adott esetben konkrét utasításai szerint az adatkezelő számára adatfeldolgozást végez. Adatfeldolgozó az Intézettel szerződéses viszonyban álló harmadik személy (jogi, vagy természetes) lehet.
(4) Harmadik személy adatfeldolgozó esetén az adatfeldolgozás feltételeit írásbeli megállapodásba kell foglalni. A megállapodás más szerződés részeként is megkötheto. (5) Adatfeldolgozás történhet jogszabályi előírás alapján is, ez esetben az adatfeldolgozói jogviszonyra a jogszabályi előírások az irányadók.

(6) Az adatfeldolgozási megállapodás tartalmazza legalább:
a) az adatfeldolgozás tárgyát, célját, időtartamát, a személyes adatok típusát és az érintettek körét;
b) azt, hogy – ha jogszabály másként nem rendelkezik – az adatfeldolgozó az adatfeldolgozást az adatkezelő írásbeli utasításai szerint végzi, valamint az utasításadás körülményeit, így különösen az arra jogosult szervezeti egység vagy személynevét.
c) azt, hogy az adatfeldolgozó jogosult-e további adatfeldolgozó igénybevételére, és – amennyiben jogosult – a további adatfeldolgozó igénybevételével vagy cseréjével kapcsolatos tájékoztatási kötelezettséget;
d) az adatfeldolgozó adatbiztonsági intézkedéseit;
e) az adatvédelmi incidensekről való tájékoztatásrendjét;
f) az érintett jogainak biztosításával kapcsolatos együttműködési szabályokat;
g) az adatfeldolgozó titoktartási kötelezettségét;
h) az arra vonatkozó kötelezettséget, hogy az adatfeldolgozó – jogszabály eltérő rendelkezése hiányában – az adatfeldolgozás befejezését követően az adatkezelő döntésének megfelelően

valamennyi személyes adatot (ideértve a meglévő másolatokat) töröl vagy azokat az adatkezelőnek visszajuttatja;

i) azt, hogy az adatfeldolgozó rendelkezésre bocsát minden olyan információt, amely az adatkezelő jogszabályi kötelezettségeinek betartásához szükséges;

j) azt, hogy az adatfeldolgozó az adatkezelő rendelkezésére bocsát minden olyan információt, amely az adatfeldolgozás jogszerűségének igazolásához szükségesek, valamint együttműködik az adatkezelés ellenőrzése, helyszíni vizsgálata vagy auditja során;

k) szükség esetén az adatkezelő és adatfeldolgozó további jogait és kötelezettségeit.

IV. fejezet
Az adatkezelések szabályai

Az adatkezelés célja

5. § (1) Az Intézet személyes adatot a működésével összefüggésben felmerült célokból, így különösen foglalkoztatási célból, felsőoktatási szakképzési tevékenység végzése céljából, személy- és vagyonbiztonságot szolgáló eszközök üzemeltetése céljából, az intézeti működéshez kapcsolódó iratkezelési folyamatok, informatikai műveletek és az információbiztonság biztosítása céljából, kutatási célból, az Egészségügyi Adatvédelmi Szabályok részben foglaltaknak megfelelően egészségügyi szolgáltatások nyújtása, valamint az Intézet Alapító Okiratában meghatározott további alaptevékenységek ellátása céljából kezel.

(2) Az Intézet további adatkezelési célokkal is végezhet adatkezelést, ha annak jogszabályi feltételei fennállnak.

(3) Az egyes rendszeres adatkezelések pontos célját az adatkezelési nyilvántartás rögzíti.

Az adatkezelés jogalapja

6. § (1) Az Intézet személyes adatot akkor kezelhet, ha:

a) Az adatkezelést törvény a közérdekű tevékenység gyakorlásának keretében végzett feladat végrehajtása érdekében elrendeli (kötelező adatkezelés). Ilyen adatkezelés különösen a foglalkoztatással, vagy az egészségügyi szolgáltatások nyújtásával összefüggő adatkezelés.

b) Az adatkezelés jogi kötelezettség teljesítéséhez szükséges (pl. kötelező adatszolgáltatás).

c) Az érintett az adatkezeléshez hozzájárulását adta. Ilyen adatkezelés különösen a tudományos kutatásban való részvétellel összefüggő adatkezelés.

d) 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. Ilyen adatkezelés lehet különösen valamely intézet által nyújtott, önkéntesen igénybe vehető szolgáltatás során történő adatkezelés (pl. az intézet dolgozóinak szervezett csereüdülés, vagy harmadik felek számára szerződés alapján végzett egészségügyi tevékenység).

e) Az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges.

f) Az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

(2) (1) c) ponthoz: A hozzájárulás az érintett akaratának önkéntes, konkrét és megfelelő

tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez. Az érintett a hozzájárulását bármikor visszavonhatja.

(3) A hozzájárulással csak olyan adatkezelés folytatható, amelynek során az előzetes tájékoztatás követelményeinek betartása és az önkéntesség igazolható. Nem igazolható az önkéntesség, amennyiben a kizárólag az Intézet érdekeit szolgáló adatkezeléshez a hozzájárulást alá- fölérendeltségi viszonyban, tömegesen, meghatározott személyi körben kivétel nélkül adták meg az érintettek.

(4) A hozzájárulás bármely olyan formában megadható, amelynek során az érintett azonosítható, és a hozzájárulás ténye rögzített, így különösen:

a) írásban (az érintett aláírásával);

b) elektronikus úton az érintettnek az Intézet által nyilvántartott elektronikus levelezési címéről küldött üzenetben, amennyiben az üzenet változtatások nélküli rögzítése és megőrzése biztosított.

(5) (1) f) ponthoz: Amennyiben kifejezetten indokolt, az adott adatkezelés előtt az adatkezelő szervezeti egység érdekmérlegelést végezhet. Érdekmérlegelésen alapuló adatkezeléseknél az érdekmérlegelés elvégzését és eredményét dokumentálni kell. A dokumentum az adatkezelési nyilvántartás mellékletét képezi.

(6) Érdekmérlegelésen alapuló adatkezelés megkezdése előtt az adatkezelő szervezeti egység az adatvédelmi tisztviselővel előzetesen írásban konzultál.

(7) Különleges adat kizárólag a Rendelet 9. cikk (2) bekezdésben foglalt valamely feltétel fennállása esetén kezelhető.

Előzetes tájékoztatás

7. § (1) Ha a személyes adatokat az Intézet az érintettől gyűjti, az adatkezelés megkezdése előtt közölni kell vele a Rendelet 13. cikkében meghatározott információkat, így különösen, de

nem kizárólag:

1. az adatkezelés célját és jogalapját,
2. az adatkezelés várható időtartamát vagy az időtartam meghatározásának szempontjait, 3. az adatkezelő és képviselője elérhetőségeit, valamint az intézmény adatvédelmi tisztviselője nevét és elérhetőségét,
4. az érintettnek a rá vonatkozó személyes adatok kezelésével kapcsolatos jogait és a jogorvoslat lehetőségeit,
5. adott esetben a személyes adatok címzettjeit, illetve a címzettek kategóriáit. (2) A fentiek alapján meghatározott információkat tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva, főszabály szerint írásban – beleértve az elektronikus utat is – kell közölni az érintettel.

(3) Az érintett előzetes tájékoztatását a Balatonfüredi Állami Szívkórház Adatkezelési tájékoztatója jelenti, amely elérhető nyomtatottan az intézet főportáján, elektronikusan az intézet honlapján, illetve az x meghajtó ISO könyvtárának szabályzatai között is.

Titoktartási kötelezettség

8. § Az Intézetben adatkezelést vagy adatfeldolgozást végző alkalmazottak kötelesek a tevékenységük során általuk megismert személyes adatokat bizalmasan kezelni és titokként megőrizni. Adatkezeléssel, adatfeldolgozással, vagy személyes adatok megismerésével járó munkakörben csak az foglalkoztatható, aki titoktartási nyilatkozatot tett.

Az adatkezelési nyilvántartás

9. § (1) Az Intézetben folyó adatkezelési tevékenységek nyilvántartása valamint az egyes adatkezelésekre vonatkozó további különös szabályok megállapítása céljából – e szabályzat felhatalmazása alapján – valamennyi adatkezelésről adatkezelői nyilvántartást kell készíteni. A nyilvántartást az egyes adatkezelő szervezeti egységek vezetői készítik el és tartják karban,

szükség szerint az adatvédelmi tisztviselő szakmai segítségével.
(2)Az adatkezelési nyilvántartás a jogszabályok és az intézeti szabályzatok keretei között az egyes adatkezelésekre nézve dokumentálja az adatkezelés alapvető körülményeit és szabályozza az adatkezeléssel kapcsolatos egyes kérdéseket. Az adatkezelés alapvető körülményei különösen:
a) az adatkezelés megnevezése és rövid leírása;
b) az adatkezelő megnevezése
c) adatfeldolgozó igénybevétele esetén az adatfeldolgozás célja és egyéb körülményei, az adatfeldolgozó neve, elérhetőségei, az adatfeldolgozás helye és az adatfeldolgozói megállapodás elérhetősége;
d) az adatkezelésre vonatkozó jogszabályhelyek megnevezése;
e) az adatkezelés célja(i);
f) az adatkezelés jogalapja(i);
g) az érintettek köre és (becsült)száma;
h) a nyilvántartott adattípusok köre;
i) az adatok forrása (az érintett, vagy más adatkezelés);
j) az adatokon végzett gyakori adatkezelési műveletek (tárolás, módosítás, aktualizálás, adattovábbítás, stb.);
k) adattárolás helye;
l) technikai és szervezési intézkedések;
m) az adatok megőrzésének, törlésének ideje.

(3)Az adatkezelési nyilvántartás mellékletként tartalmazza:
a) amennyiben az adatkezelés jogalapja érdekmérlegelés, az érdekmérlegelés elvégzését és eredményét bemutató leírást;
b) amennyiben az adott adatkezeléshez szükséges, az elvégzett adatvédelmi hatásvizsgálat, a felügyeleti hatósággal történő konzultáció eredményét;

Adatvédelmi hatásvizsgálat és előzetes hatósági konzultáció

10. § (1) Az Intézet az adatkezelést megelőzően szükség esetén hatásvizsgálatot végezhet arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik, ha valamely új adatkezelés – különösen új technológia alkalmazására, az adatkezelés jellegére, hatókörére, körülményére és céljaira tekintettel – valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve.

(2) Nem kell adatvédelmi hatásvizsgálatot folytatni a törvényen alapuló (kötelező) adatkezelések, és a jogi kötelezettség teljesítéséhez szükséges adatkezelések esetén, valamint azon adatkezelések esetén, amelyek a felügyeleti hatóság adatvédelmi hatásvizsgálat alól mentességet élvező adatkezelések jegyzékében találhatók.
(3) A hatásvizsgálat kiterjed legalább:
a) a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak és jogalapjának ismertetésére; ideértve az érdekmérlegelésen alapuló adatkezelés esetén az adatkezelő által érvényesíteni kívánt jogos érdeket is;
b) az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
c) az érintettek jogait és szabadságait érintő kockázatok vizsgálatára; és d) a kockázatok kezelését célzó intézkedések bemutatására, ideértve a jogszabályoknak és e szabályzatnak való megfelelés igazolását szolgáló, az érintettek jogos érdekeit figyelembe vevő garanciákat és adatbiztonsági intézkedéseket.
(4) Az adatvédelmi hatásvizsgálat lefolytatása az adatkezelő szervezeti egység és az adatvédelmi tisztviselő együttes feladata.
(5) Az elkészült hatásvizsgálat eredményét az adatvédelmi tisztviselőnek meg kell küldeni. Az adatvédelmi tisztviselő a hatásvizsgálattal kapcsolatban észrevételeket tehet. Amennyiben a tervezett adatkezelés megvalósul, a hatásvizsgálat eredményét az adatkezelés nyilvántartásához csatolni kell, illetve amennyiben az adatkezelés jellege indokolja, az intézet honlapján is közzé kell azt tenni.

(6) Amennyiben az adatvédelmi hatásvizsgálat megállapítja, hogy a tervezett adatkezelés – a kockázatok mérséklése céljából tett intézkedések hiányában – ténylegesen magas kockázattal járna, a személyes adatok kezelését megelőzően az Intézet az adatvédelmi tisztviselő közreműködésével konzultál a felügyeleti hatósággal. Az előzetes konzultáció szükségességével kapcsolatban az adatvédelmi tisztviselő véleményét ki kell kérni.

Az érintett jogai

11. § (1) Az adatkezeléssel érintett személy jogosult a Rendelet 15-22. cikkében foglalt jogai gyakorlására, így különösen:
1. a rá vonatkozó adatkezeléshez kapcsolódó, a Rendeletben meghatározott információkhoz hozzáférni,
2. a rá vonatkozó téves vagy pontatlan személyes adatok, kijavítására, helyesbítésére,

3. jogszabályban meghatározott esetekben a rá vonatkozó személyes adat törlésére, vagy az adatkezelés korlátozására,
4. az Intézet rendelkezésére bocsátott, rá vonatkozó személyes adatokat széles körben használt elektronikus formában megkapni és az adatokat más adatkezelő részére továbbítani,
5. érdekmérlegelésen alapuló adatkezelés esetén a saját helyzetével kapcsolatos okokból tiltakozni személyes adatainak a Rendeletben meghatározottakon alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben az Intézet személyes adatokat nem kezelheti tovább, kivéve, ha az Intézet 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,
6. a Rendeletben meghatározottak szerint kérheti a személyes adataira vonatkozó adatkezelés korlátozását.

(2)Az (1) bekezdésben meghatározott érintetti jogok gyakorlását az Intézet kérelemre biztosítja, amelyet elsőként az adatvédelmi tisztviselőhöz kell intézni, aki azt jogszerűsége esetén az adatkezelés nyilvántartása alapján meghatározott, illetékes ügyintézőhöz irányítja. Amennyiben az érintetti jogok gyakorlása személyes adatok megismerését eredményezi, az csak az érintett azonosítása mellett gyakorolható, így különösen
a) írásban (az érintett aláírásával);
b) az érintett egyedi azonosítását követően elektronikusan, amennyiben a hozzáférés ténye rögzített (naplózott);
c) elektronikus úton az érintettnek az Intézet által nyilvántartott elektronikus levelezési címéről küldött üzenetben, amennyiben az üzenet változtatások nélküli rögzítése és megőrzése biztosított;
d) szóban (kizárólag személyesen), amennyiben az azonosítás azonosításra szolgáló igazolvánnyal biztosított.
(3) A személyes adatokhoz való hozzáférést úgy kell biztosítani, hogy ezalatt az érintett más személy adatait ne ismerhesse meg.
(4) Az Intézet az érintetti jogokat az érintett számára közvetlen hozzáférést, helyesbítést vagy törlést biztosító elektronikus eszközzel is biztosíthatja.
(5) Az érintetti jogok gyakorlásának részletes feltételeit az adatkezelési nyilvántartás mellékletként tartalmazza.
(6) A minősített adat védelméről szóló 2009. évi CLV. törvény 12. § (1) bekezdése alapján a minősített adat kezelője a személyes adatok védelméről szóló törvény alapján az érintettet megillető tájékoztatást megtagadhatja, ha a minősítés alapjául szolgáló közérdeket az érintettnek a személyes adatainak kezelésére vonatkozó tájékoztatása veszélyeztetné.

Tájékoztatáshoz való jog
12.§ (1) Az érintett kérelmére az adatkezelő tájékoztatást ad az általa kezelt adatairól, azok céljáról, jogalapjáról, időtartamáról valamint arról, hogy kik és milyen célból kapják meg az

adatokat.
(2) Az adatkezelő köteles a tájékoztatást a kérelem benyújtásától számított legrövidebb időn, de legkésőbb 30 napon belül írásban, közérthető formában megadni.
(3) A tájékoztatás ellenében költségtérítés állapítható meg az Intézet térítési díj ellenében igénybe vehető egészségügyi szolgáltatásainak térítési szabályzata alapján. **13.§** (1) Az érintett tájékoztatását az adatkezelő csak az Info törvény 21. §-ában foglaltak esetében tagadhatja meg.

(2) Érintettet a megtagadás okáról tájékoztatni kell.
(3)Az elutasított kérelmekről az adatvédelmi tisztviselő nyilvántartást vezet.

Helyesbítéshez való jog
14.§ A valóságnak nem megfelelő adatot az adatkezelő köteles helyesbíteni.

Adatkezelés törléséhez, korlátozásához való jog
15.§ (1) A személyes adatot törölni kell, ha
a) a kezelése jogellenes,
b) az érintett kéri, kivéve, ha az adatkezelést jogszabály rendeli el,
c) az hiányos vagy téves – és ez az állapot jogszerűen nem korrigálható, feltéve, hogy a törlést törvény nem zárja ki,
d) az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben, meghatározott határideje lejárt,
e) azt a bíróság vagy a hatóság elrendelte.
(2) Törlés helyett az adatkezelő a személyes adatot az Info tv. 19.§-a szerint. (4) A helyesbítésről, zárolásról, a törlésről az érintettet, vagy azokat, akiknek korábban az adatot továbbították, tájékoztatni kell, kivéve, ha ez az érintett jogos érdekeit sérti.

Bírósági jogérvényesítés
16.§ (1) Az érintett jogainak megsértése esetén az adatkezelő ellen bírósághoz fordulhat. A bíróság az ügyben soron kívül jár el.
(2) Az adatkezelés a jogszabályban foglaltaknak megfelelőségét az adatkezelő köteles bizonyítani.
(3) A bírósági per körülményeire, a per következményeire vonatkozóan az Info tv. 23. §-a az irányadó.

Kártérítés és sérelemdíj
17.§ (1) Ha az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak kárt okoz, köteles azt megtéríteni. (2) Ha az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével az érintett személyiségi jogát megsérti, az érintett az adatkezelőtől sérelemdíjat követelhet.
(3) Az érintettel szemben az adatkezelő felel az adatfeldolgozó által okozott kárért és az adatkezelő köteles megfizetni az érintettnek az adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is. Az adatkezelő mentesül az okozott kárért való felelősség és a sérelemdíj megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső elháríthatatlan ok idézte elő.
Nem kell megtéríteni a kárt és nem követelhető a sérelemdíj annyiban, amennyiben a kár a károsult vagy a személyiségi jog megsértésével okozott jogsérelem az érintett szándékos vagy súlyosan gondatlan magatartásából származott

18.§ Az adatkezeléssel kapcsolatos jogainak megsértése esetén az érintett az adatvédelmi tisztviselőhöz fordulhat, aki felveszi a kapcsolatot az ügyben illetékes adatkezelő szervezeti egység vezetőjével.

V. fejezet
Adatközlések

19. § (1) A személyes adatok közlése belső adattovábbítás, harmadik személyhez történő adattovábbítás, külföldre történő adattovábbítás vagy nyilvánosságra hozatal formájában valósulhat meg.
(2) Adattovábbítás, ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik, ideértve az adatokba történő betekintés vagy kivonat készítés lehetővé tételét is. Nem minősül adattovábbításnak az Intézet, mint adatkezelő szervezeti rendszerén belüli adattovábbítás, az adatok adatfeldolgozó részére történő átadása, valamint az érintett saját személyes adataihoz való hozzáférése.
(3) Harmadik országba történő adattovábbítás az Európai Gazdasági Térség (továbbiakban: EGT) tagállamain kívüli országba történő adattovábbítás.
(4) Nyilvánosságra hozatal, ha az adatot bárki számára hozzáférhetővé teszik.

20.§ (1) Az Intézet a személyes adatokat bizalmasan kezeli. Adattovábbításra, harmadik országba vagy nemzetközi szervezet számára történő adattovábbításra, személyes adatok nyilvánosságra hozatalára csak jogszabályi kötelezettség teljesítése céljából kerülhet sor. (2) Az egyéb okból történő adattovábbításról, harmadik országba vagy nemzetközi szervezet számára történő adattovábbításról, személyes adatok nyilvánosságra hozataláról az adatvédelmi tisztviselővel történő konzultációt követően az orvosigazgató dönt.

Intézményen belüli adattovábbítás

21.§ (1) Az Intézet, mint adatkezelő szervezeti rendszerén belül az Intézet által kezelt személyes adatok – a feladat elvégzéséhez szükséges mértékben és ideig – továbbíthatók olyan szervezeti egységhez, amelynek a törvényben, intézeti szabályzatban vagy utasításban foglalt feladatainak ellátásához az adatra szüksége van (továbbiakban: belső adattovábbítás).
(2) Amennyiben az adatkezelő szervezeti egység és az adatokat megismerni kívánó szervezeti egység között az egymás közti továbbíthatósággal kapcsolatban vita merül fel, azt a főigazgató vagy az orvos igazgató dönti el az adatvédelmi tisztviselő véleményét is meghallgatva.

Adattovábbítás külső megkeresés alapján

22. § (1) Az Intézeten kívüli szervtől vagy magánszemélytől érkező, EGT-n belüli, az aktuális adatkezelési nyilvántartásban nem szereplő, újkeletű adattovábbításra irányuló megkeresés csak akkor teljesíthető, vagy személyes adat más célból akkor továbbítható, ha e szabályzat 6. § (1) bekezdésben foglalt valamely jogalap fennáll. A rendszeresen előforduló adattovábbításokat és azok lehetséges jogalapját, illetve az adattovábbítás egyéb körülményeit az adatkezelési nyilvántartásban rögzíteni kell.
(2) A hozzájáruláson alapuló adatkezelésekből történő adattovábbítás esetén a hozzájárulásnak kifejezetten az adattovábbításra is ki kell terjednie.
(3) Nem teljesíthető olyan adatigénylés, amelyeknek jogszerűsége – az adatigénylés vagy az adattovábbítás joglapjául szolgáló dokumentum, különösen az érintetti hozzájárulás hiányos adattartalmára, nem egyértelmű jellegére vagy más körülményre tekintettel – nem állapítható meg egyértelműen. Ennek megállapítása az adatvédelmi tisztviselő jogköre a főigazgató vagy az orvos igazgató előzetes tájékoztatásával.

(4) Az ilyen adattovábbításokra egyebekben a 6. § (2)-(6) bekezdései megfelelően alkalmazandók.
(5) A nemzetbiztonsági szolgálatok adatkérésre irányuló megkereséseiről az érintett szervezeti egység vezetője tájékoztatja az adatvédelmi tisztviselőt, egyúttal az Intézet főigazgatóját és az orvos igazgatóját. Az ilyen megkeresések teljesítésével kapcsolatban a főigazgató vagy az orvos igazgató nem halasztó hatályú állásfoglalást kérhet a fenntartó

szervtől.
(6) A nemzetbiztonsági szolgálatoktól érkező megkeresésre, adatbetekintésre vonatkozó adatokról – ideértve a megkeresés, betekintés tényét is –, és a megtett intézkedésekről az érintett vagy más személy, szervezet nem tájékoztatható.

23.§ (1) Az adattovábbítás körülményeit dokumentálni kell, amely tartalmazza legalább: a) az adatkezelést végző szervezeti egység nevét, az adatok forrásának megnevezését; b) az adattovábbítás címzettjét és elérhetőségeit;
c) az ügyintéző munkatárs(ak) nevét, beosztását,elérhetőségeit;
d) az adattovábbítás célját;
e) az adattovábbítás jogalapját;
f) az adattovábbítás időpontját;
g) az adattovábbítással érintett személyeket;
h) a továbbított adatok körét;
i) az adattovábbítás módszerét (manuális, elektronikus, vegyes);
(2) Az adattovábbítással kapcsolatos érintetti jogok gyakorlása érdekében az egyedi, nem rendszeresen végzett adattovábbításokról adattovábbítási nyilvántartást kell vezetni, amely tartalmazza az érintett nevét, az azonosításához szükséges adatait, az adattovábbítás időpontját és a címzett szervezet megnevezését. A nyilvántartás vezetését az egyes szervezeti egységek vezetőitől kapott információk alapján az adatvédelmi tisztviselő végzi.

Harmadik országba vagy nemzetközi szervezet részére történő adattovábbítás

24.§ (1) A harmadik országba vagy nemzetközi szervezet részére történő adattovábbításokra kizárólag a Rendelet V. fejezetében foglalt rendelkezéseknek megfelelően kerülhet sor. (2) Az adatkezelő szervezeti egység a harmadik országba tervezett adattovábbítás előtt konzultál az adatvédelmi tisztviselővel az adattovábbítás jogszerű feltételeinek fennállásáról.

VI. fejezet
Adatbiztonsági rendszabályok

25.§ (1) Az Intézet megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása céljából, hogy az Intézet az adatok megfelelő szintű biztonságát garantálja, ideértve különösen a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását, ellenálló képességét, valamint egy incidens esetén a személyes adatokhoz való hozzáférés és az adatok rendelkezésre állásának kellő időben való visszaállítását.
(2) A konkrét adatbiztonsági intézkedéseket az Intézet a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembe vételével választja meg.

(3) A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

Manuális kezelésű adatok

27.§ (1) A manuális kezelésű (nem elektronikus, jellemzően papír alapú) személyes adatok biztonsága érdekében az alábbi intézkedéseket kell foganatosítani.

a) *Tűz- és vagyonvédelem:* Az irattári kezelésbe vett iratokat zárható, száraz, az iratok állagának megóvására alkalmas helyiségben kell elhelyezni.

b) *Hozzáférés-védelem:* A folyamatos aktív kezelésben lévő iratokhoz csak az illetékes ügyintézők férhetnek hozzá. Az intézetben ápolt betegek kezelésével kapcsolatos iratokat, a személyzeti valamint a bér- és munkaügyi iratokat zárható helyiségben és zárható lemezszekrényben, az egyéb személyes adatokat pedig legalább zárható helyiségben kell őrizni.
c) *Archiválás:* Az archiválást az Intézet iratkezelési szabályzatának, valamint az irattári tervnek megfelelően kell végrehajtani.
(2) Az adatokat keletkezésükkor megfelelő minőségű adathordozóra kell rögzíteni. (3) Az adatok olvashatóságáért az azokat felvevő, illetve rögzítő személy felel. (4) Az adatokat az ellátás időtartama alatt rendezett, visszakereshető formában, zárható körülmények között, illetve megfelelő felügyelet mellett kell tárolni.
(5) Az adatok visszakereshetőségét olyan megoldással kell biztosítani, hogy az ellátáshoz szükséges optimális időn belül, illetve egyéni igény esetén elfogadható határidővel megvalósítható legyen.
(6) A Szabályzat előírásainak megfelelő adatkezelést szükség szerinti rendszerességgel az adatvédelmi tisztviselő ellenőrzi, és arról jegyzőkönyvet vesz fel. Az ellenőrzés eredményéről az intézet vezetőjét és az orvos igazgatót tájékoztatni kell.
(7) Személyes adatokat tartalmazó adathordozó kezelésében csak az intézettel munkavégzésre irányuló jogviszonyban álló dolgozó vehet részt.
(8) Azokban a helyiségekben, amelyekben személyes adatok kezelése történik, csak az alábbi személyek tartózkodhatnak:
a) munkavégzés vagy oktatás, tanulás céljából jelen lévő személy,
b) az érintett vagy törvényes képviselője, valamint az érintett által írásban felhatalmazott személyek.
(10) A közös terekben történő kényszer tárolás esetében a tárolók zárhatóságát és a zárás tényét az adatvédelmi tisztviselő köteles rendszeresen ellenőrizni. Mindemellett törekedni kell arra, hogy ilyen helyiségekben dokumentáció ne kerüljön tárolásra.

Elektronikus eszközökkel kezelt személyes adatok

29.§ (1) Az elektronikus eszközökkel kezelt személyes adatok adatbiztonságára vonatkozó részletes szabályokat – ideértve az adatbiztonsági intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást – az Intézet Informatikai Biztonsági Szabályzata állapítja meg.
(2) Elektronikusan tárolt adatok esetében adatot csak az informatikai csoport által nyilvántartott

hozzáférési listára felvett, nyilvántartott adatkezelő kezelhet. Az adatkezelőnek egyéni, titkos jelszóval kell bejelentkeznie a rendszerbe. Az adatkezelés befejeztével a rendszerből ki kell lépni. A rendszerbe történt, jelszóval védett adatkezelésért az adatkezelő felel. Az esetleges visszaélések elkerülése érdekében az adatkezelő kötelessége, hogy egyéni jelszava titkosságát biztosítsa.
(3) A rendszer fejlesztése az adatkezelés aktuális adatait tároló és működtető egységeitől elkülönítetten történhet. A fejlesztés során a fejlesztő köteles együttműködni az informatikai csoportvezetővel és az adatvédelmi tisztviselővel is az adatvédelmet érintő kérdésekben. (4) Hálózati rendszerek esetén a szervereket önálló gépteremben kell elhelyezni. A tűzvédelemi szempontok miatt a gépteremben a dohányzás tilos. A teremben a burkolatnak nehezen éghetőnek kell lenni. A gépterem ajtaja nem éghető anyagú legyen. A gépteremben tűzvédelmi riasztóberendezést kell felszerelni. A megfelelő hőmérsékletet klímaberendezéssel kell biztosítani. A vízkár elleni védekezésül a potenciálisan veszélyeztetett helyiségek esetén a gépteremben a számítógépeket minimálisan 1 m padlózat feletti magasságban kell elhelyezni. A gépterem számítástechnikai eszközeinek áramellátása szünetmentes áramforrással legyen biztosított. Tartós áramhiány esetén tartalék áramforrást kell biztosítani. Túlfeszültség ellen a gépterem áramellátását galvanikusan el kell különíteni részhálózattá. Bármilyen *nem* informatikai karbantartás vagy szerelés a gépteremben csak az adatvédelmi tisztviselő engedélyével történhet. A takarítószemélyzetet a takarítás során követendő speciális eljárásokra ki kell oktatni. Az oktatás az informatikai vezető feladata.

(5) Jogosulatlan tartózkodás elleni védelem: A gépteremben csak az informatikai csoport vezetője, közvetlen felettese(i), az adatvédelmi tisztviselő, vagy az ezek által felhatalmazott személy tartózkodhatnak. A géptermet riasztóberendezéssel kell ellátni. (6) Hálózati elemek védelme: A számítógépes hálózaton kezelőszervvel ellátott részegység csak megfelelő fizikai védelemmel (zártan) helyezhető el. A közüzemi hálózaton történő karbantartás vagy szerelés esetén különös gondot kell fordítani a számítógépes hálózat vezetékének épségére. Az informatikai csoportnak rendelkeznie kell a számítógépes hálózat vázlati rajzával, és azt a szerelést, karbantartást végző külső vállalkozók számára a szerelés, karbantartás idejére át kell adni.
(7) Munkaállomások védelme: A munkaállomásokat, különösen az adatok saját adathordozón történő tárolása esetén az eltulajdonítás ellen fizikai eszközökkel is védeni kell (a helységekben folyamatos személyes jelenlétet kell biztosítani, ennek hiányában azokat zárva kell tartani).

Az adatvédelmi incidensek eljárásrendje

30.§ (1) 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 adatokhoz való jogosulatlan hozzáférést eredményez.
(2) Amennyiben az Intézet bármely munkatársa adatvédelmi incidens gyanúját észleli, vagy az adatfeldolgozótól adatvédelmi incidensre vonatkozó jelzést kap, haladéktalanul értesíti az adatkezelő szervezeti egység vezetőjét, aki közvetlenül az adatvédelmi tisztviselőt tájékoztatja. Az adatvédelmi tisztviselő dönt arról, hogy az esemény adatvédelmi incidensnek minősül-e, majd incidens esetén haladéktalanul rögzíti annak körülményeit, így különösen: (2)az incidens jellegét, és – amennyiben lehetséges – az érintettek körét és (becsült) számát, valamint az érintett személyes adatok körét;
(3)az incidensből eredő valószínűsíthető következményeket;
(4)az incidens orvoslására adott szervezeti egységnél tett vagy tervezett, vagy más szervezeti

egységek számára javasolt intézkedéseket, különösen azokat, amelyek az esetleges hátrányos következmények enyhítését célozzák;
(5)azon intézkedéseket, amelyeket adott esetben az érintett megtehet az esetleges hátrányos következmények enyhítése érdekében.
(6) Az intézet vezetője az adatvédelmi tisztviselővel közösen egyeztetve javaslatot tesz az incidens súlyának besorolására, amely lehet jelentéktelen, valószínűsíthetően kockázattal járó vagy valószínűsíthetően magas kockázattal járó incidens.
(7) Az adatvédelmi tisztviselő dönt az incidens súlyának megfelelő további intézkedésekről, szükség esetén további tájékoztatást kérhet azon szervezeti egységtől, amely az incidenssel kapcsolatban várhatóan további információkkal rendelkezik. A megkeresett szervezeti egység 24 órán belül köteles a rendelkezésre álló információközlésére.
(8) Amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatvédelmi tisztviselő az intézet főigazgatójának jóváhagyása alapján – az incidens észlelésétől számított 72 órán belül – a vonatkozó jogszabályi rendelkezéseknek megfelelően – értesíti a felügyeleti hatóságot.
(9) Amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, vagy az incidens hátrányos következményeinek enyhítésére az érintett közreműködése szükséges, és nem állnak fenn a vonatkozó jogszabályi kivételek, az adatvédelmi tisztviselő haladéktalanul javaslatot tesz az adatkezelő szervezeti egység vezetőjének, hogy tájékoztassa az érintettet az adatvédelmi incidensről. A szerv vezetője – amennyiben a javaslattal egyetért – haladéktalanul tájékoztatja az érintettet. A tájékoztatás tartalmazza legalább
a) az incidens jellegét, és az érintett személyes adatok körét;
b) az adatvédelmi tisztviselő, egészségügyi adatok érintettsége esetén az egészségügyi adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó kapcsolattartó nevét és elérhetőségeit;
(10) Az adatvédelmi tisztviselő valamennyi adatvédelmi incidensről nyilvántartást vezet az

alábbi adattartalommal:

a) az incidensben érintett személyes adatok köre és száma,
b) incidenssel érintettek köre és száma,
c) incidensről tudomásszerzés időpontja,
d) incidens körülményei, hatásai,
e) elhárítás céljából tett intézkedések,
f) incidenssel kapcsolatban adott tájékoztatások adatai.

(11) Az adatkezelő szervezeti egységek indokolt esetben, továbbá az adatvédelmi tisztviselő jelzése alapján intézkedési tervet készítenek az adatvédelmi incidensek számának és súlyának csökkentése érdekében.

VII. fejezet
Az adatvédelem ellenőrzési rendszere

Az adatkezelő szervezeti egységek feladatai

31.§ (1) Az adatvédelemmel kapcsolatos jogszabályi előírások és intézeti szabályzatok, így különösen jelen szabályzat rendelkezéseinek betartását az adatkezelő szervezeti egységek vezetői – vezetői ellenőrzésük részeként – folyamatosan ellenőrzik.
(2) A szervezeti egység vezetők szabálysértés észlelése esetén haladéktalanul intézkednek annak megszüntetéséről, továbbá különösen indokolt esetben az illetékes munkáltatói jogkör

gyakorlójánál az érintett dolgozó felelősségre vonását kezdeményezhetik. (3) A személyes adatok kezelésével, feldolgozásával vagy szabályozásával kapcsolatos kérdésekben bármely szervezeti egység vezetője szükség esetén az adatvédelmi tisztviselőhöz fordulhat.
(4) Bármely olyan érintett, akinek a személyes adatai kezelése e szabályzat hatálya alá tartozik közvetlenül is fordulhat az adatvédelmi tisztviselőhöz személyes adatai kezelésével kapcsolatos panaszával. A panaszt az adatvédelmi tisztviselő kivizsgálja, a vizsgálat eredményéről értesíti az érintettet, és indokolt esetben kezdeményezi az adatkezelő szervezeti egységnél a szükséges intézkedések megtételét.

Az adatvédelmi tisztviselő jogállása és feladatai

32.§ (1) A főigazgató az adatkezeléssel kapcsolatos jogszabályi és szabályzati előírások teljesítése és az érintettek jogainak érvényesítése érdekében adatvédelmi tisztviselőt nevez ki vagy bíz meg. Az adatvédelmi tisztviselő feladatkörével az bízható meg, aki kellő rátermettséggel bír, illetve a személyes adatok védelmére vonatkozó jogi előírások megfelelő szintű ismeretével rendelkezik. Ugyanazon személy megbízási idejének lejártát követően újra megbízható.
(2) Az adatvédelmi tisztviselő más feladatokat is elláthat, feltéve, hogy e feladatai nem összeférhetetlenek. Összeférhetetlen különösen az olyan feladatkör, amely adatkezeléssel kapcsolatos döntéseket is magában foglal (pl. adatkezelő szervezeti egység vezetőjének feladatköre).
(3) Az adatvédelmi tisztviselő közvetlenül és kizárólag a főigazgatónak alárendelten, szakmailag függetlenül látja el feladatait, konkrét utasításokat nem fogadhat el. Az adatvédelmi tisztviselő megbízatása – a kinevezésének időtartamán belül – feladatai ellátásával összefüggésben felmerülő okból nem vonható vissza, az adatvédelmi tisztviselő nem bocsátható el, valamint szankcióval nem sújtható, kivéve, ha olyan magatartást tanúsít, amely alapján az általános munkajogi szabályok szerint azonnali hatályú felmondásnak lenne helye.
(4) Az adatvédelmi tisztviselő munkáját segítik az adatkezelési megbízottak. (5) Tevékenységéért az adatvédelmi tisztviselőt havi rendszeres díjazás illeti meg. Az Intézet gondoskodik az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükséges forrásokról.

33.§ (1) **Az adatvédelmi tisztviselő**
a) tájékoztatást és szakmai tanácsot ad az adatvédelmi rendelkezések szerinti

kötelezettségekkel kapcsolatban, ennek keretében konkrét ügyben állásfoglalást vagy általános kérdésekben ajánlást készít;
b) az általa megállapított rendben, időközönként és területeken ellenőrzi az adatvédelmi rendelkezéseknek (jogszabályoknak és intézeti szabályzatoknak) való megfelelést; c) igény szerint közreműködik az adatkezelési műveletekben részt vevő munkatársak tudatosság-növelésében és képzésében, valamint a személyes adatokat is érintő belső vizsgálatokban (auditokban);
d) kérésre közreműködik az adatkezelési nyilvántartás elkészítésében és felülvizsgálatában, valamint biztosítja, hogy nyilvántartás nála is elérhető legyen;
e) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
f) együttműködik az adatvédelmi felügyeleti hatósággal; és az adatkezeléssel összefüggő

ügyekben kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele;
g) elősegíti az érintettet megillető jogok gyakorlását, így különösen megvizsgálja az érintettek panaszait és – szükség esetén – kezdeményezi az orvosláshoz szükséges intézkedések megtételét;
h) közreműködik az intézeti adatvédelmi szabályzat, valamint más szabályzatok személyes adatokat érintő rendelkezéseinek megalkotásában, módosításában.

(2) Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.
(3) Az Intézet biztosítja, hogy az adatvédelmi tisztviselő a feladataihoz kapcsolódó ügyekbe megfelelő módon és időben bekapcsolódjon, ideértve az ilyen ügyeket érintő megbeszéléseken való részvételi lehetőség biztosítását is. Az adatvédelmi tisztviselő – feladatai ellátása érdekében
– az Intézet valamennyi szervezeti egységénél jogosult beletekinteni az adatkezelésekbe valamint a hozzájuk kapcsolódó bármely iratba. Az egység vezetőjétől és munkatársaitól szóban vagy írásban felvilágosítást kérhet. A tájékoztatás valóságtartalmáért a tájékoztatást adó felelősséggel tartozik. A vizsgálata során megismert személyes adatokkal kapcsolatban az adatvédelmi tisztviselőt – a jogviszonya fennállása alatt és annak megszűnését követően is – titoktartási kötelezettség terheli.
(4) Az adatvédelmi szabályok megsértése, jogsértés vagy a szabályzatok megsértésének veszélye vagy más, a személyes adatokat érintő visszásság esetén az adatvédelmi tisztviselő javaslatot tesz a jogsértés vagy a szabályok megsértésének megszüntetése, elkerülésére vagy a visszásság orvoslására. Az adatvédelmi tisztviselő tájékoztatja a kialakult helyzetről az Intézet vezetőségét, valamint segítséget nyújt a törvényes állapot helyreállításához.

2. rész
Egészségügyi adatvédelmi szabályok

I. fejezet
Értelmező rendelkezések és alapelvek

34.§ (1) Ezen rész személyi hatálya kiterjed:
a) minden egészségügyi ellátást nyújtó szervezeti egységre, szakmai felügyeletet, ellenőrzést végző szervezetre és természetes személyre, és egyéb adatkezelő szervre, amely, vagy aki egészségügyi és személyes adatot kezel,
b) minden, az egészségügyi ellátóhálózattal, valamint az egyéb adatkezelő szervvel kapcsolatba került vagy kerülő, illetve annak szolgáltatásait igénybe vevő természetes személyre (a továbbiakban: érintett),
c) az adatkezeléssel kapcsolatba került vagy kerülő külső szolgáltatóra, amely a Intézet feladatkörébe tartozó személyes adatot kezel, vagy azzal kapcsolatba kerül, (2) Ezen rész tárgyi

hatálya kiterjed:

a) minden, az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (a továbbiakban: Eüak.tv.) előírásai szerint kezelt, az érintettre vonatkozó egészségügyi és személyazonosító adatra,

b) a Balatonfüredi Állami Szívkórházban az a) pontban foglaltakon felül kezelt valamennyi egészségügyi és személyes adatra.

35.§ Értelmező rendelkezések:

a) érintett: minden, az adatkezelő szervvel kapcsolatba került vagy kerülő, illetve annak szolgáltatásait igénybe vevő természetes személy, függetlenül attól, hogy beteg-e, vagy egészséges.

b) adattovábbítás: ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik.

c) adathordozó: minden olyan anyag vagy eszköz, amely adatok lejegyzésére, tárolására és visszaolvasására alkalmas.

d) adatkezelő: A betegellátó, az intézményvezető, a betegjogi képviselőket foglalkoztató szerv; az egészségügyi dokumentációt kezelő szerv; továbbá közegészségügyi-járványügyi közérdekből az Eüak.tv. 5. § (3) bekezdésében meghatározott szervek és személyek; továbbá a 22. § szerinti esetekben az ott meghatározottak szerint az egészségbiztosítási szerv; a 22/E. §-ban meghatározottak szerint az orvosszakértői, rehabilitációs, illetve szociális szakértői szerv, rehabilitációs hatóság; a Nyugdíjbiztosítási Alap kezeléséért felelős nyugdíjbiztosítási szerv és a nyugdíjbiztosítási igazgatási szerv; továbbá a 16/A. §-ban meghatározottak szerint, valamint a lakossági célzott szűrővizsgálatok szervezése érdekében a 3. § b) pont szerinti személyazonosító adat tekintetében az egészségügyi államigazgatási szerv; a 14/A. §-ban meghatározott adatok tekintetében a gyógyszer, gyógyászati segédeszköz, gyógyászati ellátás kiszolgáltatója, illetve nyújtója; a 15/A. §-ban meghatározottak szerint a munkavédelmi hatóság és a munkahigiénés és foglalkozás-egészségügyi szerv; továbbá a 23. § (1) bekezdés f) pontjában meghatározott esetben az első- és másodfokú etikai eljárást lefolytató kamarai szerv;

e) adatfeldolgozó: az a természetes vagy jogi személy, jogi személyiséggel nem rendelkező szervezet, aki, vagy amely az adatkezelő megbízásából – beleértve a jogszabály rendelkezése alapján történő megbízást is – a személyes adatok feldolgozását végzi.

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

g) egészségügyi ellátóhálózat: egészségügyi ellátást nyújtó, valamint szakmai felügyeletét, ellenőrzését végző szervezet és természetes személy

h) gyógykezelés: minden olyan tevékenység, amely az egészség megőrzésére, továbbá a megbetegedések megelőzése, korai felismerése, megállapítása, gyógyítása, a megbetegedés következtében kialakult állapotromlás szinten tartása vagy javítása céljából az érintett közvetlen vizsgálatára, kezelésére, ápolására, orvosi rehabilitációjára, illetve mindezek érdekében az érintett vizsgálati anyagainak feldolgozására irányul, ideértve a gyógyszerek, gyógyászati segédeszközök gyógyfürdőellátások kiszolgálását, a mentést és betegszállítást, valamint a szülészeti ellátást is.

i) orvosi titok: a gyógykezelés során az adatkezelő tudomására jutott egészségügyi és személyazonosító adat, továbbá a szükséges vagy folyamatban lévő, illetve befejezett gyógykezelésre vonatkozó, valamint a gyógykezeléssel kapcsolatban megismert egyéb adat. j) egészségügyi dokumentáció: a gyógykezelés során a betegellátó tudomására jutott egészségügyi és személyazonosító adatokat tartalmazó feljegyzés, nyilvántartás vagy bármilyen más módon rögzített adat, függetlenül annak hordozójától vagy formájától. k) közeli hozzátartozó: a házastárs, az egyenes ágbeli rokon, az örökbe fogadott, a mostoha és nevelt gyermek, az örökbe fogadó, a mostoha- és nevelőszülő, valamint a testvér és az élettárs. l) sürgős szükség: az egészségi állapotában hirtelen bekövetkezett olyan változás, amelynek következtében azonnali egészségügyi ellátás hiányában az érintett közvetlen életveszélybe kerülne, illetve súlyos vagy maradandó egészségkárosodást szenvedne.

m) egészségügyi dolgozó: az orvos, a fogorvos, a gyógyszerész, az egyéb felsőfokú egészségügyi

szakképesítéssel rendelkező személy, az egészségügyi szakképesítéssel rendelkező személy, továbbá az egészségügyi tevékenységben közreműködő egészségügyi szakképesítéssel nem rendelkező személy.
n) betegellátó: a kezelést végző orvos, az egészségügyi szakdolgozó, az érintett gyógykezelésével kapcsolatos tevékenységet végző egyéb személy, a gyógyszerész.

Az egészségügyi adatkezelés célja

36.§ (1) Az egészségügyi és személyazonosító adatok a következő célok elérése érdekében kezelhetők:
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, közegészségügyi és járványügyi érdekből szükségessé váló intézkedések megtétele,
e) a betegjogok érvényesítése céljából.
(2) Az (1) bekezdésben felsoroltakon kívül törvényben meghatározott esetekben a következő célokból lehet egészségügyi és személyazonosító adatot kezelni:
a) egészségügyi szakember-képzés,
b) orvos-szakmai és epidemiológiai vizsgálat, elemzés, az egészségügyi ellátás tervezése, szervezése, költségek tervezése,
c) statisztikai vizsgálat,
d) tudományos kutatás,
e) az egészségügyi adatot kezelő szerv vagy személy hatósági vagy törvényességi ellenőrzését, szakmai vagy törvényességi felügyeletét végző szervezetek munkájának elősegítése, ha az ellenőrzés célja más módon nem érhető el, valamint az egészségügyi ellátásokat finanszírozó szervezetek feladatainak ellátása,
f) a társadalombiztosítási, illetve szociális ellátások megállapítása, amennyiben az az egészségi állapot alapján történik,
g) az egészségügyi ellátásokra jogosultak részére a kötelező egészségbiztosítás terhére igénybe vehető szolgáltatások rendelésének és nyújtásának, valamint a gazdaságos gyógyszer-, gyógyászati segédeszköz- és gyógyászati ellátás rendelési szabályai betartásának a vizsgálata, továbbá a külön jogszabály szerinti szerződés alapján a jogosultak részére nyújtott ellátások finanszírozása, illetve az ártámogatás elszámolása,
h) bűnüldözés,továbbá a rendőrségről szóló 1994. évi XXXIV. törvényben meghatározott feladatok ellátására kapott felhatalmazás körében bűnmegelőzés,
i) a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben meghatározott feladatok ellátása, az abban kapott felhatalmazás körében,
j) közigazgatási eljárás,
k) szabálysértési eljárás,
l) ügyészségi eljárás,
m) bírósági eljárás,
n) az érintettnek nem egészségügyi intézményben történő elhelyezése, gondozása, o) a munkavégzésre való alkalmasság megállapítása függetlenül attól, hogy ezen tevékenység munkaviszony, közalkalmazotti és közszolgálati jogviszony, hivatásos szolgálati viszony vagy

egyéb jogviszony keretében történik,
p) közoktatás, felsőoktatás és szakképzés céljából az oktatásra, illetve képzésre való alkalmasság megállapítása,
q) a katonai szolgálatra, illetve a személyes honvédelmi kötelezettség teljesítésére való alkalmasság megállapítása,
r) munkanélküli ellátás, foglalkoztatás elősegítése, valamint az ezzel összefüggő ellenőrzés. s) az egészségügyi ellátásokra jogosultak részére vényen rendelt gyógyszer, gyógyászati

segédeszköz és gyógyászati ellátás folyamatos és biztonságos kiszolgáltatása, illetve nyújtása érdekében,
t) a munkabalesetek, foglalkozási megbetegedések - ideértve a fokozott expozíciós eseteket is - kivizsgálása, nyilvántartása és a szükséges munkavédelmi intézkedések megtétele, u) az egészségügyi dolgozókkal szemben lefolytatott etikai eljárás,
v) eredményesség alapú támogatásban részesülő gyógyszerek, gyógyászati segédeszközök eredményességének, támogatásának megállapítása, és ezen gyógyszerekkel kezelt kórképek finanszírozási eljárásrendjének alkotása,
w) betegút-szervezés.
x) az egészségügyi szolgáltatások minőségének értékelése és fejlesztése, az egészségügyi szolgáltatások értékelési szempontjainak rendszeres felülvizsgálata és fejlesztése, y) az egészségügyi rendszer teljesítményének ellenőrzése, mérése és értékelése, z) az egészségügyi ellátásokra jogosult részére a hatásos és biztonságos gyógyszerelés elősegítése, valamint a költséghatékony gyógyszeres terápia kialakítása érdekében, zs) az Európai Unión belüli határon átnyúló egészségügyi ellátáshoz kapcsolódó jogok érvényesítése.
(3) Az (1) és a (2) bekezdésben meghatározott céloktól eltérő célokra akkor lehet egészségügyi és személyazonosító adatot kezelni, ha a megfelelő tájékoztatást követően az érintett, illetve törvényes vagy meghatalmazott képviselője (a továbbiakban együtt: törvényes képviselő) ehhez írásban határozottan hozzájárul.
(4) Az (1)-(2) bekezdések szerinti adatkezelési célokra csak annyi és olyan egészségügyi, illetve személyazonosító adat kezelhető, amely az adatkezelési cél megvalósításához elengedhetetlenül szükséges.

Az érintettek jogai és a jogok érvényesítése

Lásd 11.-18.§

II. fejezet
Az egészségügyi ellátóhálózat szerveinek adatkezelése

Adatfelvétel

37.§ (1) Az adatfelvétel során az egészségügyi dokumentációban rögzíteni kell az adatfelvétel időpontját és az adatfelvevő személyét.
(2) A beteg dokumentációjában történt minden feljegyzést, beírást aláírással vagy kézjeggyel, és ha szükséges, dátummal kell hitelesíteni, illetve elektronikus adatkezelés esetén a bejegyzést végző egyértelmű azonosítását a rendszernek biztosítania kell.
(3) A dolgozók aláírás mintáját nyilvántartásban kell rögzíteni. A nyilvántartás vezetéséért az

adott szervezeti egységen belül az ezzel a feladattal megbízott dolgozó felel (adatkezelési megbízott). Elektronikus adatkezelés esetén az adatkezelő bejelentkező nevének és jelszavának titkosan történő kezelése az adatkezelő kötelezettsége.

Adatmódosítás

38.§ Ha tévesztés, vagy más ok miatt a beírt adatot módosítani kell, ez csak úgy végezhető, hogy az eredeti adat megállapítható legyen. A módosítást kézjeggyel el kell látni, illetve elektronikus adatkezelés esetén a bejegyzést végző egyértelmű azonosítását és a bejegyzés naplózását a rendszernek biztosítania kell.

Adattörlés

39.§ Adatot törölni csak ezen szabályzatban rögzítettek szerint lehet. A törlés során be kell tartani az adatvédelmi előírásokat. A törlés során a manuálisan kezelt adatokat fizikailag meg kell semmisíteni, elektronikusan tárolt adatok esetében azokat helyrehozhatatlanul meg kell változtatni. Az érintettet a törlés következményeiről és veszélyeiről a törlés előtt tájékoztatni kell, és ezt az érintettel aláíratva a beteg dokumentációjában a kérelemmel együtt meg kell őrizni. A törlést az adatvédelmi tisztviselő és az orvos igazgató együttes engedélyével lehet elvégezni, illetve ezekről az esetekről az adatvédelmi tisztviselő nyilvántartást vezet. Amennyiben az egészségügyi dokumentációnak tudományos jelentősége van, a kötelező nyilvántartási időt követően át kell adni a Semmelweis Orvostörténeti Múzeum, Könyvtár és Levéltár részére.

III. fejezet
Az adatkezelés egyes esetei
Gyógykezelés céljából történő adatkezelés

40.§ Az egészségügyi adatok felvétele a gyógykezelés része. Az egészségügyi és a személy azonosító adatoknak a gyógykezelt személy (törvényes képviselője) részéről történő szolgáltatása – az egészségügyi ellátás igénybevételéhez kötelezően előírt személyazonosító adatok megadása jogszabályi kötelezettség.

41.§ A gyógykezelés alatt az egészségügyi dokumentációban rögzíteni kell a szakmai szabályoknak megfelelő adatokat. A kezelést végző orvos dönti el az adattakarékosság elvét is figyelembe véve, hogy a szakmai szabályoknak megfelelően – a kötelezően felveendő adatokon kívül – mely egészségügyi adat felvétele szükséges.

42.§ Kerülni kell azon adatok rögzítését, amelyek közvetlenül nem kapcsolatosak a beteg gyógykezelésével. Ezen adatok felvételére a kórlapba csak akkor kerülhet sor, ha azok a beteg gyógykezelésében szerepet játszanak.

43.§ A gyógykezelés során az egészségügyi dokumentáció kezelésének rendjét úgy kell kialakítani, hogy a dokumentációhoz, illetve a beteg személyes adataihoz kizárólag a gyógykezelt személy gyógykezelését végzők férhessenek hozzá.

44.§ A lázlapok nem tarthatók a betegágy végén vagy másutt a kórteremben, illetve szabadon hozzáférhetően nem tárolhatók, kivéve a vizit idejét. A betegek nevét nem lehet a kórtermek ajtajánál kifüggeszteni. A kórlapokat nem lehet a nővérpulton vagy másutt úgy tárolni, hogy a személyazonosító adatok a helyiségben tartózkodók, a beteg ellátásában részt nem vevők által hozzáférhetők legyenek. A fekvőbetegek neve helyett azonosításukra alkalmas vonalkód (törzsszám, azonosítószám) szerepel az ellátás ideje alatt használt karszalagokon.

Orvosi titok védelme

45.§ (1) A betegellátót, valamint a kórházzal közalkalmazotti jogviszonyban álló más személyt a beteg egészségi állapotával kapcsolatos adat, továbbá a munkavégzéssel kapcsolatosan tudomására jutott egyéb adat vonatkozásában időbeli korlátozás nélkül titoktartási kötelezettség terheli, függetlenül attól, hogy az adatokat milyen módon ismerte meg. A titoktartási kötelezettség az intézmény minden dolgozóját terheli.
(2) A betegellátót – a gyógykezelt személy választott háziorvosa, valamint az igazságügyi orvosszakértő kivételével - a titoktartási kötelezettség azzal a betegellátóval szemben is köti, aki a beteg gyógykezelésében nem működött közre, kivéve, ha az adatok a gyógykezelt személy további gyógykezelése érdekében szükségesek
(3) A titoktartási kötelezettség alól írásban felmentést adhat a beteg, vagy törvényen alapuló adatszolgáltatási kötelezettség.
(4) Az orvosi titok védelme érdekében szükséges, hogy az intézmény valamennyi dolgozója kötelezettséget vállaljon az orvosi titok megtartására. A kötelezettséget a dolgozó munkaköri leírásába kell foglalni, illetve ahhoz csatolni kell.

Gyógykezelés során jelen lévő személyek

46.§ (1) A gyógykezelés során a kezelést végző orvos és a betegellátásban részt vevő más személyek lehetnek jelen, valamint az, akinek jelenlétéhez a beteg hozzájárult. (2) A beteg emberi jogainak és méltóságának tiszteletben tartása mellett az érintett hozzájárulása nélkül jelen lehet a gyógykezelés során:
a) más személy, ha a gyógykezelés rendje több beteg egyidejű ellátását igényli, b) a rendőrség hivatásos állományú tagja, amennyiben a gyógykezelésre fogvatartott személy esetében kerül sor,

c) a büntetés-végrehajtási szervezet szolgálati jogviszonyban álló tagja, amennyiben a gyógykezelésre olyan személy esetében kerül sor, aki a büntetés-végrehajtási intézetben szabadságelvonással járó büntetését tölti, és a gyógykezelést végző betegellátó biztonsága, illetve szökés megakadályozása céljából erre szükség van,
d) a b)-c) pontok szerinti személyek, ha bűnüldözési érdekből a beteg személyi biztonsága ezt indokolttá teszi, azonban nyilatkozattételre képtelen állapotban van.
(3) Ezen túlmenően jelen lehet az,
a) aki a beteget az adott betegség miatt már kezelte,
b) akinek az intézet igazgatója és az adatvédelmi tisztviselő szakmai-tudományos ok miatt engedélyt adott. A gyógykezelt személy kifejezett tiltakozásának ebben az esetben helyt kell adni.
(4) Az egészségügyi szakemberképzés céljából jelen lehet: orvos, orvostanhallgató, egészségügyi szakdolgozó, egészségügyi főiskola vagy szakiskola hallgatója, feltéve, hogy a megjelölt személy képzésére kijelölt intézmény az Intézet. Ebben az esetben a gyógykezelt személy hozzájárulására nincs szükség, de a betegtájékoztatóban az intézet oktató jellegéről és a szakemberképzésről a gyógykezelteket tájékoztatni kell.
(5) A hozzájárulást a gyógykezelt személy szóban is megadhatja a kezelést végző orvosnak, de törekedni kell az írásbeliségre a további nézeteltérések elkerülése miatt.

Adattovábbítás a háziorvos részére

47. § (1) A kezelést végző orvos az általa megállapított, a betegre vonatkozó adatokat – amennyiben a beteg ezt írásban nem tiltotta meg – továbbítja a beteg háziorvosának. A tiltás lehetőségéről, annak következményeiről a beteget a kezelés megkezdése előtt tájékoztatni kell
(2) Az érintett háziorvosa és a kezelését végző orvos - ha az érintett ezt írásban nem tiltotta meg - jogosult az érintett által a kötelező egészségbiztosítás terhére igénybevett egészségügyi ellátás adatairól tudomást szerezni úgy, hogy az adatokat az egészségbiztosítási szerv elektronikus lekérdezés formájában biztosítja számára. A háziorvos a hozzá bejelentkezett biztosított adatait ismerheti meg. Az érintettet a kezelést végző orvos írásban vagy szóban tájékoztatja a tiltakozás lehetőségéről. Az érintett a tiltakozását az egészségbiztosítási szerv részére elektronikus úton

(EESZT), személyesen vagy postai úton juttatja el.

Tájékozódási, tájékoztatási jog és kötelezettség
A beteg joga a tájékoztatáshoz

48.§ (1) A betegellátás megkezdése előtt a beteget tájékoztatni kell az intézet adatvédelmi rendjéről. A beteg tájékoztatása az adatvédelemről a felvevő kötelessége. A tájékoztatás megadását a beteg aláírásával igazolja. Az aláírt tájékoztatót a beteg egészségügyi dokumentációjához csatolni kell. A beteg dokumentációjához csatolni kell a beteg esetleges korlátozó nyilatkozatát is.
(2) A gyógykezelt személy gyógykezelésével kapcsolatos tájékoztatást a beteg kezelését végző orvos vagy a betegellátó osztály vezetője adja meg. A beteg gyógykezelésének ápolási vonatkozásairól az őt ellátó diplomás ápoló is felvilágosítást adhat. Szakdolgozó, illetve más dolgozó a beteg gyógykezeléséről tájékoztatást nem adhat, kivéve, ha a beteg kezelését végző orvos erre az adott beteg esetében felhatalmazta. A tájékoztatás személyesen történik.
(3) Telefonon a beteg gyógykezeléséről érdemi tájékoztatás nem adható, kivéve a beteg által előzetesen megjelölt személyek számára, a beteg előzetesen meghatározott adatainak bemondását követően.

Hozzátartozó és más személy tájékoztatása

49.§ (1) A beteg az intézménybe történt felvételkor vagy kezelése alatt rendelkezhet arról, hogy betegségéről, annak várható kimeneteléről, egészségi állapotának változásáról mely személyeknek adható részleges vagy teljes felvilágosítás, illetve ebből kik zárandók ki. A beteget a rendelkezés lehetőségéről tájékoztatni kell, illetve az erre szolgáló nyilatkozat formanyomtatványokat rendelkezésre bocsátani.
(2) Az intézetben fekvő betegek állapotáról csak orvos, kezelőorvos adhat tájékoztatást az arra jogosult személy számára. Telefonon történő érdeklődés esetén az orvos azonosító kódot kér a hozzátartozótól (beteg születési dátuma), és csak ezt követően kezdheti meg a tájékoztatást.

Az egészségügyi dokumentáció megismerésének joga

50.§ (1) A beteg (törvényes képviselője) jogosult tájékoztatást kapni a rá vonatkozó személyazonosító és egészségügyi adatokról, betekinthet az egészségügyi dokumentációba, illetve azokról saját költségére másolatot kérhet. Ennek díját a hatályos Térítési díj ellenében igénybe vehető egészségügyi szolgáltatások jegyzéke c. szabályzat tartalmazza. A dokumentum első kiadott példánya díjmentes.
(2) Fekvőbeteg gyógyintézetből történő elbocsátáskor a beteg jogosult térítésmentesen zárójelentést kapni. A dokumentum első kiadott példánya díjmentes.
(3) Egészségügyi adatairól indokolt célra – saját költségére – jogosult összefoglaló vagy kivonatos írásos véleményt kapni. Ennek díját az intézet Térítési díj ellenében igénybe vehető egészségügyi szolgáltatások jegyzéke c. szabályzat tartalmazza. A dokumentum első kiadott példánya díjmentes. Elektronikus formában kiadott adatigénylés díjmentes.
(4) A beteg élhet azon jogával, hogy az (1) bekezdés szerinti jogát más személy számára megengedje, vagy megtiltsa. A tiltás érvényesítésétől csak gondozása érdekében közeli hozzátartozó vagy a gondozásra köteles személy kérésére lehet eltekinteni. (5) A felhatalmazást a gyógykezelés ideje alatt írásban lehet megtenni, azon kívül csak teljes bizonyító erejű magánokirat formájában.
(6) Megkezdett, de még be nem fejezett ellátás esetén a tájékoztatást az adott ellátással kapcsolatban a kezelést végző orvos adja meg. Folyamatban lévő ellátás esetén a beteg a dokumentációról másolatot saját költségére kaphat a betegellátást végző dolgozó által. A dokumentum első kiadott példánya díjmentes.

51. § (1) A gyógykezelt személy halála esetén a halál okával összefüggésbe hozható, továbbá a halál bekövetkeztét megelőző gyógykezeléssel kapcsolatos adatokat megismerheti az elhunyt
a) törvényes képviselője,

b) Ptk. szerinti közeli hozzátartozója,
c) örököse, a jogcím hiteles igazolása után.
(2) A megjelölt személyek a fenti adatokról – saját költségükre – másolatot kaphatnak. A másolat kiadása az orvos igazgató engedélyével és az intézet adatvédelmi tisztviselőjének jóváhagyásával történhet, melyről az utóbbi nyilvántartást vezet.

Közegészségügyi, járványügyi célból történő adatkezelés

52.§ (1) A betegellátó haladéktalanul továbbítja az egészségügyi államigazgatási szervnek az

egészségügyi és személyazonosító adatot, ha a jogszabály szerinti fertőző betegséget észlel, vagy annak gyanúja merül fel.
(2) Egyes fertőző betegségek előfordulása esetén a betegellátó személyazonosító adatok nélkül csak az egészségügyi adatokat jelentheti az egészségügyi államigazgatási szervnek. egészségügyi államigazgatási szerv közegészségügyi vagy járványügyi közérdekre hivatkozva - az anonim szűrővizsgálat keretében vizsgált HIV fertőzött és AIDS beteg kivételével- kérheti az érintett személyazonosító adatait.
(3) Egyes mikrobiológiai laboratóriumi vizsgálati eredménnyel igazolt betegségek, illetve kórokozóik előfordulását valószínűsíti vagy igazolja, a mikrobiológiai vizsgálatot végző betegellátó az egészségügyi adatokat személyazonosításra alkalmatlan módon jelenti az egészségügyi államigazgatási szervnek.
(4) A betegellátó az (1), (2) és (3) bekezdésben meghatározott, továbbá közegészségügyi, járványügyi esetekben az Eüak.tv. 15.§ (1)-(9) bekezdésekben meghatározottak szerint jár el.

53. § (1) Az észlelő orvos köteles haladéktalanul továbbítani a munkavédelmi hatóságnak a munkavállaló egészségügyi és személyazonosító adatát, ha
a) jogszabály szerinti foglalkozási eredetű megbetegedést észlel vagy annak gyanúja merül fel, b) az érintett foglalkozása gyakorlása közben, azzal összefüggésben
ba) jogszabályban felsorolt egészségkárosító hatású anyag hatásának van kitéve, és szervezetében az anyag koncentrációja a megengedett mértéket meghaladja, valamint bb) zaj esetében a 4000 Hz-en 30 dB bármely fülön bekövetkező halláscsökkenés fordul elő. (2) A betegellátó az (1) bekezdésben meghatározott esetekben az Eüak.tv. 15/A.§(2)-(3) bekezdésekben meghatározottak szerint jár el.

Egészségügyi szakemberképzés

54.§ A gyógykezelés során szakemberképzés céljából – tekintettel arra, hogy a Balatonfüredi Állami Szívkórház oktató tevékenységet is folytató intézmény – jelen lehet az érintett hozzájárulása nélkül is orvos, vagy orvostanhallgató.

Népegészségügyi célból történő adatkezelés

55.§ (1) Daganatos eredetű betegség észlelése esetén a betegellátó továbbítja az érintett egészségügyi és személyazonosító adatait a külön jogszabály szerint vezetett Nemzeti Rákregiszternek.
(2) A betegellátó szívinfarktussal diagnosztizált betegség észlelése esetén továbbítja az érintett személyazonosító és a szívinfarktus megbetegedésre vonatkozó egészségügyi a miniszteri rendeletben meghatározott Nemzeti Szívinfarktus Regiszter részére.
(3) A lakossági célzott szűrővizsgálatok, a népegészségügyi szűrővizsgálatok, valamint a népegészségügyi szűrővizsgálatok körébe is tartozó szűrést végző egészségügyi szolgáltatók szűrővizsgálatai eredményeinek értékelése, monitorozása a feladat ellátásához szükséges mértékben és ideig az egészségügyi államigazgatási szerv értékeléssel, monitorozással megbízott munkatársa kezelheti a szűrővizsgálaton részt vevő személyek egészségügyi és személyazonosító adatait.
(4) A betegellátó népegészségügyi célból történő adatkezelések során az Eüak.tv. 16.§ (1)-

(12), a 16/A§ (2)-(3) és a 16/B§ (3)-(5) bekezdésekben meghatározottak szerint jár el.

Epidemiológiai vizsgálatok, elemzések, az egészségügyi ellátás tervezése, szervezése, minőség-, és teljesítményértékelés

56. § (1) A szakmai minőségértékelésért felelős szerv a jelen szabályzat 36.§ (2) bekezdés x) pontja szerinti célból - ide nem értve az (5) bekezdésben meghatározott eljárást - jogosult az egészségügyi szolgáltatások minőségének értékeléséhez és fejlesztéséhez, az egészségügyi szolgáltatások értékelési szempontjainak rendszeres felülvizsgálatához és fejlesztéséhez szükséges egészségügyi adatok, valamint - más személyazonosító adattal történő összekapcsolás nélkül - az ahhoz kapcsolódó TAJ szám, nem, születési dátum és postai irányítószám kezelésére. Az egészségügyi ellátóhálózat, illetve az egészségbiztosítási szerv a szakmai minőségértékelésért felelős szerv megkeresésére átadja ezen adatokat a szakmai minőségértékelésért felelős szerv részére, illetve gondoskodik az adatokhoz történő hozzáférésről.
(2)A betegellátó a szakmai minőségértékelési célból történő adatkezelések során az Eüak.tv. 18.§ (1)-(5) bekezdésekben meghatározottak szerint jár el.

57. § A teljesítményértékelésért felelős szerv jelen szabályzat 36. § (2) bekezdés y) pontja szerinti célból kezelheti az érintett egészségügyi adatait, valamint az érintett TAJ számát, nemét, születési dátumát és postai irányítószámát az adatok átadása, az adatkezelés és a kapcsolati kód képzése tekintetében az Eüak.tv. 18. § (1)-(4) bekezdésében foglaltak szerint.

58. § Az országos szervek és intézetek, a térségi betegút-szervezésért felelős szerv, továbbá az egészségügyi államigazgatási szerv - saját szakterületén, a feladata ellátásához szükséges ideig és mértékben - kezelheti az érintett egészségügyi adatait, valamint - más személyazonosító adattal történő összekapcsolás nélkül - az érintett TAJ-számát, nemét, életkorát és postai irányítószámát.

Statisztikai célú adatkezelés

59.§ (1) Az egészségügyi adatok statisztikai célra személyazonosításra alkalmatlan módon korlátlanul kezelhetők, személyazonosításra alkalmas módon csak az érintett írásos hozzájárulásával.
(2) Az egészségügyi ellátó hálózat a statisztikáról szóló törvényben meghatározott adatgyűjtéssel kapcsolatos feladatai teljesítése céljából kezeli a népmozgalmi adatszolgáltatás körébe tartozó adatokat.

60.§ A statisztikai célra felvett, átvett vagy feldolgozott személyes adatok csak statisztikai célra használhatók fel. A külön törvény szerinti egyedi statisztikai adatok – beleértve a személyes adatokat is – a statisztikai céltól eltérő célra semmilyen módon vagy jogcímen nem adhatók és vehetők át, nem dolgozhatók fel, és nem hozhatók nyilvánosságra.

Tudományos kutatás céljából történő adatkezelés

61.§ (1) Tudományos kutatás céljából kutatási kérelem alapján a tárolt adatokba be lehet tekinteni. A kutatási kérelemben meg kell határozni a megismerni kívánt adatok körét, a kutatás célját. A kutatásra az engedélyt az orvosigazgató az adatvédelmi tisztviselő ellenjegyzésével adja meg. A kutatási kérelmek engedélyezéséről és elutasításáról az adatvédelmi tisztviselő nyilvántartást vezet.

(2) A kutatási kérelmekről és a megadott engedély alapján adatokhoz hozzájutott személyekről nyilvántartást kell vezetni, melyet 10 évig meg kell őrizni.
(3) Tudományos közleményben nem szerepelhetnek egészségügyi és személyazonosító adatok

oly módon, hogy a gyógykezelt személy személyazonossága megállapítható legyen. Tudományos kutatás során a tárolt adatokról nem készíthető személyazonosító adatokat is tartalmazó másolat.
(4) A kutatási kérelem megtagadását írásban meg kell indokolni. A kérelmező a megtagadás esetén bírósághoz fordulhat. E tekintetben az Info tv. szabályai az irányadóak. (5) A kölcsönzés, jóváhagyás és a folyamat dokumentálásának további szabályait a Felvételi iroda működéséről szóló szabályzata rögzíti.

62.§ (1) Tudományos kutatás céljára felvett vagy tárolt személyes adat csak tudományos kutatás céljára használható fel.
(2) A személyes adatot – mihelyt a kutatási cél megengedi – anonimizálni kell. Addig is külön kell tárolni azokat az adatokat, amelyek meghatározott, vagy meghatározható természetes személy azonosítására alkalmasak. Ezek az adatok egyéb adatokkal csak akkor kapcsolhatók össze, ha az kutatás céljára szükséges.
(3) A tudományos kutatást végző szerv vagy személy személyes adatot csak akkor hozhat nyilvánosságra, ha az érintett abba beleegyezett.
63.§ Klinikai vizsgálatok esetén közös adatfeldolgozás történik, ahol az érintett a kapcsolódó adatkezeléshez hozzájáruló nyilatkozatát a gyógyszer kipróbálási vizsgálat szponzora felé teszi meg, míg a kórház a beteg (érintett) személyes adatait változatlanul jogszabályi kötelezettség alapján kezeli.

Társadalombiztosítási igazgatási szervek adatkezelése

64.§ (1) A társadalombiztosítási igazgatási szervek részére abban az esetben továbbítható egészségügyi és személyazonosító adat, amennyiben
a) arra az érintettnek járó társadalombiztosítási ellátások megállapítása, folyósítása céljából van szükség, és az az egészségi állapot alapján történik, valamint
b) az a társadalombiztosítási alapok kezelői gazdálkodásának, továbbá a társadalombiztosítási ellátások folyósításának ellenőrzése céljából indokolt, c) jelen szabályzat 36. § (2) g) pontja szerinti cél teljesítéséhez szükséges. (2) A betegellátó a társadalombiztosítási igazgatási szervek részére történő adattovábbítások során az Eüak.tv. 22 és 22/A.§-ban meghatározottak szerint jár el.

Központi implantátumregiszter

65. § (1) Az egészségügyről szóló 1997. évi CLIV. törvény 101/C. § (1) bekezdése szerinti adatokat tartalmazó nyilvántartás adatainak az implantátum beültetésével, kivételével és cseréjével kapcsolatos beavatkozáson átesett érintett további gyógykezelése, egészségi állapotának nyomon követése, váratlan esemény gyors elhárítása, valamint a beültethető orvostechnikai eszközök megfelelőségének ellenőrzése céljából vezetett központi implantátumregiszter részére történő továbbítását követően a központi implantátumregisztert működtető egészségbiztosítási szerv a személyazonosító adatok tekintetében kapcsolati kódot képez. A kapcsolati kódot az egészségbiztosítási szerv minden személyazonosító adat tekintetében azonos kódképzési módszer alapján hozza létre úgy, hogy az a személyes adatokra történő visszafejtést ne tegye lehetővé és ugyanazon beteg tekintetében valamennyi adattovábbítás -

függetlenül a beavatkozást végző egészségügyi szolgáltatótól - azonos kapcsolati kódhoz kapcsolódjon.
(2) A betegellátó a központi implantátumregiszterrel kapcsolatban az Eüak.tv. 22/B.§-ban meghatározottak szerint jár el.

Az orvosszakértői, rehabilitációs, illetve szociális szakértő szerv, rehabilitációs hatóság adatkezelése

66. § (1) Az orvosszakértői, rehabilitációs, illetve szociális szakértői szerv, rehabilitációs hatóság, továbbá az igazságügyi szakértő részére az egészségbiztosítási szerv abban az esetben továbbít

egészségügyi és személyazonosító adatokat, amennyiben arra az érintettnek járó társadalombiztosítási vagy szociális ellátásra, kedvezményre való jogosultsága egészségi állapota alapján történő megállapításához, illetve ellenőrzéséhez szükséges tevékenységének, szakértői tevékenységének ellátása céljából van szükség. Az orvosszakértői, rehabilitációs, illetve szociális szakértői szerv, rehabilitációs hatóság, az igazságügyi szakértő az egészségbiztosítási szervnél rendelkezésre nem álló adatok továbbítása érdekében megkeresheti a kezelőorvost. A megkeresésére és a kezelőorvos adatátadási kötelezettségére az Eüak.tv. 23. § (1) és (2) bekezdésében foglaltakat értelemszerűen alkalmazni kell.
(2) A betegellátó az orvosszakértői, rehabilitációs, illetve szociális szakértői szerv, rehabilitációs hatóság részére történő adattovábbítások során az Eüak.tv. 22/E.§-ban meghatározottak szerint jár el.

Adattovábbítás az egészségügyi ellátóhálózaton kívüli szerv

megkeresésére A továbbítás hatályossága

67.§ (1) A személyazonosításra alkalmatlan egészségügyi adat időbeli és területi korlát nélkül továbbítható.
(2) Az alábbi szervek részére írásbeli megkeresés alapján a kezelést végző orvos átadja az érintett egészségügyi és személyes adatait:
a) büntetőügyben a nyomozó hatóság, az ügyészség, a bíróság, az igazságügyi szakértő, polgári peres és nem peres valamint közigazgatási hatósági ügyben a közigazgatási hatóság az ügyészség, a bíróság, az igazságügyi orvos szakértő,
b) szabálysértési eljárás során az eljárást lefolytató szervek,
c) potenciális hadköteles és hadköteles személy esetén a fővárosi és megyei kormányhivatal járási hivatala, a Magyar Honvédség katonai igazgatási és központi adatfeldolgozó szerve, valamint a katonai egészségügyi alkalmasságot megállapító bizottság,
d) a nemzetbiztonsági szolgálatok, a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben meghatározott feladatok ellátása érdekében, az abban kapott felhatalmazás körében.
e) a Magyar Honvédség katonai igazgatási és központi adatfeldolgozó szerve, a kiképzett tartalékosok békeidőszakban történő hadi beosztásra történő kiírása és a kiképzett tartalékosok gyors és differenciált behívása érdekében, a honvédelemről és a Magyar Honvédségről szóló törvényben meghatározott körben,
f) az egészségügyi dolgozóval szemben folyamatban lévő etikai eljárás során az eljárás lefolytatása hatáskörrel és illetékességgel rendelkező kamarai szerv,
g) a rendőrségről szóló törvényben meghatározott belső bűnmegelőzési és bűnfelderítési

feladatokat ellátó, valamint a terrorizmust elhárító szervek a törvényben meghatározott feladatok ellátása érdekében, az abban kapott felhatalmazás körében.
h) halottvizsgálat során a halottvizsgálatot végző orvos.
i) a légi-, a vasúti és a víziközlekedési balesetek és egyéb közlekedési események szakmai vizsgálatáról szóló törvényben, valamint a polgári légiközlekedési balesetek és repülőesemények vizsgálatáról és megelőzéséről és a 94/56/EK irányelv hatályon kívül helyezéséről szóló, 2010. október 20-i 996/2010/EU európai parlamenti és tanácsi rendeletben meghatározott szakmai vizsgálat során a közlekedésbiztonsági szerv.
(3) A kezelést végző orvos a nyomozó hatóságot a „halaszthatatlan intézkedés” jelzéssel ellátott, külön jogszabályban előírt ügyészi jóváhagyást nélkülöző megkeresésére is köteles tájékoztatni az általa kezelt, az adott üggyel összefüggő egészségügyi és személyazonosító adatokról. (4) Ha az egészségügyi adatokra a halottvizsgálat során soron kívül van szükség, a) büntetőügyben a nyomozó hatóság, valamint az ügyészség halaszthatatlan nyomozási cselekmény keretében,
b) a rendkívüli halállal kapcsolatos hatósági eljárás során a bűncselekményre utaló adat kizárása érdekében az eljáró hatóság az (1) bekezdés szerinti megkeresést rövid úton is előterjesztheti, a kezelőorvos a megkeresést soron kívül teljesíti.

(3) A megkeresésnek tartalmaznia kell az adatkezelés célját, és meg kell jelölni az adatok körét. Csak annyi és olyan adat továbbítható, mely az adatkezelési cél megvalósulásához el engedhetetlenül szükséges.
(4) A (3) bekezdésen kívüli esetekben az egészségügyi és ahhoz kapcsolódó személyes adat csak törvény alapján, vagy az érintett hozzájárulásával továbbítható.
(5) A betegellátó az egészségügyi ellátóhálózaton kívüli szerv megkeresésére történő adattovábbítások során az Eüak.tv. 23.§-ban és a 23/A.§-ban meghatározottak szerint jár el.

Bűncselekményből eredő sérülés esetén

68.§ (1) A kezelést végző orvos a gyógykezelt személy első ellátása során a rendőrségnek haladéktalanul bejelenti a gyógykezelt személy személyes adatait, ha a gyógykezelt személy 8 napon túl gyógyuló sérülést szenvedett, és a sérülés feltehetően bűncselekmény következménye.
(2) Kiskorú érintett első ízben történő ellátása esetén, amennyiben feltételezhető, hogy sérülése vagy betegsége bántalmazás, vagy elhanyagolás következménye, illetve az ellátás során erre utaló körülményekről szerez tudomást, a kezelést végző orvos köteles értesíteni az illetékes gyermekjóléti szolgálatot.
(3) A bejelentéshez a gyógykezelt személy hozzájárulása nem szükséges. A bejelentés az első ellátó orvos által történik, telefonon. A jelentés tényét az egészségügyi dokumentációban rögzíteni kell.

Közigazgatási eljárás, intézményi elhelyezés

69.§ Egészségügyi és személyazonosító adatot közigazgatási eljárás, illetve az érintettnek intézményi elhelyezése, gondozása céljából csak akkor lehet továbbítani, ha arra az érintett jogai érvényesítéséhez vagy kötelezettségei teljesítéséhez van szükség.

Adattovábbítás más személy érintettsége esetén

70.§ (1) Amennyiben az érintett egészségügyi adatai más személyt is érintenek, az egészségügyi és személyazonosító adatok továbbításához e harmadik személy (törvényes képviselője) írásbeli hozzájárulását be kell szerezni. Nincs szükség a hozzájárulásra az Eüak.tv. 13. § (fertőző betegség, szűrő és alkalmassági vizsgálatok, mérgezés, foglalkozási eredetű megbetegedés, gyermek gyógykezelése, bűnüldözés, bűnmegelőzés, nemzetbiztonság), 20. § (3) bekezdése (élve születés és halálozás) és 24. § (1)–(3) bekezdés (az érintett első ízben történő orvosi ellátásakor, ha az érintett 8 napon túl gyógyuló sérülést szenvedett és a sérülés feltehetően bűncselekmény következménye) szerinti esetekben azzal, hogy polgári peres eljárás során a harmadik személyt érintő szexuális úton terjedő fertőző betegségre vonatkozó egészségügyi adat nem adható ki.

Egészségügyi és személyazonosító adatok nyilvántartása

71.§ (1) Az érintettről felvett, a gyógykezelés érdekében szükséges egészségügyi és személyazonosító adatot, valamint azok továbbítását nyilván kell tartani. Mivel ez a kórház alaptevékenységéhez elengedhetetlen, mindennapos feladat, az intézeti adatnyilvántartásban foglaltan tároljuk.

72.§ (1) A betegellátó osztály/részleg nyilvántartja:
a) azokat az érintetteket, akikről bebizonyosodott, vagy valószínűsíthető, hogy fertőző betegségben szenvednek. Ezzel összefüggésben nyilván kell tartani a megelőző gyógyszeres kezelésre, a szűrővizsgálatra, járványügyi megfigyelésre, járványügyi zárlatra kötelezett

személyeket.
b) a védőoltásra kötelezett személyeket,
c) kábítószert élvező, kóros mértékben gyógyszert fogyasztó, egyéb, függőséget okozó anyagot használó személyeket.
(2) Az (1) bekezdés c) pontja szerinti személyek esetében a személyazonosító és egészségügyi adatokat elkülönítetten kell tárolni.

Az egészségügyi dokumentáció tárolásának és archiválásának rendje

73.§ (1) A beteg vizsgálatával és gyógykezelésével kapcsolatos adatokat az egészségügyi dokumentáció tartalmazza. Az egészségügyi dokumentációt úgy kell vezetni, hogy az a valóságnak megfelelően tükrözze az ellátás folyamatát.
(2) Az egészségügyi dokumentációban fel kell tüntetni
a) a beteg személyazonosító adatait,
b) cselekvőképes beteg esetén az értesítendő személy, kiskorú, illetve gondnokság alatt álló beteg esetében a törvényes képviselő nevét, lakcímét, elérhetőségét,
c) a kórelőzményt, a kórtörténetet,
d) az első vizsgálat eredményét,
e) a diagnózist és a gyógykezelési tervet megalapozó vizsgálati eredményeket, a vizsgálatok elvégzésének időpontját,
f) az ellátást indokoló betegség megnevezését, a kialakulásának alapjául szolgáló betegséget, a kísérőbetegségeket és szövődményeket,
g) egyéb, az ellátást közvetlenül nem indokoló betegség, illetve a kockázati tényezők

megnevezését,
h) az elvégzett beavatkozások idejét és azok eredményét,
i) a gyógyszeres és egyéb terápiát, annak eredményét,
j) a beteg gyógyszer-túlérzékenységére vonatkozó adatokat,
k) a bejegyzést tévő egészségügyi dolgozó nevét és a bejegyzés időpontját, l) a betegnek, illetőleg tájékoztatásra jogosult más személynek nyújtott tájékoztatás tartalmának rögzítését,
m) a beleegyezés, illetve visszautasítás tényét, valamint ezek időpontját, n) minden olyan egyéb adatot és tényt, amely a beteg gyógyulására befolyással lehet. (3) Az egészségügyi dokumentáció részeként meg kell őrizni:
a) az egyes vizsgálatokról készült leleteket,
b) a gyógykezelés és a konzílium során keletkezett iratokat,
c) az ápolási dokumentációt,
d) a képalkotó diagnosztikus eljárások felvételeit, valamint
e) a beteg testéből kivett szövetmintákat.
(4) Az egészségügyi dokumentáció esetében különös figyelmet kell fordítani arra, hogy az részletes, szakszerű, olvasható és visszakereshető legyen.

74.§ Az egészségügyi dokumentáció tárolását három szinten célszerű kialakítani: a) Napi tevékenységgel kapcsolatos dokumentumtárolás bent fekvő betegek esetében.

Helye: az osztályos vizsgáló helyiség.

Célja: a napi betegellátással és kapcsolódó tevékenységekkel összefüggő dokumentumok biztonságos és könnyen kezelhető tárolásának és hozzáférésének a biztosítása.

b) Közepes időtartamú archív tárolás rehabilitációs ellátás esetén általában az ápolás 22. napjától 48 hónapos időszakra.

Helye: a felvételi iroda által erre a célra kialakított átmeneti irattár.

Célja: a 48 hónapon belül távozott betegek papír alapú dokumentumainak visszakereséséhez biztonságos és könnyen kezelhető tárolás és hozzáférés, valamint a kivételek követhetőségének biztosítása.

c) Hosszú időtartamú archív tárolás.

Helye: az intézet különböző irattáraiban, kapacitásuk függvényében, az Eüak törvényben meghatározott időtartamig.

Az egészségügyi és személyes adatok megsemmisítése

75.§ (1) Az egészségügyi dokumentációt - a képalkotó diagnosztikai eljárással készült felvételek, az arról készített leletek kivételével az adatfelvételtől számított legalább 30 évig, a zárójelentést legalább 50 évig kell megőrizni. A kötelező nyilvántartási időt követően gyógykezelés vagy tudományos kutatás érdekében - amennyiben indokolt - az adatok továbbra is nyilvántarthatók. Ha a további nyilvántartás nem indokolt - a (3) bekezdés kivételével - a nyilvántartást meg kell semmisíteni.
(2) Képalkotó diagnosztikai eljárással készült felvételt az annak készítésétől számított 10 évig, valamint a felvételről készített leletet - a felvétel készítésétől számított 30 évig kell megőrizni.
(3) Amennyiben az egészségügyi dokumentációnak tudományos jelentősége van, a kötelező nyilvántartási időt követően át kell adni a Semmelweis Orvostörténeti Múzeum, Könyvtár és Levéltár részére.

(4) A meg nem semmisített, illetve a (3) bekezdés szerinti levéltárnak átadott egészségügyi dokumentációra e szabályzat előírásai értelemszerűen vonatkoznak.
(5) A gyógyszer, gyógyászati segédeszköz és gyógyászati ellátás kiszolgáltatója a vényeket 5 évig őrzi meg. A kötelező őrzési időt követően a vényeket meg kell semmisíteni. (6) Az adatmegőrzés érdekében folyamatosan biztosítani kell, hogy az adathordozó az adott technikai feltételek mellett olvasható maradjon, vagy olvasható állapotba kerüljön.

76.§ (1) A intézeti irattárban elhelyezett bármely iratot, dokumentációt (legyen az egészségügyi vagy gazdasági jellegű) csak iratselejtezés útján szabad az irattárból megsemmisítés céljából kiemelni.
A selejtezés részletszabályait az intézet Irat,- és dokumentumkezelési szabályzata tartalmazza.

Az egészségügyi adatvédelmi rendszer felépítése, szabályozása

77.§ (1) A Intézet az Info tv. és az Eüak.tv. rendelkezései alapján belső adatvédelmi rendszert alakít ki, és annak működését az alábbiakban határozza meg.

Az adatvédelmi szervezet felépítése

Az orvosigazgató

78. § Az orvos igazgató a főigazgatótól átruházott adatvédelmi feladatai körében: a) részt vesz az intézeti betegellátással kapcsolatos személyes adatok védelmében, felügyeli az egészségügyi adatok kezelésére vonatkozó szabályok betartását,
b) gondoskodik az egészségügyi adatkezelésre vonatkozó jogszabályok alapján az intézet adatvédelmi szabályzatának elkészítéséről és módosításáról,
c) részt vesz az egészségügyi adatok védelme érdekében megfelelő adatbiztonsági rendszer kidolgozásában,
d) együttműködik az adatvédelmi tisztviselővel,
e) ellenőrzi, jóváhagyja az adatvédelmi tisztviselő által az érintettek kéréseivel kapcsolatban benyújtott előterjesztéseket.

Az adatvédelmi tisztviselő

79.§ (1) Az adatvédelmi tisztviselő támogatja az intézet vezetőségét egészségügyi adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában. (2) *Az adatvédelmi tisztviselő feladatai az egészségügyi vonatkozású adatkezelésben:* a) Az intézet egészségügyi adatkezelésben résztvevő diagnosztikus,- járó,- és

fekvőbeteg osztályai adatvédelemért felelős dolgozóit tanácsokkal látja el, és munkájukat adatbiztonsági, adatvédelmi szempontok szerint koordinálja, ellenőrzi.
b) Felügyeli folyamatosan az intézetben folyó egészségügyi adatkezelési tevékenységet. c) Részt vesz a diagnosztikus,- járó,- és fekvőbeteg osztályok adatvédelemért felelős dolgozóinak adatvédelmi oktatásában.
d) Az orvos igazgatót tanácsokkal látja el az intézet adatvédelmi szabályzatának kidolgozásában, felülvizsgálatában.
e) Hatáskörén belül gondoskodik az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, és az egészségügyi és a hozzájuk

kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény előírásainak, valamint az intézet adatvédelmi szabályzatában foglaltaknak betartásáról. f) Tudományos kutatás esetén az orvos igazgatóval közösen engedélyezi az egészségügyi dokumentációba való betekintést, amelyről nyilvántartást vezet. A nyilvántartás megőrzési ideje 10 év.
g) Kezdeményezi az adatvédelem területén kifejlesztett új technológiák és eszközök alkalmazását.
h) Új adatkezelés esetén közreműködik annak az intézet adatkezelési nyilvántartásába való felvételéről.
i) Kivizsgálja a hozzá érkezett egészségügyi adatkezeléssel kapcsolatos bejelentéseket, és jogosulatlan, vagy szabálytalan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót.

A betegellátás adatvédelemért felelős dolgozói

80. § A kórházban minden fekvőbeteg osztályon ki kell jelölni egy dolgozót (adatkezelési megbízott), aki az egészségügyi adatkezelés felügyeletét ellátja. Ezt az osztályvezető javaslata alapján a dolgozó munkaköri leírásában kell rögzíteni.
Az ezzel járó feladatok:
a) Vezeti az egészségügyi dokumentációba bejegyzést tenni jogosultak aláírás minta nyilvántartását.
b) Az osztály dolgozóinak továbbképzést tart az adatvédelmi szabályzat végrehajtásáról. c) Az osztályvezetőnek javaslatot tesz az adatvédelmi szabályzat és általánosságban az adatvédelem betartása érdekében szükséges intézkedésekre. Észrevételeit továbbítja az adatvédelmi tisztviselőnek is, ha azok jelentősége megkívánja.
d) Osztályán folyamatosan ellenőrzi az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény, valamint az intézeti Adatvédelmi és adatkezelési szabályzat előírásainak érvényesülését, és gondoskodik azok betartásáról.
e) Adatvédelmi incidens, vagy adatkezelés során felmerült szabálytalanság esetén tudomásszerzését követően haladéktalanul tájékoztatja az adatvédelmi tisztviselőt. f) Tevékenységéről rendszeresen beszámol az adatvédelmi tisztviselőnek.

Az adatvédelmi képzés szabályozása

81.§ (1) A betegellátás adatvédelemért felelős dolgozóinak adatkezelési és adatvédelmi képzése az adatvédelmi tisztviselő feladata.
(2) Az új, belépő dolgozók általános adatvédelemmel kapcsolatos felkészítését az adatvédelmi tisztviselő végzi. Az egészségügyi adatkezelést is végző dolgozók egészségügy specifikus adatvédelmi oktatását az illetékes osztályok adatvédelemért felelős dolgozói végzik. Az oktatások megtörténtét és a szabályok tudomásul vételét írásban rögzíteni kell, melyet a munkaügyi osztály tárol a dolgozó munkaügyi iratai között.
(3) Jogszabályi változások esetén a változás jellegétől, terjedelmétől függően körlevél, vagy

szervezett tájékoztatás alkalmazandó. Ennek koordinálása, szervezése az adatvédelmi tisztviselő feladata.

Az adatvédelmi jelentési kötelezettség szabályozása

82.§ Az adatvédelmi tisztviselő éves beszámolójának leadási határideje tárgyévet követő január 15.
Példányszám: 4 db (1 db az főigazgatónak, 1 db az orvos igazgatónak küldendő, 1 db az irattárba helyezendő, 1 db az adatvédelmi tisztviselő saját példánya).

IV. fejezet
Különleges rendelkezések
Intézményi várólista

Adatkezelés

83.§ (1) Az intézményi várólista kezelését és vezetését az arra írásban kijelölt és feljogosított személy(ek) végezheti(k).
(2) A várólista nem nyilvános formája az adott egészségügyi ellátásra besorolt biztosítottak legfontosabb személyazonosító adatait (családi és utónév, anyja neve, nem, születési év, lakóhely, társadalombiztosítási azonosító jel) az ellátásra való jogosultság sorrendjét, és az ellátás igénybevételének várható időpontját tartalmazza. A biztosítottak egyéb adatait az egészségügyi dokumentáció tartalmazza. A várólistán szereplő adatokat és a biztosítottak egyéb adatait az egészségügyi és személyazonosító adatok kezelésére vonatkozó jogszabályokban meghatározott rendelkezések szerint kell kezelni.
(3) A biztosítottak várólistán történő azonosítása érdekében egyedi azonosítót kell meghatározni. Az egyedi azonosító nem tartalmazhat a biztosított egészségügyi és személyazonosító adataival összefüggő, továbbá a várólistára történő felvétel időpontjára vonatkozó adatot. Az egészségügyi szolgáltatónál az intézményi várólista kezelésével megbízott az egyedi azonosítót annak meghatározásakor, személyesen vagy kezelőorvosa útján zárt borítékban átadja a beteg számára.
(4) A várólista személyes adatokat is tartalmazó változatához való hozzáférés esetén biztosítani kell a jogosulatlan hozzáférés elleni teljes körű védelmet (jelszavas bejelentkezés, tűzfallal ellátott internet csatlakozás, adatbázisok védelme).
Az intézet által rögzített adatok alapján a beteg számára a részletes lista adataihoz való hozzáférést az egyedi azonosító birtokában a Nemzeti Egészségbiztosítási Alapkezelő biztosítja saját honlapján keresztül.

Tájékoztatás

84.§ Az egyedi azonosító tartalmára vonatkozó szabályokról a biztosítottat kezelőorvosa tájékoztatja. A kezelőorvosnak tájékoztatási kötelezettsége keretében fel kell világosítania a beteget az adott ellátás esetében létező várólistára való felkerülés lehetőségéről.

V. fejezet
Adatbiztonság

Adatok védelme

85.§ (1) Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket, és kialakítani azokat az eljárási szabályokat, amelyek az Információs önrendelkezési jogról és az információszabadságról szóló törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
(2) Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés valamint a véletlen megsemmisülés és sérülés ellen. A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak, illetőleg a távközlési vagy informatikai eszköz üzemeltetőjének, ha a személyes adatok továbbítása hálózaton, vagy egyéb informatikai eszköz útján történik.
(3) Minden adatkezeléssel foglalkozó személy munkája közben köteles az elvárható legnagyobb gondossággal eljárni az adatok hitelessége, megőrzése és az illetéktelen hozzáférés megakadályozása érdekében.
(4) Az adatok tárolása és továbbítása során az általános baleset- és tűzvédelmi előírásokat figyelembe kell venni.
(5) Továbbiakban jelen szabályzat 25 és 26.§-ban foglalt részletszabályok az

érvényesek. **Adatok jogosulatlan megismerése, adathordozók eltulajdonítása**

86.§ Manuálisan tárolt adatok esetében:
Az eltulajdonítás ellen az alábbi rendelkezések betartása minden dolgozó kiemelt feladata: a) az ellátás alatti, illetve az azzal kapcsolatos dokumentálást követően a betegdokumentációt el kell zárni, illetve olyan helyen kell tartani, ahol az egészségügyi dolgozók folyamatos jelenléte által a felügyelet biztosított,
b) a beteg szállítása, más intézményben történő vizsgálata során a betegdokumentációt személy szerint a vizsgálatért, vagy beavatkozásért felelős, vagy az átvételt intéző egészségügyi dolgozónak kell átadni. Az átvétel tényét az időpont megadásával az átvevő által aláírva a beteg dokumentációjában fel kell tüntetni, és az adatok helyességéről meg kell győződni, c) a betegdokumentációk megfelelő biztonságos tárolásának tárgyi feltételeit, az archiválás feltételeit a Intézet vezetésének biztosítania kell,
d) a beteggel kapcsolatos dokumentációk, adatok eltulajdonításának gyanúja esetén az észlelő értesíti az érintett osztály vezetőjét és az osztály adatvédelemért felelős dolgozóját, aki a probléma súlyosságától függően értesíti az adatvédelmi tisztviselőt,
e) az adattárolás megfelelőségét az adatvédelmi tisztviselő rendszeresen ellenőrzi.

87.§ (1) Az elektronikusan tárolt adatok esetében a központi szerverek védelme és az adatok archiválása során használt adathordozók védelme az Informatikai Biztonsági Szabályzatban meghatározott módon történik.

Az adatkezelő azonosítása

88.§ (1) A szervezeti egységekben az adatkezeléssel foglalkozó dolgozók aláírás mintáját nyilvántartásban kell rögzíteni. Ennek eredeti példányát az adott egység központi irodájában (pl. kezelők, titkárság stb.) kell elhelyezni, a másolatokat minden papíralapú dokumentumot kezelő helységekben. Elektronikus adatkezelés esetén az aláírást az elektronikus felhasználónév –jelszó páros helyettesíti. A nyilvántartás vezetéséért az informatikai csoportvezető,- míg a belépési jogosultság engedélyezéséért az érintett osztály vezetője felel. A jelszó titkosan történő kezeléséért, azzal történő bármilyen visszaélésért a jelszó tulajdonosa felel. Csak olyan elektronikus rendszert szabad alkalmazni, amely a jelszavak kezelését képes titkosan kezelni, beleértve ebbe a rendszergazdát is.
(2) Hagyományos adatkezelés esetén az adatkezelő, vagy módosító személy azonosítása az

aláírásnak a nyilvántartásban rögzített aláírás mintával való összevetésével történik. Elektronikus adatkezelés esetén a rendszernek naplóznia kell a beavatkozás tényét. (3) A munkaviszony alatti, adatkezelési jogosultsággal összefüggő változásokról a dolgozó közvetlen felettese haladéktalanul értesíti az adott osztály adatvédelemért felelős dolgozóját, aki tovább értesíti erről az adatvédelmi tisztviselőt és az informatikai vezetőt.

Eljárás az adatok sérülése esetén

89.§ (1) Az egészségügyi és személyes adatokat ért sérülés vagy megsemmisülés esetén a rendelkezésre álló egyéb adatforrásokból meg kell kísérelni a lehetséges mértékig a károsodott adatok pótlását. A sérült adat pótlásáért annak a szervezeti egységnek a vezetője felelős, ahol a sérülés bekövetkezett. A pótolt adatokon a pótlás tényét fel kell tüntetni. A pótlásról jegyzőkönyvet kell felvenni, amit a szervezeti egység vezetőjének kell hitelesítenie.
(2) Elektronikusan tárolt adatok esetén a mentési-archiválási eljárás során alkalmazott adathordozók adatait felhasználva kell az adatok helyreállítását végrehajtani.

90.§ A manuálisan kezelt adatok esetén
(1) A hagyományos adathordozók tárolásakor a fizikai védelem biztosításán túl a Balatonfüedi Állami Szívkórház általános iratkezelési szabályai szerint kell eljárni az adatok visszakereshetőségének érdekében.
(2) A következmények felszámolásakor lehetőségekhez mérten a visszaállítás érdekében minden lehetőt el kell követni, felhasználva a bármely egységben, vagy a betegnél fennmaradt hiteles dokumentumot.
(3) A visszaállítást és annak mértékét a lehetőségek felmérésével, indokolásával és mérlegelésével az egység adatvédelmi felelőse írásban rendeli el. Amennyiben a visszaállítás nem valósítható meg, arról az adatvédelmi tisztviselő írásos feljegyzést készít.
(4) A visszaállításról, amennyiben az méltányos és megoldható, a mulasztásért felelős köteles gondoskodni. A személyes felelősség megítélésében az irányadó és hatályos jogszabályokat kell alkalmazni. A személyes felelősség megállapítása az adatvédelmi tisztviselő írásbeli véleményének megkérése alapján a szervezeti egység vezetőjének hatáskörébe tartozik. A visszaállításról nyilvántartást kell vezetni.

Az adatkezelési rendszer sérülése, illetve károsodása esetére tervezett intézkedések

91.§ (1) Manuális adatkezelés esetén
a) a dokumentumokat a tároló hely sérülésének elhárítása idejéig szükség esetén biztonságos

helyre kell szállítani,
b) az adatok hozzáférésének biztonságát veszélyeztető állapot elhárítását azonnal meg kell kezdeni, az elhárítás idejére folyamatos felügyeletet kell biztosítani, vagy a dokumentumokat zárható helyre kell szállítani.
(2) Elektronikus adatkezelés esetén
a) hálózat esetén a központi egységeinek (szerverek) sérülésekor az adatfeldolgozóval kötött szerződésben foglalt feltételeknek megfelelően azokat helyettesíteni kell, b) a rendszer működésképtelensége alatt az adatokat manuális módszerekkel kell rögzíteni, és a helyreállítást követően azokat a rendszerbe pótlólag felvenni.

3. rész
Munkaügyi célú adatkezelés

Személyes adatok, iratok kezelésének adatvédelmi követelményei

A személyi iratok köre

92.§ (1) a személyi anyag iratai (továbbiakban: alapnyilvántartás) az egészségügyi szolgálati jogviszonyról szóló 2020. évi C. törvény 2. melléklete szerint.

A személyi iratok kezelése

93.§ A munkavállalóktól kizárólag olyan adatok kérhetők és tarthatók nyilván, valamint olyan munkaköri orvosi alkalmassági vizsgálatok végezhetők, amelyek munkaviszony létesítéséhez, fenntartásához és megszüntetéséhez, illetve a szociális-jóléti juttatások biztosításához szükségesek és a munkavállaló személyhez fűződő jogait nem sértik.
Szakszervezeti tagsággal összefüggő adatokat munkáltató kizárólag az érintett munkavállaló hozzájárulásával kezel, a tagdíjak közvetlen utalása céljából, a munkavállaló által igényelt időtartamig.

94.§ A személyi iratokat, ezen belül a személyi anyag iratait az iktató programban külön gyűjtőszámon kell iktatni. A papír alapú iratokat a munkaügyi szervezeti egységnél elhelyezett, zárható szekrényben kell tárolni. Elektronikusan nyilvántartott adatok intézeti kezelői egyéni felhasználó névvel és jelszóval férnek hozzá a nyilvántartó programokhoz.

95.§ A személyes adatok kezelési jogosultságát munkakörhöz kötötten rögzíti a munkáltató, az alábbiak szerint:

- munkaügyi- és bérosztályvezető
- bérügyintéző
- társadalombiztosítási ügyintéző

96.§ Személyi iratra csak olyan adat, megállapítás vezethető rá, amelynek
alapja: a) közokirat,
b) bírósági vagy más hatóság döntése,
c) jogszabályi rendelkezés,
d) a munkáltatói jogkör gyakorlójának írásbeli rendelkezése,

e) a dolgozó írásbeli nyilatkozata.

97.§ (1) Munkakör-, megüresedett álláshelyek betöltésére irányuló hirdetések megfogalmazása során a munkáltatót meg kell nevezni, nem lehet anonim tartalmú hirdetést feladni.
A kezelhető személyes adatok köre: a természetes személy neve, születési ideje, helye, anyja neve, lakcíme, képesítési adatok, szakmai tapasztalat, fénykép, telefonszám, e-mail cím, a jelentkezőről készített munkáltatói feljegyzés (ha van). Az eljárás során a személyes adatokat (önéletrajz) a munkáltatói jogkör gyakorlói, a munkaügyi osztályvezető, az érintett terület/osztály vezetője, valamint a munkaügyi feladatokat ellátó munkavállalók kezelik.

(2) A beérkezett önéletrajzokat a titkárság iktatás után továbbítja az interjúztatásban illetékes munkáltatói jogkör gyakorlójának, illetve egyéb vezetőnek is érintettsége esetén. A pályázati anyagokat kizárólag a bírálatban érintett személyek kaphatják kézhez, a dokumentumok ennél szélesebb körű terjesztése nem megengedett. Az önéletrajzok azon példányait, melyeken esetlegesen bírálati megjegyzések szerepelnek, a bírálatot követően meg kell semmisíteni.

(2) A sikertelen pályázati anyagokat a bírálatot követő 6 hónap elteltével automatikusan meg kell semmisíteni. Ennek felelőse a munkaügyi osztály vezetője. A pályázók figyelmét az álláshirdetésben fel kell hívni erre a körülményre, valamint írásban hozzájárulásukat kell kérni adataiknak a pályázat ideje+6 hónap időtartamig történő kezelésére. Amennyiben a pályázó elnyerte az állást, önéletrajza és egyéb személyi iratai a munkaügyi osztályvezetőhöz kerülnek további ügyintézésre, majd a munkavállaló munkaügyi dossziéjában való tárolásra.

(3) Álláspályázat kiírása nélkül érkezett önéletrajzok esetén a munkaügyi osztály vezetője

dönthet úgy, hogy:
a) érdemben nem foglalkozik vele, és megsemmisíti azt,
b) érdemben nem foglalkozik vele, és visszaküldi a feladónak,
c) érdemben foglalkozik vele, és továbbítja az iratot az illetékes munkáltatói jogkör gyakorlójához interjúztatás céljából.
Mindhárom eshetőség esetén a feladó tudtára kell hozni az önéletrajzában szereplő adatai további életútját.

98.§ Intézetünk az egyes vagyonnyilatkozat tételi kötelezettségekről szóló 2007. évi CLII. törvény hatálya alá esik, így az ott meghatározott munkavállalói körben vagyonnyilatkozatot kell tenni. A kiállított nyilatkozatok átvételét és őrzését a kórház a törvényben meghatározottak szerint végzi, és gondoskodik a nyilatkozatokban szereplő személyes adatok biztonságos tárolásáról. A nyilatkozatokat kizárólag papír alapon fogadja be az intézet. Az előírt megőrzési időt követően a vagyonnyilatkozatokat felbontás nélkül, jegyzőkönyv felvétele mellett megsemmisítjük. A megsemmisítésnél jelen vannak: munkaügyi osztályvezető, gazdasági igazgató, adatvédelmi tisztviselő.
Az őrzésért felelős gazdasági igazgató kizárólag a törvény 13.§ esetében ismerheti meg a nyilatkozat tartalmát.

99.§ A munkavégzésre irányuló jogviszony megszűnése után a közalkalmazott személyi iratait az irattárban kell elhelyezni. A személyi anyagot - a más közigazgatási szervnek átadottak kivételével - a jogviszony megszűnésétől számított 50 évig meg kell őrizni. Tárolásról és levéltárba helyezésről részletesen az Iratkezelési szabályzat rendelkezik.

100.§ (1) 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. Amennyiben jogszabály írja elő a vizsgálat elvégzését, akkor tájékoztatni kell a munkavállalókat a jogszabály címéről és a pontos jogszabályhelyről is.

(2) A munkaalkalmasságra, felkészültségre irányuló teszteket a munkáltató mind a munkaviszony létesítése előtt, mind pedig a munkaviszony fennállása alatt készíttethet a munkavállalókkal. A vizsgálat előtt részletesen tájékoztatni kell a munkavállalókat többek között arról, hogy az alkalmassági vizsgálat milyen készség, képesség felmérésére irányul, a vizsgálat milyen eszközzel, módszerrel történik.

(3) A munkaköri alkalmassági vizsgálat eredményét a vizsgált munkavállalók, illetve a vizsgálatot végző szakember ismerhetik meg. A munkáltató csak azt az információt kaphatja meg, hogy a vizsgált személy a munkára alkalmas-e vagy sem, illetve milyen feltételek biztosítandók ehhez. A vizsgálat részleteit, illetve annak teljes dokumentációját azonban a munkáltató nem ismerheti meg.
Munkaviszonnyal kapcsolatos, a munkafolyamatok hatékonyabb ellátása, megszervezése érdekében folytatott vizsgálatokkal kapcsolatos információkat a munkavállaló, az adott szervezeti egység vezetője, valamint a munkáltatói jogkör gyakorlására jogosult személyek ismerhetik meg.

Az alapnyilvántartás vezetésének adatvédelmi szabályai

101.§ Az alapnyilvántartást a munkaügyi osztályvezető vezeti.
102.§ Az adatfelvételi lap is személyi irat, amely a személyi anyag része, és az erre vonatkozó szabályok szerint bizalmasan kell kezelni.
103.§ A munkaügyi osztályvezető köteles biztosítani, hogy a dolgozó a róla nyilvántartott adatokba és iratokba korlátozás nélkül betekinthessen, azokról másolatot vagy kivonatot kaphasson.
A munkaügyi osztályvezető a dolgozó olyan adatait is kezelheti, amelyek átadására törvény a

munkavállalót nem kötelezheti. Ezek az adatok csak a dolgozó által megjelölt célra használhatók fel és csak írásbeli hozzájárulása esetén továbbíthatók más szerv részére. Az előzőekben említett adatokat elkülönítetten kell kezelni, az ezekben szereplő személyazonosító adatokat a munkavállaló kérésére haladéktalanul törölni kell. Ezen adatokból személyazonosításra alkalmatlan módon adatfeldolgozás, illetve adatszolgáltatás készíthető.
104.§ Az adatlap, illetve az alapnyilvántartás hagyományosan vagy elektronikusan is vezethető. Intézetünkben az adatvezetés a két módszer együttes alkalmazásával történik. Mindenképpen papír alapú adatlapot kell alkalmazni az alábbi esetekben: a) a munkavállaló adatainak első alkalommal történő felvételkor,
b) áthelyezésekor,
c) dolgozó egészségügyi szolgálati jogviszonyának megszűnése esetén.
Az érintett, vagy betekintési joggal rendelkező személy vagy szerv erre irányuló külön kérelmére is ki kell nyomtatni azokat az adatokat, amelyekre betekintési joga kiterjed. **105.§** Az elektronikusan vezetett és tárolt adatok esetén a munkaügyi osztályvezetőnek kell gondoskodni a felvett adatok kimentéséről és tárolásáról.

106. § Az alapnyilvántartásból személyazonosító adatokat is tartalmazó adatszolgáltatás

teljesíthető:
a) közigazgatási vagy más hatósági szerv részére törvényben előírt adatszolgáltatási kötelezettség esetén,
b) a munkavállaló írásbeli hozzájárulása alapján, az abban meghatározottak szerint. A statisztikai adatfeldolgozás vagy adatszolgáltatás céljából a személyazonosításra alkalmatlan adatok továbbra is felhasználhatók.
107.§ Az intézet közzéteheti honlapján, vagy épületében tájékoztató táblák formájában a saját munkavállalók/partnerek/betegek és hozzátartozóik (érintettek) eligazítása, illetve a dolgozók azonosítása céljából a dolgozó nevét, beosztását, intézeti elérhetőségeit. **108.§** Az egészségügyi szolgálati jogviszony megszűnése után az alapnyilvántartás adatlapját a személyi iratokkal együtt az irattárba kell elhelyezni.
109.§ A munkavállaló jogosult megismerni, hogy az alapnyilvántartásban szereplő adatait kinek, milyen célból és milyen terjedelemben továbbították. Ennek biztosítása érdekében a munkaügyi osztályvezető az adattovábbításokról nyilvántartást vezet, melyet az adat kiadásától számított 5 évig meg kell őrizni. A munkaügyi osztályvezető a megszokottól eltérő adatszolgáltatási kérelmek vonatkozásában az adatvédelmi tisztviselő tanácsát kéri. Az általa vezetett nyilvántartást rendszeres időközönként továbbítja az adatvédelmi tisztviselőnek.

A betekintési jog gyakorlójának szabályairól

110.§ A személyi iratokba az alábbi szervek és személyek jogosultak
betekinteni: a) saját adataiba a munkavállaló,
b) a munkavállaló felettese,
c) a minősítést végző vezető,
d) a törvényességi ellenőrzést végző,
e) a fegyelmi eljárást lefolytató testület vagy személy,
f) a munkaügyi per kapcsán a bíróság,
g) feladatkörükben eljárva a nemzetbiztonsági szolgálatok, továbbá az egészségügyi szolgálati jogviszonnyal összefüggésben indult büntetőeljárásban a nyomozó hatóság, az ügyész és a bíróság,
h) a személyzeti, munkaügyi és illetmény-számfejtési feladatokat ellátó intézeti munkatársak feladatkörükön belül,
i) más jogviszony alapján keletkezett iratokba az arra vonatkozó törvény szerint jogosultak (adóellenőr, társadalombiztosítási ellenőr, stb.).

111.§ A munkavállaló jogosult a róla nyilvántartott helytelen adat helyesbítését, a jogellenesen nyilvántartott adat törlését kérni, a jogellenesen kért adat közlését megtagadni. Az adatkezelő köteles a helytelen adatot haladéktalanul helyesbíteni, illetve törölni.

A közérdekű adatok kivételével a munkavállaló nyilvántartott adatairól tájékoztatás nem adható, személyi anyagát kiadni nem lehet.
A személyi iratokba való betekintés a munkaügyi osztályvezető hivatali helyiségében történhet. A munkaügyi osztályvezető hivatali helyiségéből személyi iratot - az irattározás kivételével - kizárólag a gazdasági igazgató és az adatvédelmi tisztviselő előzetes engedélyével lehet elvinni. Az érintett számára a munkáltató (munkaügyi osztályvezető) köteles átadni az egyedi technikai azonosító kódját tartalmazó igazolást, amelynek alapján a központi nyilvántartásban a nyilvántartott teljes adatkörét személyesen megtekintheti.

E-mail fiók használatának szabályai

112. § (1) Az intézet e-mail fiókot bocsát meghatározott körben a munkavállaló rendelkezésére a munkaköri feladatok ellátása céljából annak érdekében, hogy a munkavállalók ezen keresztül tartsák egymással a kapcsolatot, vagy a munkáltató képviseletében levelezzenek az ügyfelekkel, más személyekkel, szervezetekkel.

(2) A munkavállaló az e-mail fiókot személyes célra eseti jelleggel használhatja, a fiókban személyes leveleket nem tárolhat, azt olvasást követően haladéktalanul törölni kell a beérkezés napján, akadályoztatás esetén az akadályoztatás megszűnésének napján.

(3) A munkavállaló az e-mail fiókot köteles úgy használni, hogy az abban fellelhető adatokhoz illetéktelen személy ne férhessen hozzá. Köteles gondoskodni arról - különösen a személyes adatok tekintetében, hogy az ilyen adatokat tartalmazó levelezések a felhasználást követően haladéktalanul, nem visszaállítható módon törlésre kerüljenek.
A munkáltató ezen adatokat ellenőrizheti.

Számítógép, laptop, tablet ellenőrzésével kapcsolatos szabályok

113.§ A munkáltató által a munkavállaló részére munkavégzés céljára rendelkezésre bocsátott számítógépet, laptopot, tabletet a munkavállaló kizárólag munkaköri feladata ellátására használhatja, ezek magáncélú használatát munkáltató megtiltja, ezen eszközökön a munkavállaló semmilyen személyes adatot, levelezését nem tárolhat. A munkáltató ezen eszközökön tárolt adatokat ellenőrizheti.

Intézeti mobiltelefon használatának ellenőrzésével kapcsolatos szabályok

114.§ Munkáltató engedélyezi az intézeti mobiltelefon magáncélú használatát, az nem csak munkavégzéssel összefüggő célokra használható, ezért a munkáltató a használathoz kapcsolódóan keretösszegeket határoz meg, mely keretösszeg túllépése esetén a munkavállaló köteles a túlforgalmazás összegét a munkáltató részére megtéríteni. Amennyiben a munkavállaló vitatja a túlforgalmazás összegét, abban az esetben kifejezett kérésére a munkáltató részletes számlát kér ki, mely alapján a felek közösen egyeztetik a magáncélú használat mértékét.

Munkáltató egyes sajátos ellenőrzéseinek szabályai

115.§ Amennyiben munkáltató beléptető rendszert kíván bevezetni, vagy munkavállalóin motozást, illetve alkoholszondázást hajtana végre, azt előzetes érdekmérlegelési tesztnek kell megelőznie.
Ugyanígy, amennyiben a kórházi e-mail fiókokat, a munkavállalók internet használatát, vagy telefonhasználatukat ellenőrzés alá kívánja vetni a munkáltató, előzetesen érdekmérlegelési tesztet kell készítenie. Ennek felelőse az intézet vezetője, aki a kivitelezésben az adatvédelmi tisztviselő tanácsát kérheti

A kórházban üzemelő zártláncú kamera rendszerre vonatkozó érdekmérlegelési teszt a Kamerás megfigyelő rendszer – Adatvédelmi tájékoztató c. dokumentum mellékletét képzi.

Hatályba léptető és záró rendelkezések

116.§ Jelen szabályzat a Balatonfüredi Állami Szívkórház 2021. szeptember 01-én hatályba lépett Adatvédelmi és Adatbiztonsági Szabályzatában tett módosításokat tartalmazza egységes szerkezetben, mely módosítások 2024. szeptember 01-én lépnek hatályba. Jelen szabályzat függelékeként lép életbe az OKFŐ (ÁEEK) által egységesített és tömörített tartalmú Adatvédelmi szabályzat is azzal, hogy ahol ellentmondás tapasztalható a két szabályzat között, ott utóbbi meghatározásai a mérvadóak.

Balatonfüred, 2024. 09. 01.

Dr. Simon Attila
mb. főigazgató

1. SZÁMÚ FÜGGELÉK:

A BALATONFÜREDI ÁLLAMI SZÍVKÓRHÁZ – ADATVÉDELMI SZABÁLYZATA (DATINF – OKFŐ)

A Balatonfüredi Állami Szívkórház - adatvédelmi szabályzata

Tartalomjegyzék

45

1. A szabályzat célja, hatálya, alapelvek, alapfogalmak

1.1. Bevezető rendelkezések

1. Az Állami Szívkórház - Balatonfüred (a továbbiakban: Intézmény) jelen szabályzatban (a továbbiakban: Szabályzat) határozza meg a természetes személyek személyes adatainak kezelésével és védelmével kapcsolatos irányelveket, valamint az adatvédelmi tevékenység ellátásában résztvevő szervezeti egységek feladatait és együttműködésük kereteit.

2. A Szabályzat hatálya alá tartozó személyek kötelesek a tevékenységük során az Intézmény kezelésében lévő személyes adatokat a mindenkori jogszabályi rendelkezéseknek megfelelően, így különösen a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679/EU európai parlamenti és tanácsi rendelet (a továbbiakban: GDPR), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) alkalmazandó rendelkezései, valamint az Intézményre irányadó egyéb jogszabályok rendelkezései szerint kezelni. Az Intézmény a személyes adatok kezelésével járó tevékenysége során érvényre juttatja a GDPR alapelveit, így különösen:
   a/ jogszerűség, tisztességes eljárás és átláthatóság elve: a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni;
   b/ célhoz kötöttség elve: a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történik, és azokat az Intézmény nem kezeli ezekkel a célokkal össze nem egyeztethető módon;
   c/ adattakarékosság elve: a kezelt személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk;
   d/ pontosság elve: a kezelt személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;
   e/ korlátozott tárolhatóság elve: a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé;
   f/ integritás és bizalmas jelleg: a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve;
   g/ beépített adatvédelem elve: olyan megfelelő technikai és szervezési intézkedések végrehajtása, amelyek már az adatkezeléssel járó folyamatok tervezésétől (az

   adatkezelés módjának meghatározásától) kezdődően az adatkezelés megszüntetéséig terjedő időszakban azt célozzák, hogy az adatvédelmi elvek hatékony megvalósítása, illetve a GDPR-ban foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépüljenek az adatkezelés folyamatába;
   h/ alapértelmezett adatvédelem elve: olyan technikai és szervezési intézkedések végrehajtása, amelyek biztosítják, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek, továbbá, hogy a gyűjtött személyes adatok mennyisége,

kezelésük mértéke, tárolásuk időtartama és hozzáférhetőségük is csak az adatkezelési cél szempontjából szükséges mértékre korlátozódjon. Különösen azt kell biztosítani, hogy a személyes adatok alapértelmezés szerint természetes személy beavatkozása nélkül arra illetéktelen személyek számára ne válhassanak hozzáférhetővé.

3. A Szabályzat hatálya alá tartozó személyek kötelesek az olyan tevékenységük során, amely szükségszerűen együtt jár személyes adatok kezelésével, az adott tevékenységre vonatkozó – a Szabályzat **Hiba! A hivatkozási forrás nem található.**. fejezetében felsorolt – speciális szabályzatokban foglalt rendelkezések mellett a jelen szabályzat rendelkezései szerint eljárni azzal, hogy amennyiben a speciális szabályzat a jelen szabályzattal ellentétes rendelkezést tartalmaz, úgy jelen szabályzat alkalmazandó.

1.2. A Szabályzat célja

4. Jelen Szabályzat célja, hogy biztosítsa az Intézmény tevékenysége során a személyes adatok védelméhez fűződő jog érvényesülését, továbbá, hogy az Intézmény által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes és különleges adatok kezelése során irányadó adatvédelmi szabályokat.

5. A Szabályzat célja továbbá, hogy meghatározza azokat a szervezési és technikai intézkedéseket, amelyek kialakításával az Intézmény gondoskodik a személyes adatok kezelése során a személyes adatok biztonságáról. Erre tekintettel a Szabályzat az Intézmény által folytatott adatkezelési tevékenységek során figyelembe veendő és követendő elveket, rendelkezéseket tartalmaz. Ezeket az előírásokat minden egyes adatkezelési folyamat, tevékenység során, annak teljes tartama alatt figyelembe kell venni.

6. A Szabályzat további célja, hogy meghatározza az Intézmény szervezeti egységeinél vezetett, személyes adatokat tartalmazó nyilvántartások vezetésének és működtetésének jogszerű rendjét, valamint biztosítsa a személyes adatok védelme elveinek és az adatbiztonság követelményeinek érvényesülését.

1.3. A szabályzat személyi hatálya

7. Jelen Szabályzat személyi hatálya kiterjed az Intézmény irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek (a munkavégzésre irányuló jogviszony jellegétől függetlenül), továbbá azon természetes személyekre (a továbbiakban: érintett), akik személyes adatait a jelen Szabályzat hatálya alá tartozó adatkezelések tartalmazzák, továbbá azon érintettekre, akik jogait vagy jogos érdekeit az adatkezelés érinti. Az Intézmény megbízásából személyes adatok kezelését vagy feldolgozását végzők esetén az erre a jogviszonyra az Intézmény által kötött szerződésben a GDPR 28. cikkének megfelelően rendelkezni kell arról, hogy az Intézmény által megbízott adatfeldolgozó a feladata ellátása során hogyan juttatja érvényre jelen Szabályzat rendelkezéseit.

1.4. A szabályzat tárgyi hatálya

8. A Szabályzat tárgyi hatálya az Intézmény mindazon adatkezeléseire kiterjed – függetlenül attól, hogy az adatkezelés elektronikusan vagy papíralapon történik –, amelyek

a/ az egészségügyi ellátás nyújtásához kapcsolódó adatkezelést valósítanak meg a Szabályzat **Hiba! A hivatkozási forrás nem található.**. fejezetében felsorolt jogszabályok és belső szabályzatok szerint;

b/ az egészségügyi ellátáson kívüli ügyfélkapcsolati jellegű adatkezelést valósítanak meg (az Intézménnyel kapcsolatba lépni szándékozó, kapcsolatban álló vagy kapcsolatban állt személyek, beleértve ezek meghatalmazottait, képviselőit is);

c/ foglalkoztatási jogviszonyhoz kapcsolódó adatkezelést valósítanak meg [az Intézménnyel egészségügyi szolgálati jogviszonyban, munkaviszonyban vagy egyéb foglalkoztatási jogviszonyban (együtt: foglalkoztatási jogviszony) álló, állt, vagy foglalkoztatási jogviszonyba lépni szándékozó személyek);

d/ az Intézménnyel szerződéses kapcsolatban álló társaságok képviselőinek, kapcsolattartóinak az adataira vonatkoznak.

1.5. Dokumentálási kötelezettség

9. Az Intézmény felelős a személyes adatok kezelésére vonatkozó alapelvek [GDPR 5. cikk (1) bek.] betartásáért. Az Intézménynek képesnek kell lennie a személyes adatok kezelésére vonatkozó alapelvek betartásának igazolására [GDPR 5. cikk (2) bek.]. A megfelelőség igazolása különösen az adatkezeléshez kapcsolódó döntéseket megalapozó körülmények és a döntések (pl. az adatkezelés feltételeit meghatározó döntéselőkészítő iratok), az érintetteknek szóló adatkezelési tájékoztatók, az érintettől származó nyilatkozatok (pl. hozzájáruló nyilatkozatok, az adatkezelési tájékoztató megismerését igazoló dokumentumok), továbbá a személyes adatokat tartalmazó (elektronikus vagy papír alapú) dokumentumok szervezeten belüli vagy azon kívüli mozgásának megfelelő dokumentálásával történik. Az Intézmény – a GDPR 30. cikkének megfelelően – nyilvántartást vezet az általa végzett adatkezelésekről.

10. A megfelelőség igazolása adatvédelmi incidens esetén különösen az incidenssel érintettek körének, az incidenssel érintett személyes adatok körének, az incidens kezelése során tett intézkedéseket megalapozó körülmények és a döntések dokumentálásával történik. Az Intézmény – a GDPR 33. cikkének megfelelően – nyilvántartást vezet a bekövetkezett incidensekkel kapcsolatos tényekről és intézkedésekről.

2. Alapfogalmak

11. Jelen Szabályzat alkalmazása során a GDPR 4. cikkében és az Infotv. 3. § 3., 4., 6., 11., 12., 13., 16., 17., 21., 23-24. pontjában meghatározott fogalmakon kívül az alábbi fogalmakat kell alkalmazni:

a/ adatbiztonság: a személyes adatok jogosulatlan kezelése, így különösen jogosulatlan megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások, valamint eljárási szabályok összessége; az adatkezelés azon állapota, amelyben az adatok sérülésének, illetéktelen felhasználásának, megsemmisülésének kockázati tényezőit – és ezáltal a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a minimálisra csökkentik,

b/ Adatkezelési Nyilvántartás: jelen utasítás **Hiba! A hivatkozási forrás nem található.**. fejezetében meghatározott adattartalmú, folyamatosan karbantartott nyilvántartás; c/ adatkezelésért felelős szervezeti egység: az Intézmény azon szervezeti egysége, amelynek feladatkörébe tartozik az Intézmény kezelésében lévő valamely

nyilvántartási rendszer létrehozása, fenntartása, illetve üzemeltetése,

d/ adatvédelmi felügyeleti hatóság: a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság),

e/ adatvédelmi hatásvizsgálat: olyan vizsgálat, amelyet az adatkezelésért felelős szervezeti egység kijelölt munkavállalója (adatkezelési megbízott) köteles elvégezni, amennyiben valamely tervezett adatkezelés – figyelemmel annak jellegére, hatókörére, körülményeire és céljaira, ideértve különösen az új technológiák alkalmazásának esetét – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, és amelynek célja annak megállapítása, hogy a tervezett adatkezelés a személyes adatok védelmét hogyan érinti. Az adatvédelmi hatásvizsgálat egy olyan eljárás, amelynek során az adatkezelő a tervezett adatkezelési műveletet vagy műveleteket áttekinti, megvizsgálja az adatkezelés érintettekre gyakorolt esetleges hatását, felméri annak kockázatait, a kockázatok kezelésének módját, és mindezt megfelelően dokumentálja,

f/ adatvédelmi incidens jellege: személyes adatok megsemmisülése, személyes adatok jogosulatlan megsemmisítése, személyes adatok rendelkezésre állásának sérülése, személyes adatok integritásának sérülése, személyes adatok elvesztése, személyes adatok jogosulatlan megváltoztatása, személyes adatok jogosulatlan közlése vagy jogellenes továbbítása, személyes adatokhoz történő jogosulatlan hozzáférés, személyes adatok bizalmasságának sérülése (pl. titoksértés) stb.

g/ adatkezelési megbízott: az adatkezelésért felelős szervezeti egység azon, e feladatkör ellátására kijelölt munkavállalója, aki a jelen utasításban, illetve az adatkezelést szabályozó más belső szabályozó dokumentumokban meghatározottak szerint az adatkezelésért felelős szervezeti egység felelősségi körébe tartozó adatkezelések tekintetében, vagy adatkezeléseknek az adatkezelésért felelős szervezeti egység felelősségi körébe tartozó részében gondoskodik az adatkezelőt terhelő feladatok elvégzéséről,

h/ adatvédelmi tisztviselő: az Intézmény szervezetében működő, a GDPR 39. cikkében meghatározott feladatokat az Intézmény jelen szabályzatában foglaltak szerint ellátó, az Intézménnyel foglalkoztatási jogviszonyban álló természetes személy,

i/ *álnevesítés (pszeudonimizálás)* 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,

j/ deperszonalizálás (anonimizálás): a nyilvántartási rendszerben tárolt személyes adatok közül a személyazonosításra alkalmas adatok eltávolítása olyan, visszafordíthatatlan módon, hogy a nyilvántartási rendszerben megmaradó adatok a továbbiakban semmilyen körülmények között nem teszik lehetővé egy természetes személy azonosítását,

k/ dolgozói személyes adat: az Intézménnyel foglalkoztatási jogviszonyban álló személyek adata,

l/ érdekmérlegelési teszt: jogos érdeken alapuló adatkezelés tervezett bevezetése esetén annak írásbeli dokumentálása, hogy az adatkezelő számba vette az adatkezelést megalapozó érdekeket, érveket, valamint az érintettek személyes adatok védelméhez fűződő – a tervezett adatkezelés ellen ható – jogait és érdekeit, és ezen érdekek és érvek összevetésével megalapozza az adatkezelés bevezetését

vagy a bevezetés elutasítását,

m/ informatikai szakterület: az informatikai rendszerek üzemeltetéséért, az informatikai biztonság ellátásáért felelős szervezeti egység vagy egységek, ideértve az Intézmény információbiztonsági felelősét is,

n/ titkosítás: az adatok olyan átalakítása, melynek során az adat értelmezhetetlenné válik a megfelelő kulcs ismerete nélkül,

o/ törlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása a továbbiakban már nem lehetséges. A törlés célja megvalósítható deperszonalizálással (anonimizálással) [**Hiba! A hivatkozási forrás nem található.** pont] is,

p/ ügyvitel: az Intézmény tevékenységére vonatkozó jogszabályokban az Intézmény részére meghatározott közfeladatok ellátásával összefüggő eljárás.

3. A szabályzathoz kapcsolódó jogszabályok, belső szabályzatok

GDPR	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 irányelv hatályon kívül helyezéséről
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [az Infotv-nek a GDPR hatálya alá eső adatkezelésekre alkalmazandó szabályai – lsd. Infotv. 2. § (2) és (4) bekezdése]
Eüak.	1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről, és a végrehajtására kiadott jogszabályok
Eütv.	1997. évi CLIV. törvény az egészségügyről, és a végrehajtására kiadott jogszabályok
Ebtv.	1997. évi LXXXIII. törvény kötelező egészségbiztosítás ellátásairól, és a végrehajtására kiadott jogszabályok
Eszjtv.	2020. évi C. törvény az egészségügyi szolgálati jogviszonyról és annak az egészségügyi ágazatban történő végrehajtására vonatkozó jogszabályok
Mt.	2012. évi I. törvény a Munka Törvénykönyvéről
	az Állami Szívkórház Balatonfüred Közérdekű adatok közzétételi szabályzata
	az Állami Szívkórház Balatonfüred Informatikai Biztonsági Szabályzata
	az Állami Szívkórház Balatonfüred Adatvédelmi és Adatbiztonsági Szabályzata
	az Állami Szívkórház Balatonfüred Szervezeti Integritást Sértő Események Kezelésének Eljárásrendje
	az Állami Szívkórház Balatonfüred Irat- és dokumentumkezelési szabályzata
	az Állami Szívkórház Balatonfüred szervezeti egységei által kezelt nyilvántartási rendszereket szabályozó utasítások

4. Az adatvédelmi tevékenység szervezete és irányítása az Intézménynél

4.1. Az adatvédelmi tevékenység ellátásában résztvevők

Az adatvédelmi tevékenység irányításában és ellátásában az Intézmény szervezeti egységei – az Intézmény Szervezeti és Működési Szabályzatában meghatározott feladatkörükön belül – az

alábbiak szerint vesznek részt.

12. A főigazgató felelős azért, hogy az Intézmény – mint adatkezelő, illetve adatfeldolgozó – működése az adatvédelmi szabályoknak megfeleljen. Ennek érdekében:
    a/ gondoskodik az adatvédelmi tevékenység irányításában és ellátásában résztvevő szervezeti egységek kijelöléséről, feladataik, az adatvédelmi tárgyú ügyekkel kapcsolatos döntési jogkörök meghatározásáról, az egyes adatkezelési döntési szintek kialakításáról;
    b/ biztosítja az adatvédelmi tevékenység irányításához és ellátásához, valamint az érintett jogai gyakorlásához szükséges személyi és tárgyi feltételeket;
    c/ felelős az adat- és titokvédelmi, valamint biztonsági és információbiztonsági szabályzatok kiadásáért és betartatásáért;
    d/ gondoskodik arról, hogy az adatvédelmi tevékenység során esetleg előforduló, feltárt hiányosságok megszűntetéséről, szükség szerint a felelősségre vonásról;

    e/ kinevezi az Intézmény adatvédelmi tisztviselőjét, és az adatvédelmi tisztviselő nevét és elérhetőségét bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak;
    f/ munkajogi értelemben vett közvetlen felettese az adatvédelmi tisztviselőnek;
    g/ kijelöli az egyes szervezeti egységek adatkezelési megbízottját;
    h/ biztosítja az Intézmény adatvédelmi tisztviselője feladatainak ellátásához szükséges személyi és tárgyi feltételeket.

13. Az Intézmény szervezeti egységeinek adatkezelési megbízottjai adatvédelmi szempontból az irányításuk alá tartozó szervezeti egység tekintetében:
    a/ betartják és betartatják az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírásokat; az adatvédelmi tisztviselővel, valamint az informatikai szakterülettel együttműködve gondoskodnak az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról;
    b/ gondoskodnak arról, hogy az irányításuk alá tartozó szervezeti egységek felelősségi körébe tartozó nyilvántartási rendszerek naprakészek, megbízhatóak legyenek; c/ gondoskodnak arról, hogy az irányításuk alatt álló szervezeti egységek dolgozói az adatkezelés meghatározott feltételeinek megfelelően járjanak el [GDPR 32. cikk (4) bek.];
    d/ az adatkezelési megbízott előterjesztésére – az Intézmény döntéselőkészítésre vonatkozó szabályainak megfelelően – döntenek a jelen utasításban, illetve az adatkezeléssel járó folyamatot szabályozó egyéb belső szabályzatokban a feladat- és hatáskörébe utalt kérdésekben.

14. A Főigazgatói Titkárság
    a/ az Intézménynek a főigazgatói utasítások előkészítésére és kiadására vonatkozó szabályai szerint biztosítja, hogy az adatvédelmi tisztviselő véleményét kikérjék az Intézmény adatvédelmi tárgyú vagy adatvédelmi vonatkozású belső szabályzatainak előkészítése során,
    b/ az adatvédelmi tisztviselő szükség szerinti közreműködésével ellátja az érintetti jogok gyakorlásával kapcsolatos beadványok megválaszolását (**Hiba! A hivatkozási forrás nem található.**. pont) a személyes adatok kezelését, illetve a GDPR szerinti jogaik gyakorlását érintő panaszok (**Hiba! A hivatkozási forrás nem található.**. pont **Hiba! A hivatkozási forrás nem található.** alpont) kivételével.

15. Az informatikai szakterület az Intézmény szervezeti és működési szabályzatában, valamint az Intézmény információbiztonsági szabályzatában meghatározott feladatkörében: a/ ellátja az informatikai biztonsági biztonsággal kapcsolatos feladatokat a folyamatos üzemeltetési feladatok kivételével, különösen az Intézmény Adatvédelmi és Adatbiztonsági Szabályzatban meghatározott feladatokat;

b/ ellátja az informatikai fejlesztéseknél és beszerzéseknél a beépített adatvédelem kontrolljai meglétének biztosításával, az adatminőség biztosításával, az informatikai

biztonság kockázatarányos szintjét biztosító jogosultsági és naplózási rendszer kialakításának megfelelőségével, a biztonságos szoftverfejlesztés alapelveinek érvényesítésével kapcsolatos feladatokat,

c/ az informatikai rendszerek üzemeltetése területén ellátja a személyes adatok kezelésével kapcsolatos technikai védelem megvalósítását, ellátja – az Intézmény Adatvédelmi és Adatbiztonsági Szabályzatban meghatározott – hatáskörébe tartozó információbiztonsági feladatokat, valamint rendelkezésre állási kontrollok biztosítását, a tárolt és továbbított személyes adatok bizalmasságának védelmét, az incidensfelderítési és -kezelési tevékenység támogatását,

d/ gondoskodik az információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról.

16. A jogtanácsos

a/ szakmai támogatást nyújt az adatkezeléssel összefüggő, nem adatvédelmi jogszabályok értelmezésében,

b/ biztosítja az Intézmény képviseletét az érintett által az Intézmény ellen az érintett adatvédelmi jogainak megsértése miatt indított, illetve az Intézmény által a Nemzeti Adatvédelmi és Információszabadság Hatóság határozatainak felülvizsgálata iránt indított perekben, illetve egyéb eljárásokban.

17. Az adatkezelési megbízott a felelősségi körébe tartozó szervezeti egység(ek) feladatkörén belül jelen szabályzat és egyéb belső szabályzatok szerint:

a/ előkészíti az adatkezeléssel kapcsolatos, az adatkezelőt terhelő döntéseket, illetve abban közreműködik;

b/ gondoskodik az adatkezeléshez kapcsolódó adminisztratív teendők ellátásáról (az adatkezeléssel összefüggő döntések dokumentálása, érdekmérlegelési teszt elvégzése, hatásvizsgálat lefolytatása, az adatkezeléssel összefüggő szerződések előkészítése, az Adatkezelési Nyilvántartás naprakészen tartásához szükséges információk átadása az adatvédelmi tisztviselő részére stb.), illetve abban közreműködik;

c/ együttműködik az ugyanazon adatkezelésben érintett más adatkezelési megbízottakkal;

d/ közreműködik az érintettek jogai gyakorlásának biztosításában;

e/ közreműködik az adatvédelmi incidensek következményeinek elhárításában;

f/ közreműködik az adatvédelmi tisztviselő vizsgálataiban;

g/ közreműködik az adatvédelmi tisztviselővel az adatvagyon-felmérés elkészítésében,

h/ közreműködik az adatvédelmi tisztviselővel az Intézmény kezelésében lévő az adatok biztonsági osztályba sorolásában.

18. Adatkezelési megbízottat valamennyi fekvőbeteg osztályon ki kell jelölni. Adatkezelési megbízottnak olyan személyt kell kijelölni, aki az adott szakterületet, üzleti/adminisztratív folyamato(ka)t, illetve a szakterületek tevékenységét támogató informatikai rendszereket

illetően kellő ismeretekkel bír.

4.2. Az adatvédelmi tisztviselő

19. Az adatvédelmi tisztviselőt a főigazgató főorvos nevezi ki az olyan, az Intézménnyel foglalkoztatási jogviszonyban álló természetes személyek közül, aki ismeri az Intézmény működését, feladatait, munkafolyamatait és rendelkezik:
    a/ az európai és hazai adatvédelemmel kapcsolatos főbb szabályozók, hatósági és bírósági határozatok, iránymutatások ismeretével;
    b/ alapvető adatvédelmi és informatikai folyamatok ismeretével;
    c/ legalább 2 év adatvédelmi területen szerzett gyakorlattal.

20. Az adatvédelmi tisztviselő kinevezése mellett az Intézmény adatvédelmi tanácsadási feladattal egyéb, jogi vagy természetes személy szakértőt is megbízhat.

21. 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.

22. Az Intézmény elősegíti az adatvédelmi tisztviselő megfelelő szakmai feladatellátását, ennek érdekében az Intézmény biztosítja különösen az adatvédelmi tisztviselő feladatai végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáférést, valamint a szakértői szintű ismereteinek fenntartásaihoz szükséges forrás biztosítását, elegendő idő biztosítását feladatai ellátásához, valamint az informatikai és a biztonsági szakterület együttműködése révén az adatvédelmi tisztviselő bevonását:
    a/ a megfelelő technikai-eljárási intézkedésekhez szükséges források meghatározása (költségvetési tervezés) során annak érdekében, hogy teljesüljenek az adatvédelem alapelvei a technikai vívmányok alkalmazása (beépített adatvédelem) és az adatvédelem-barát megoldások (alapértelmezett adatvédelem) révén;
    b/ a felügyeleti hatósággal történő együttműködés során, amellyel az adatvédelmi tisztviselő – a jogtanácsos és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – tartja a kapcsolatot.

23. Az adatvédelmi tisztviselő véleményét – a jelen szabályzat rendelkezései szerint – ki kell kérni az adatkezelést érintő döntések, szerződések és belső szabályzatok tervezetéről.

24. Az adatvédelmi tisztviselőt tisztsége fennállása alatt és annak megszűnését követően titoktartási kötelezettség terheli a tevékenysége során tudomására jutott, közérdekű vagy közérdekből nem nyilvános adatnak nem minősülő információk kapcsán.

25. Az Intézményben nem lehet adatvédelmi tisztviselő az a természetes személy, aki az Intézményben az adatkezelési tevékenység céljainak, kereteinek, eszközeinek meghatározásáról dönt, különösen a főigazgató, az intézet magasabb vezetői, adatkezelésért felelős szervezeti egységek vezetője.

26. Az adatvédelmi tisztviselő az adatvédelmi tisztviselői feladatokon kívül a főigazgató döntése alapján más munkakörhöz kötődő feladatokat is elláthat, amennyiben azok nem eredményeznek összeférhetetlenséget.

27. Az adatvédelmi tisztviselő nevét és elérhetőségeit az Intézmény honlapján, székhelyén, telephelyén a nyilvánosság részére mindenkor elérhetővé kell tenni. Az Intézmény továbbá közli az adatvédelmi tisztviselő nevét és elérhetőségét a Nemzeti Adatvédelmi és Információszabadság Hatósággal.

28. Az adatvédelmi tisztviselő feladatai:

a/ közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;

b/ ellenőrzi a GDPR, az Infotv. és az adatkezelésre vonatkozó más jogszabályok, valamint a jelen szabályzat, továbbá az Intézmény egyéb belső szabályzatai rendelkezéseinek a megtartását, belső adatvédelmi ellenőrzési eljárást folytat le;

c/ kivizsgálja – az érintett szakterületek és a jogtanácsos bevonásával – a neki címzett panaszokat, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;

d/ megszövegezi a hozzájáruló nyilatkozat (GDPR 7. cikk (2) bek), illetve a megfelelő szerződéses rendelkezéseket;

e/ megfogalmazza az adatkezelésről szóló tájékoztatást (GDPR 13-14. cikk); f/ az informatikai szakterület közreműködésével gondoskodik az adatkezelésről szóló tájékoztatás könnyen hozzáférhető módon való közzétételéről (GDPR 12. cikk (2) bek.);

g/ a jogtanácsossal és az informatikai szakterülettel együttműködve elkészíti az adatvédelmi és adatbiztonsági szabályzatot;

h/ a jogtanácsossal együttműködve gondoskodik az adatvédelmi ismeretek oktatásáról [elsősorban az intraneten közzétett segédanyagok útján];

i/ a jogtanácsossal együttműködve személyes adatok kezelésére vonatkozó előírásokról tájékoztatást nyújt, tanácsot ad;

j/ személyes adatot is kezelő új informatikai rendszer belső fejlesztéssel történő bevezetése során közreműködik az adatvédelmi hatásvizsgálatot lefolytatásában; k/ az adatvédelmi incidenskezeléssel kapcsolatban ellátja a jelen szabályzat szerinti feladatokat;

l/ vezeti az Adatkezelési Nyilvántartást (**Hiba! A hivatkozási forrás nem található.**. fejezet);

m/ éves összefoglaló jelentést készít a főigazgatónak;

n/ kapcsolatot tart és – a jogtanácsos és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – együttműködik a Hatósággal; o/ az Állami Egészségügyi Ellátó Központ számára adatszolgáltatást teljesít.

5. Adatkezelés bevezetésével, módosításával és megszüntetésével kapcsolatos feladatok

5.1. Adatkezelés bevezetésével kapcsolatos feladatok

29. Jogszabályban elrendelt vagy jogszabály rendelkezése miatt szükséges, vagy az Intézmény döntése alapján létrehozandó nyilvántartási rendszer (a továbbiakban együtt: adatkezelés) bevezetése esetén, amennyiben az természetes személyek adatainak kezelésével (beleértve meglévő nyilvántartási rendszer adatainak új célú felhasználásával, új célú adatkezelés bevezetésével, nyilvántartási rendszerbe adatok felvételével, adatok tárolásával, harmadik

személynek továbbításával stb.) jár, az adatkezelés bevezetése során az Intézménynek a főigazgatói utasítások előkészítésére és kiadására vonatkozó szabályait e fejezet rendelkezéseit figyelembe véve kell alkalmazni.

30. Adatkezelés bevezetése főigazgatói engedéllyel történik. A főigazgatói engedélyre való felterjesztés tartalmazza
    a/ az adatkezelésért felelős szervezeti egységnek és egyéb szervezeti egységeknek az adatkezeléssel kapcsolatos feladatait, így különösen:
        aa/ az adatok felvételének, módosításának, törlésének rendje,
        ab/adatszolgáltatási kötelezettségek meghatározása az adatok naprakészen tartása érdekében,
        ac/ a nyilvántartási rendszerből történő adattovábbítás, az ahhoz való hozzáférés rendje;
    b/ az adatkezelésre vonatkozó különös adatbiztonsági intézkedések meghatározása;
    c/ mellékletként
        ca/ a GDPR-nak, az Infotv-nek és egyéb alkalmazandó jogszabálynak megfelelő adatkezelési tájékoztatót,
        cb/ hozzájáruláson alapuló adatkezelés esetén a hozzájáruló nyilatkozat mintáját.

31. Az adatkezelésért felelős szervezeti egység adatkezelési megbízottját az új adatkezelés bevezetésére vonatkozó igény megfogalmazásától kezdve be kell vonni az adatkezelés feltételeinek kidolgozása folyamatába.

32. Amennyiben az új adatkezelés bevezetése több szakterületet/szervezeti egységet érint, az adatkezelésért felelős valamennyi érintett szervezeti egység adatkezelési megbízottját be kell vonni az adatkezelés feltételeinek kidolgozása folyamatába. Az informatikai szakterület vezetőjét minden esetben be kell vonni a folyamatba.

33. Az adatkezelés feltételeinek kidolgozásában érintett szervezeti egységek adatkezelési megbízottjai kötelesek egymással és az adatvédelmi tisztviselővel együttműködni. Az adatkezelés feltételeinek kidolgozásában érintett szervezeti egységek adatkezelési megbízottjai tevékenységének koordinálásáról az adatvédelmi tisztviselő gondoskodik.

34. Az adatkezelés bevezetésével, az adatkezelés feltételeinek meghatározásával kapcsolatban

    a/ a leendő adatkezelésért annak tárgya szerint felelős szervezeti egység adatkezelési megbízottja az adatvédelmi tisztviselővel együttműködve
        aa/meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, és ilyen tartalmú javaslatot készít a döntésre jogosultnak (GDPR 4. cikk 7. és 16. pont);
        ab/az **Hiba! A hivatkozási forrás nem található.** alpontban meghatározott feladat részeként előterjesztést tesz a döntésre jogosultnak arról, hogy az eltérő célú adatkezelés összeegyeztethető-e az eredeti céllal, és így szolgálhat-e a tervezett adatkezelés új jogalapjául [GDPR 6. cikk (4) bek.];
        ac/ az **Hiba! A hivatkozási forrás nem található.** pontban meghatározott feladat részeként, amennyiben az adatkezelés jogalapja a jogos érdek lehet, együttműködik az érdekmérlegelési teszt dokumentumának elkészítésében [GDPR 6. cikk (1) bek. f) pont];
        ad/az **Hiba! A hivatkozási forrás nem található.** pontban meghatározott feladat részeként javaslatot tesz a döntésre jogosultnak adatvédelmi hatásvizsgálat elvégzésére [**Hiba! A hivatkozási forrás nem található.**-**Hiba! A hivatkozási forrás**

nem található.. pont]; a döntésre jogosult erre vonatkozó pozitív döntése esetén – az informatikai fejlesztéseket, az informatikai architektúra tervezést, illetve az IT üzemeltetést végző szervezeti egység vezetőjénekközreműködésével – együttműködik a hatásvizsgálat elkészítésében, elkészíti ennek dokumentumát, és kikéri róla az adatvédelmi tisztviselő, valamint – ha alkalmazható – az érintettek vagy képviselőik véleményét [GDPR 35. cikk (1)-(2) és (9) bek.];

ae/ az **Hiba! A hivatkozási forrás nem található.** pontban meghatározott feladat részeként előterjesztést tesz a döntésre jogosultnak arról, hogy az adatkezelést közös adatkezelésként indokolt-e ellátni, illetve indokolt-e adatfeldolgozót bevonni;

af/ az **Hiba! A hivatkozási forrás nem található.** pontban meghatározott feladat részeként az adatvédelmi tisztviselővel együttműködve javaslatot tesz automatizált döntéshozatali módszer, illetve profilalkotási módszer alkalmazására [GDPR 22. cikk (1) bek.];

ag/ az adatkezelés bevezetéséről való döntést követően megküldi az adatvédelmi tisztviselőnek az új adatkezelésnek az Adatkezelési Nyilvántartásban történő rögzítéséhez szükséges információkat, illetve a nyilvántartott adatokban bekövetkezett valamennyi változást [GDPR 30. cikk (1) bek.]

ah/amennyiben ennek szükségessége felmerül, egyedi esetben segítséget nyújt az adatvédelmi tisztviselőnek a döntésre jogosult felé történő előterjesztés előkészítésében az érintett vagy harmadik személy létfontosságú érdeke fennállásáról [GDPR 6. cikk (1) bek. d) pont, 9. cikk (2) bek. d) pont] mint az adatkezelés lehetséges jogcíméről;

ai/ amennyiben ennek szükségessége felmerül, a **Hiba! A hivatkozási forrás nem található.**. fejezet szabályait is figyelembe véve egyedi esetben segítséget nyújt az adatvédelmi tisztviselőnek a döntésre jogosult felé történő előterjesztés

elkészítésében arról, hogy személyes adatok harmadik országba továbbíthatók-e egyedi ügyekben [GDPR 49. cikk (1) bek.];

b/ az informatikai szakterület vezetője – szervezeti egysége feladatkörében – a személyes adatot kezelő rendszer fejlesztése és beszerzése során közreműködnek

ba/a célhoz kötött adatkezelés és az adattakarékosság elvének megfelelően gyűjtött adatokra vonatkozóan a beépített és alapértelmezett adatvédelem elveinek dokumentált érvényesüléséről;

bb/annak biztosításában, hogy az adathordozhatóság, adattörlés és adattisztítás célú módosítások szabályozott és dokumentált módon valósuljanak meg; bc/ annak biztosításában, hogy az adatvédelmi tájékoztatók és nyilatkozatok könnyen elérhetők legyenek az ügyfelek számára,

bd/annak biztosításában, hogy az adatkezeléssel kapcsolatos ügyfélrendelkezéseket visszakereshető formában tárolják;

be/az adatok sértetlenségével, bizalmasságuk megőrzésével és üzletmenet folytonossággal kapcsolatos kontrollok (pl. változáskezelés, magas rendelkezésre állás, jogosultságkezelés, adatrejtő eljárások, incidenskezelés támogatása) tervezéskori érvényesítésében, illetve dokumentált meglétében;

bf/ az adott adatkezelés különös (az Intézmény Adatvédelmi és Adatbiztonsági Szabályzatától eltérő) adatbiztonsági intézkedések meghatározásában;

bg/az **Hiba! A hivatkozási forrás nem található.**, **Hiba! A hivatkozási forrás nem található.**, **Hiba! A hivatkozási forrás nem található.**, **Hiba! A hivatkozási forrás**

nem található., **Hiba! A hivatkozási forrás nem található.** és **Hiba! A hivatkozási forrás nem található.** alpont szerinti döntések előkészítésében.

35. A **Hiba! A hivatkozási forrás nem található.**. pont alkalmazása során döntésre jogosultnak minősül az személy, aki – az Intézmény Szervezeti és Működési Szabályzata szerint – az érintett adatkezelés alapjául szolgáló tevékenységgel kapcsolatban döntésre jogosult, illetve – amennyiben a döntés testületi hatáskörbe tartozik – a testületi döntés előkészítéséért felelős.

36. A **Hiba! A hivatkozási forrás nem található.**. pontban meghatározott döntések, javaslatok véglegesítése előtt ki kell kérni az adatvédelmi tisztviselő véleményét, úgy, hogy az adatvédelmi tisztviselőnek legalább 10 munkanapja legyen a vélemény adására.

37. Az adatvédelmi tisztviselő véleményének kikéréséhez olyan dokumentumot/leírást kell benyújtani, amely kellő részletességgel meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, illetve a **Hiba! A hivatkozási forrás nem található.**. pontban meghatározott egyéb döntési javaslatokat.

38. Az adatvédelmi tisztviselő adatvédelmi jogi támogatást nyújt az adatkezelési megbízott által előkészített, megszövegezett, adatkezeléshez kapcsolódó dokumentumok elkészítésében és közreműködik azok véglegesítésében. Az adatvédelmi tisztviselő
a/ beszerzi az alábbi szervezeti egységek véleményét is:

aa/ a jogtanácsos véleményét a **Hiba! A hivatkozási forrás nem található.**. pont **Hiba! A hivatkozási forrás nem található.**, **Hiba! A hivatkozási forrás nem található.**, **Hiba! A hivatkozási forrás nem található.**, **Hiba! A hivatkozási forrás nem található.**, **Hiba! A hivatkozási forrás nem található.** és **Hiba! A hivatkozási forrás nem található.** alpont tekintetében;

ab/az informatikai szakterület véleményét a **Hiba! A hivatkozási forrás nem található.**. pont **Hiba! A hivatkozási forrás nem található.**, **Hiba! A hivatkozási forrás nem található.**, **Hiba! A hivatkozási forrás nem található.**, **Hiba! A hivatkozási forrás nem található.**, **Hiba! A hivatkozási forrás nem található.** és **Hiba! A hivatkozási forrás nem található.** alpont tekintetében;

b/ megvizsgálja a véleményezésre megküldött dokumentumot/leírást

ba/adatvédelmi jogi szempontból,

bb/abból a szempontból, hogy azok milyen módon illeszthetők be az Intézmény informatikai rendszereibe, illetve nincs-e a tervezett adatkezeléssel azonos vagy hasonló adatkezelés.

39. A végleges dokumentumok szakmai megfelelőségéért a dokumentum létrehozását kezdeményező adatkezelési megbízott, az adatvédelmi megfelelőségéért az adatvédelmi tisztviselő, az informatikai, információbiztonsági megfelelőségért pedig az informatikai szakterület a felelős. Abban az esetben, ha bármely terület eltér a megfogalmazott szakmai, adatvédelmi vagy információbiztonsági állásfoglalásoktól, az eltérésért, illetve a végleges dokumentumért az adatvédelmi tisztviselő vagy az információbiztonsági szakterület semmilyen felelősséggel nem tartozik.

40. A **Hiba! A hivatkozási forrás nem található.**. pontban említett szervezeti egységek a véleményüket az adatvédelmi tisztviselőnek küldik meg az adatvédelmi tisztviselő által meghatározott határidőben, amely nem lehet kevesebb 5 munkanapnál. A véleményeket az adatvédelmi tisztviselő összesíti és véglegesíti, szükség esetén az adatkezelési

megbízottakkal és a véleményezőkkel való konzultáció után.

41. Amennyiben az adatkezelés feltételei kidolgozásában részt vevő adatkezelési megbízottak között véleményeltérés van, illetve a jogtanácsos vagy az informatikai szakterület kifogást fogalmaz meg, az adatvédelmi tisztviselő – szükség esetén az adatkezelési megbízottakkal és a véleményezőkkel való konzultáció után – javaslatot tesz a lehetséges megoldásra.

42. Az adatvédelmi tisztviselő véleményét az adatkezelés bevezetéséről való döntést kezdeményező előterjesztésben ismertetni kell. Az adatvédelmi tisztviselő véleményétől való eltérést az előterjesztésben részletesen meg kell indokolni.

5.2. Az adatkezelési megbízott feladatai az adatkezelés során

43. Az adatkezelés során az adatkezelésért felelős szervezeti egység adatkezelési megbízottja az adatkezelésért felelős szervezeti egység feladatkörébe tartozó kérdésekben:

a/ képviseli az adatkezelőt az adatfeldolgozó felé vagy – közös adatkezelés esetén – a többi adatkezelő felé (amennyiben releváns);

b/ figyelemmel kíséri az adatkezelés feltételeinek folyamatos fennállását (beleértve az adatkezelés jogszerűségéhez szükséges tájékoztatások megadását, nyilatkozatok beszerzését stb.) és szükség esetén megteszi vagy kezdeményezi a szükséges intézkedéseket az adatkezelés feltételeinek módosítása iránt;

c/ amennyiben az adatkezelés hozzájáruláson alapul, ellenőrzi, hogy az érintett a hozzájárulását szabályosan szerezték-e be [GDPR 7. cikk (1) bek.];

d/ gondoskodik arról, hogy legalább az érintettel való első kapcsolatfelvételkor felhívják a figyelmét a tiltakozási jogra, és hogy az erről szóló tájékoztatást egyértelműen és más információtól elkülönítve jelenítsék meg [GDPR 21. cikk (4) bek.];

e/ rendszeres időközönként, de legalább évente segítséget nyújt az adatvédelmi tisztviselőnek a hatásvizsgálatban azonosított kockázatok áttekintésében, jelzi az adatvédelmi tisztviselőnek az adatkezeléssel járó kockázatok változását, közreműködik az adatvédelmi hatásvizsgálatok utóellenőrzésben [GDPR 35. cikk (11) bek.].

44. Az adatkezelés során (informatikai rendszerben kezelt adatok esetén az informatikai rendszer üzemeltetési szakaszában) az informatikai szakterület vezetője – a feladatkörébe tartozó kérdésekben – gondoskodik arról, hogy az adatkezelés általános adatbiztonsági kontrolljainak működtetése az erre vonatkozó eljárásrendeknek és az informatikai szakterület által meghatározott elvárásoknak megfelelően történjék, ezen belül gondoskodva különösen

a/ a fizikai és logikai hozzáférés-védelem kontrolljairól,

b/ a rendkívüli esemény-kezelési eljárásokról (adatvédelmi incidensek feladatkörükbe tartozó kezelése, kedvezőtlen külső vagy belső behatásokkal szembeni ellenállási képesség biztosítása),

c/ jogosultságkezelésről és

d/ az adatminőséggel, illetve adatrejtéssel kapcsolatos intézkedések végrehajtásáról.

45. A **Hiba! A hivatkozási forrás nem található.**. pont **Hiba! A hivatkozási forrás nem található.** alpont alá eső esetekben

a/ megfelelően alkalmazni kell a **Hiba! A hivatkozási forrás nem található.**-**Hiba! A hivatkozási forrás nem található.**. pont rendelkezéseit,

b/ az adatkezelés megváltozott adatait – a változást elrendelő döntés után – át kell vezetni

az Adatkezelési Nyilvántartásban.

5.3. Adatkezelés megszüntetésével kapcsolatos feladatok

46. Amennyiben a kezelt adatokra a továbbiakban nincs szükség (az adatkezelési cél megvalósult), vagy jogszabályi változások miatt, vagy az adatvédelmi felügyeleti hatóság vagy bíróság döntése értelmében az adatok kezelését meg kell szüntetni, az adatkezelési

megbízott – az adatvédelmi tisztviselővel és rajta keresztül a jogtanácsos és az informatikai szakterülettel közösen – javaslatot tesz a döntésre jogosultnak:

a/ az adatkezelés egészének vagy egyes adatfajták nyilvántartásának megszüntetésére (az adatok archiválására az adattörlési idő leteltéig),

b/ nyilvántartási rendszer egészének vagy egyes adatfajták, illetve adatok törlésére.

47. A **Hiba! A hivatkozási forrás nem található.**. pontban meghatározott esetben a/ megfelelően alkalmazni kell a **Hiba! A hivatkozási forrás nem található.**-**Hiba! A hivatkozási forrás nem található.**. pont rendelkezéseit,

b/ az Adatkezelési Nyilvántartásból az adatkezelést vagy az egyes adatfajtákat törölni kell,

c/ az adatokat – a **Hiba! A hivatkozási forrás nem található.**. pont **Hiba! A hivatkozási forrás nem található.** és **Hiba! A hivatkozási forrás nem található.** pontjában tett megkülönböztetés szerint –

ca/ az informatikai rendszerekben archiválni kell, illetve

cb/ az informatikai rendszerekből törölni kell, a papír alapú nyilvántartásban kezelt adatokat pedig – az Intézmény iratkezelési szabályzatában foglaltaknak megfelelően– selejtezni kell.

5.4. Az érdekmérlegelési teszt elvégzésének módszertana

48. Amennyiben az Intézmény valamely adatkezelésének az Intézmény vagy harmadik személy jogos érdeke a jogalapja [GDPR 6. cikk (1) bekezdés f) pont], érdekmérlegelési tesztet kell elvégezni és azt dokumentálni. Jogos érdek az a törvényes, kellően pontosan megfogalmazott, valós és fennálló, illetve elérhető előny, amelyet az adatkezelő származtat – vagy a harmadik személy származtathat – az adatkezelésből.

49. Az érdekmérlegelési tesztet az adatvédelmi tisztviselő felügyelete mellett a tervezett adatkezelésért felelős szervezeti egység adatkezelési megbízottja végzi el. Az érdekmérlegelési tesztet írásban kell elvégezni. Az elkészült dokumentumot – a **Hiba! A hivatkozási forrás nem található.**-**Hiba! A hivatkozási forrás nem található.**. pont szerint – az adatvédelmi tisztviselőnek kell megküldeni, aki azt szakmai szempontból véleményezi. A jogos érdeken alapuló adatkezelés kizárólag az érdekmérlegelési teszt elvégzését és az adatvédelmi tisztviselő véleményének beszerzését követően kezdhető meg. A **Hiba! A hivatkozási forrás nem található.**. pont rendelkezéseit jelen esetben is alkalmazni kell.

50. Az érdekmérlegelési teszt módszertanát, a megválaszolandó kérdéseket minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani, az alábbi kérdések köre csak orientáló, a tervezett adatkezelés szempontjából releváns egyéb kérdésekkel bővíthető. Abból kell kiindulni, hogy bármilyen adatkezelés beavatkozás az érintett magánszférájába és e beavatkozás jogosságát, szükségességét és arányosságát kell bizonyítani.

51. Az érdekmérlegelési teszt részei:

a/ a tervezett adatkezelés leírása és az annak keretében kezelni tervezett személyes adatok meghatározása,

b/ az adatkezelő vagy azon harmadik fél jogos érdekének azonosítása, akinek az adatkezelés érdekében áll (Miért szükséges az adatkezelés?),

c/ az érintett érdekeinek, jogainak azonosítása (Arányban van-e az adatkezelés az érintett magánszférájának korlátozásával?),

d/ az adatkezelő (vagy harmadik fél) és az érintettek érdekeinek összevetése,

e/ az adatkezelés biztosítékainak leírása,

f/ az érdekmérlegelési teszt eredménye.

5.5. Az adatvédelmi hatásvizsgálat elvégzésének módszertana

52. Ha az adatkezelés valamely, különösen új technológiákat alkalmazó típusa valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve az adatkezelést megelőzően hatásvizsgálatot kell végezni. Olyan egymással hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló kockázatokat jelentenek, egyetlen adatvédelmi hatásvizsgálat (továbbiakban hatásvizsgálat) keretei között is értékelhetők.

53. A hatásvizsgálat elvégzésének szükségességéről a tervezett adatkezelésért felelős szervezeti egység adatkezelési megbízottja szükség esetén kikéri az adatvédelmi tisztviselő véleményét.

54. A hatásvizsgálat elvégzését a tervezett adatkezelésért felelős szervezeti egység adatkezelési megbízottja koordinálja a **Hiba! A hivatkozási forrás nem található.**. pont **Hiba! A hivatkozási forrás nem található.** alpontja szerinti módon. A hatásvizsgálat megállapításait írásban kell rögzíteni. Az elkészült hatásvizsgálati dokumentációt az adatvédelmi tisztviselőnek kell megküldeni, amely azt 8 munkanapon belül szakmai szempontból véleményezi és beszerzi az információbiztonsági szakterület véleményét is. Ha az adatkezelési megbízott az adatvédelmi tisztviselővel közösen úgy ítéli meg, hogy az adatkezelés nem jár magas kockázattal, úgy meg kell indokolnia és dokumentumokkal igazolnia a mellőzés okait. A **Hiba! A hivatkozási forrás nem található.**. pont rendelkezéseit jelen esetben is alkalmazni kell. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

55. Adatvédelmi hatásvizsgálatot a GDPR 35. cikk (3) bekezdésében, illetve a Nemzeti Adatvédelmi és Információszabadság Hatóság által közzétett jegyzékben (https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf) szereplő adatkezelések, adatkezelési műveletek esetén kell végezni.

56. A fenti eseteken túl minden olyan bevezetésre kerülő – különösen az új technológiákat alkalmazó – adatkezelés esetén is hatásvizsgálatot kell végezni, mely adatkezelés az ügyfélre tekintettel jelentős joghatással bír/az ügyfelet jelentős mértékben érinti.

57. A hatásvizsgálat módszertanát minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani. Egy lehetséges módszertant alkalmazó szoftver található a Nemzeti Adatvédelmi és Információszabadság Hatóság honlapján

(https://naih.hu/adatvedelmi hatasvizsgalati-szoftver.html).

58. A hatásvizsgálat első részében összefoglalóan le kell írni a tervezett adatkezelést, különösen: a/ az adatkezelésért felelős szervezeti egységet és a tervezett adatfeldolgozó megjelölését; b/ az adatkezelés jogalapját, célját (az adatkezeléstől várt előnyöket, az adatkezelés szükségességét), terjedelmét (időben és a kezelt adatok volumenében);
c/ az adatkezeléssel érintettek körét, a kezelendő adatok körét, az adatok megőrzésének tervezett idejét,
d/ azon adatkezelők megjelölését, akiknek az adatot továbbítani tervezik, és különösen, ha harmadik országba vagy nemzetközi szervezet felé tervezik az adattovábbítást; e/ az adatkezelésre vonatkozó követelmények (jogszabályi követelmények vagy magatartási kódexből, szabványból eredő követelmények);
f/ az adatkezelés folyamatának a leírását.

59. A hatásvizsgálat második részében ki kell fejteni és meg kell indokolni
a/ az adatkezelés szükségességének és arányosságának garanciáit,
b/ az érintett jogait biztosító garanciák érvényesülését.

60. A hatásvizsgálat harmadik részében azonosítani és értékelni kell az adatkezelés potenciális kockázatait, és a kockázatok enyhítésére tervezett, elfogadott intézkedéseket, megoldásokat.

61. A hatásvizsgálat negyedik része tartalmazza a tervezett adatkezelés értékelését: a/ a **Hiba! A hivatkozási forrás nem található.**-**Hiba! A hivatkozási forrás nem található.**. pontban meghatározott szempontok értékelését a tekintetben, hogy azok egyenként megfelelőek, további intézkedésekkel megfelelőek lehetnek, illetve nem megfelelőek; b/ a tervezett kiegészítő intézkedések végrehajtásának ütemtervét;
c/ annak egyértelmű rögzítését, hogy a tervezett adatkezelés valószínűsíthetően magas kockázattal jár-e a természetes személyek jogaira nézve, és ennek alapján az adatkezelés megkezdhető-e, illetve szükség van-e az adatvédelmi felügyeleti hatósággal való konzultációra.

62. A hatásvizsgálat megállapításait az adatkezelési tevékenységbe vissza kell csatolni és ennek megfelelően kell kialakítani az adatkezelést.

63. A hatásvizsgálatot legalább háromévente felül kell vizsgálni, szükség esetén újra el kell végezni.

6. az érintetti jogok gyakorlásának elősegítése

6.1. Az adatkezelési tevékenység nyilvánossága

64. Az Intézmény a honlapján egy olyan, „Adatvédelem” nevű oldalt tart fenn, amely bármely oldalról közvetlenül elérhető. Az „Adatvédelem” oldalon közzé kell tenni: a/ az Intézmény általános adatkezelési tájékoztatóját;
b/ az Intézmény egyes adatkezelési tevékenységeihez kapcsolódó (különös) adatkezelési tájékoztatók, ide nem értve a munkavállalók, egyéb jogviszonyban foglalkoztatottak

adatainak kezelésére vonatkozó tájékoztatókat;

c/ közös adatkezelés esetén a közös adatkezelésben résztvevők közötti megállapodás lényegét, ha azt a különös adatkezelési tájékoztatók nem tartalmazzák;

d/ tájékoztatást arról, hogy az érintett kihez fordulhat az adatkezelést érintő kérdéseivel, panaszaival (az adatkezelő és az adatvédelmi tisztviselő elérhetősége, az adatvédelmi felügyeleti hatóság elérhetősége).

65. Az Intézmény honlapjának olyan aloldalain, amelyek személyes adatok kezelésével járó egyes tevékenységekről tájékoztatnak (pl. egyes ellátási formák igénybevételének feltételeit tartalmazzák), el kell helyezni legalább az adott tevékenységhez kapcsolódó a/ adatkezelési tájékoztatóra mutató hivatkozást;

b/ egyéb releváns dokumentumokat (pl. betegtájékoztatókat, formanyomtatványokat).

66. Az Intézmény az Állami Egészségügyi Ellátó Központ Adatkezelési megbízásából kidolgozott mintadokumentumok Intézményre adaptált változatát alkalmazza a tevékenysége során.

67. Az Intézmény szervezeti egységeinek vezetői gondoskodnak arról, hogy a szervezeti egység tevékenységeinek helyszínén az Intézmény általános adatkezelési tájékoztatóján kívül az adott szervezeti egység tevékenységi körébe tartozó adatkezelésekről szóló (különös) adatkezelési tájékoztatók kinyomtatott formában is rendelkezésre álljanak.

68. Az Intézmény kezelésében lévő közérdekű adatok közzétételéről, illetve rendelkezésre bocsátásáról külön szabályzat rendelkezik.

6.2. A gyermekek tájékoztatáshoz való jogának biztosítása

69. Az Intézményi adatkezelési megbízottak gondoskodnak arról, hogy az Intézményben kezelt vagy az intézménnyel más módon kapcsolatba kerülő gyermekek az adataik kezelésével kapcsolatos tájékoztatást a gyermek számára világos és elérhető módon megkapják. A tájékoztatás az alábbi módokon történhet:

a/ a gyermek törvényes képviselője útján: a gyermeket érintő adatkezelésről a gyermekkel az Intézmény részéről kapcsolatba lépő személy írásban tájékoztatja a gyermek törvényes képviselőjét, és írásban nyilatkoztatja arra vonatkozóan, hogy a tájékoztatást közli a gyermekkel;

b/ a gyermek vagy a törvényes képviselő kifejezett kérésére a gyermekkel az Intézmény részéről kapcsolatba lépő személy – a fentieken túlmenően – biztosítja a gyermek részére a rövid, szóbeli tájékoztatást is az adatai kezelésével kapcsolatban;

c/ amennyiben a gyermek életkora és érettsége lehetővé teszi, a gyermekkel az Intézmény részéről kapcsolatba lépő személy írásban közvetlenül a gyermeket is tájékoztatja az adatkezelésről. A speciális, gyermekeknek szóló tájékoztató dokumentumot az adatvédelmi tisztviselő készíti el az Intézmény szervezeti egységeinek adatkezelési megbízottjai bevonásával. A különböző életkorú gyermekek számára a gyerekek életkorához igazodó tartalmú tájékoztató anyagot kell készíteni.

6.3. Korlátozottan cselekvőképes és cselekvőképtelen (gondokság alatt álló) személyek tájékoztatáshoz való jogának biztosítása

70. Az Intézmény szervezeti egységeinek adatkezelési megbízottai gondoskodnak arról, hogy az Intézményben kezelt korlátozottan cselekvőképes vagy cselekvőképtelen nagykorú

személyek törvényes képviselői, illetve – állapotától függően – a korlátozottan cselekvőképes személy is megfelelő tájékoztatást kapjanak a személyes adatok kezeléséről. A törvényes képviselőt írásban nyilatkoztatni kell, hogy a tájékoztatást közli a gondnokság alatt álló érintettel.

6.4. Gyermekek és gondokság alatt álló személyek személyes adatainak kezelése hozzájáruló nyilatkozat alapján

71. Az Intézmény szervezeti egységeinek adatkezelési megbízottai közreműködésével gondoskodnak arról, hogy az Intézményben kezelt vagy az Intézménnyel más módon kapcsolatba kerülő gyermekek, illetve gondnokság alatt álló személyek tekintetében – amennyiben az adatkezelés hozzájáruláson alapul – a személyes adatok kezeléséhez való hozzájárulást törvényes képviselőjük adja meg.

72. A hozzájáruló nyilatkozatnak tartalmaznia kell a törvényes képviselőnek arra vonatkozó nyilatkozatát, hogy jogosult az érintett helyett a jognyilatkozat megtételére.

73. Amennyiben az érintett törvényes képviselői (pl.: szülői felügyelet gyakorlására jogosult szülők) eltérő nyilatkozatot tesznek az adatkezeléshez való hozzájárulásról, úgy az adatkezeléshez való hozzájárulást meg nem adottnak kell tekinteni.

6.5. Hozzátartozók tájékoztatása

74. Az Intézmény szervezeti egységeinek adatkezelési megbízottai gondoskodnak arról, hogy az Intézményben kezelt vagy az Intézménnyel más módon kapcsolatba kerülő személyek hozzátartozóit az adatvédelmi szabályoknak megfelelően tájékoztassák, amelyben – az érintett személy képességeit is figyelembe véve – magát az érintettet is bevonhatja.

75. A hozzátartozók adatainak kezelését önálló adatkezelési tevékenységként kell feltüntetni az adatkezelési tevékenységek között, és az adatkezelési tájékoztatóban ki kell térni a hozzátartozók adatainak kezelésére.

7. Az érintettől származó kérelmek, panaszok megválaszolásának rendje

7.1. Az adatvédelmi bejelentések típusai

76. Az érintettől a következő, személyes adatai Intézmény általi kezelését érintő beadványok érkezhetnek:
a/ bejelentheti az Intézmény által nyilvántartott adatok megváltozását; b/ tájékoztatást kérhet személyes adatai kezeléséről [milyen személyes adato(ka)t milyen célból, milyen jogalapon, milyen forrásból szerezve meddig kezeli az Intézmény, alkalmaz-e automatizált döntéshozatalt és/vagy profilalkotást az adatkezelés során, és a személyes adatokat kinek, milyen jogalapon továbbítja)] – hozzáféréshez való jog (GDPR 15. cikk);
c/ kérheti pontatlanul nyilvántartott személyes adatai helyesbítését, illetve vitathatja a nyilvántartott személyes adatok pontosságát – helyesbítéshez való jog (GDPR 16. cikk); d/ kérheti nyilvántartott személyes adatai törlését – törléshez való jog (GDPR 17. cikk); e/ kérheti személyes adatai kezelésének korlátozását (a pontatlan adat helyesbítéséig terjedő időre; a jogellenesen kezelt személyes adatok törlése helyett; jogszerűen kezelt, de

szükségtelenné vált adatok törlése helyett az érintett kérésére az érintett jogi igényének előterjesztéséhez, érvényesítéséhez vagy védelméhez; jogos érdeken alapuló adatkezelés elleni tiltakozás elbírálásáig) – az adatkezelés korlátozásához való jog (GDPR 18. cikk);

f/ kérheti, hogy a rá vonatkozó, általa az Intézmény rendelkezésére bocsátott és elektronikus adatbázisban kezelt adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja – adathordozhatósághoz való jog (GDPR 20. cikk);

g/ tiltakozhat személyes adatai kezelése ellen, ha az adatkezelés jogalapja az adatkezelő vagy harmadik személy jogos érdeke, illetve közérdekű feladat vagy közfeladat ellátása, beleértve mindkét esetben a profilalkotást is – tiltakozási jog gyakorlása (GDPR 21. cikk);

h/ automatizált döntéshozatal alkalmazása esetén az adatkezelő részéről emberi beavatkozást kérhet, közölheti álláspontját [GDPR 22. cikk (3) bek.];

i/ kifogást nyújthat be az automatizált döntéshozatal alkalmazásával meghozott döntéssel szemben [GDPR 22. cikk (3) bek.];

j/ panaszt nyújthat be a személyes adatok kezelését, illetve a GDPR szerinti jogaik gyakorlását érintően [GDPR 77. cikk, 38. cikk (4) bek.];

k/ az elhunyt érintett életében tett meghatalmazottjaként vagy közeli hozzátartozójaként gyakorolni kívánja az érintett egyes jogait [Infotv. 25. §].

7.2. Az adatvédelmi beadványok kezelésének eljárásrendje

77. Az egyes belső szabályzatoknak az érintettek adatainak felvételére, módosítására vagy helyesbítésére, illetve törlésére vonatkozó rendelkezései alkalmazását jelen szabályzat nem érinti, az adatvédelmi tisztviselő azonban bármely esetben – az érintett beadványának kivizsgálása, illetve saját ellenőrzése eredményeként, továbbá az adatvédelmi felügyeleti hatóság vagy bíróság döntése végrehajtásaként – az említett szabályzatokban meghatározott hatásköri és eljárási rendtől függetlenül kezdeményezheti személyes adat helyesbítését, törlését vagy az adatkezelés korlátozását (zárolást).

78. Az Intézmény-hez érkező, a **Hiba! A hivatkozási forrás nem található.**. pontban meghatározott beadványokat az Intézmény Panaszkivizsgálási Szabályzatban foglaltaknak megfelelően kell – a GDPR 12. cikkében írt határidők figyelembevételével – elintézni, az alábbi kiegészítésekkel és eltérésekkel:

a/ a beadvány érkezése dátumát és időpontját pontosan rögzíteni kell;

b/ a **Hiba! A hivatkozási forrás nem található.**. pont **Hiba! A hivatkozási forrás nem található.** alpontban meghatározott panasz kivizsgálását az adatvédelmi tisztviselő végzi. A panasz kivizsgálása során az érintett szervezeti egységek kötelesek az adatvédelmi tisztviselővel együttműködni. A személyes adatok kezelését, illetve a GDPR szerinti jogok gyakorlását érintő panasz megalapozottsága esetén az adatvédelmi tisztviselő az adatkezelésért felelős szervezeti egység(ek)nél intézkedést kezdeményez a panasz kiváltó okainak orvoslására, az érintett folyamatok felülvizsgálatára, valamint – szükség esetén – a személyi felelősség megállapítására,

c/ a Főigazgatói Titkárság és a Betegfelvételi Iroda bármely beadvány esetén kérheti az adatvédelmi tisztviselő véleményét a tekintetben, hogy a beadvány a **Hiba! A hivatkozási forrás nem található.**. pontban meghatározott tárgyú-e, illetve, hogy az érintett kérte-e az adatkezelés korlátozását [zárolás, GDPR 18. cikk – lsd. **Hiba! A hivatkozási forrás nem található.**. pont **Hiba! A hivatkozási forrás nem található.** alpont], és kérés esetén az adatvédelmi tisztviselő – az informatikai szakterület útján – intézkedik annak az

informatikai rendszerekben történő megvalósításáról. Az adatkezelés korlátozásának (zárolásának) feloldásáról az adatvédelmi tisztviselő külön tájékoztatja az érintett informatikai rendszer(eke)t üzemeltető szervezet egység(ek)et,

d/ az adatvédelmi tisztviselő dönt abban a kérdésben, hogy a **Hiba! A hivatkozási forrás nem található.**. pontban meghatározott tárgyú beadvány egyértelműen megalapozatlan vagy túlzó-e,

e/ az érintettnek saját adatairól szóbeli tájékoztatás csak egyértelmű azonosítás után lehetséges. Amennyiben a beadványozó nem azonosítható vagy kétség merül fel a beadványozó személyazonosságát illetően, meg kell megkísérelni a beadványozó személyének azonosítását, beleértve a személyes megjelenés igénylését. Ilyen esetekben a GDPR 12. cikk (3) bekezdése szerinti határidő a beadványozó sikeres azonosításakor kezdődik;

f/ amennyiben a beadvány a GDPR hatálya alá tartozó beadványnak minősül, a beadványozót a beadvány érkezését követő 8 napon belül értesíteni kell a beadvány

érkezéséről, a megválaszolására nyitva álló határidőről, illetve arról, hol kaphat további felvilágosítást a beadványáról. Nem kell ilyen értesítést küldeni a beadványozónak, ha a beadványban kért intézkedést ezen időn belül teljesítik;

g/ amennyiben a beadványt előreláthatóan nem lehet a GDPR 12. cikk (3) bekezdése szerinti határidőben megválaszolni, a beadványozót legkésőbb a beadvány érkezését követő 21. napon elküldött levélben vagy elektronikus üzenetben tájékoztatni kell a határidő meghosszabbításának szükségességéről, okairól és az új határidőről;

h/ amennyiben a beadványt – a beadványozó kérelme ellenére – nem lehet, vagy nem célszerű elektronikus úton megválaszolni (a kért dokumentumokat nem lehet vagy nem célszerű ilyen úton elküldeni), fel kell venni a kapcsolatot a beadványozóval annak érdekében, hogy kölcsönösen elfogadható megoldást találjanak. Különösen indokolt a beadványozóval a kapcsolatfelvétel, ha a beadványozó egészségügyi adat megküldését kéri elektronikus úton. A kapcsolatfelvételre olyan időben kell sort keríteni, hogy a beadványt akkor is meg lehessen válaszolni, ha a beadványozó ragaszkodik az elektronikus úthoz;

i/ elektronikus úton egészségügyi adat csak a beadványozó kifejezett kérésére és csak oly módon küldhető, ha előzőleg a beadványozó figyelmét felhívták a kockázatokra és a beadványozó ezek után megerősíti a szándékát, egyúttal tudomásul véve az Intézmény felelősségkizáró nyilatkozatát, továbbá az adatok bizalmassága, integritása és rendelkezésre állása biztosítható (pl. jelszavas védelemmel ellátott file, ahol a jelszót külön csatornán küldik el).

j/ az Intézmény szervezeti egységei a **Hiba! A hivatkozási forrás nem található.**. pontban meghatározott tárgyú ügyekben készített válaszlevél-tervezetét jóváhagyás végett bemutatják az adatvédelmi tisztviselőnek;

k/ a beadvány határidőben megválaszoltnak minősül, ha a válaszadásra köteles szervezeti egység a választ a határidő utolsó napján postára adja vagy elektronikus üzenetet küld a beadványozónak a megtett intézkedésekről.

79. Az adatvédelmi beadványokról olyan ügyiratnyilvántartást kell vezetni, amely segítségével bármikor egyértelműen azonosíthatók a **Hiba! A hivatkozási forrás nem található.**. pont szerinti beadványok, nyomon követhetők a beadványok elintézése során tett intézkedések, és a rendelkezésre álló adatokból bármikor statisztika készíthető a következő szempontok szerint:

a/ adott időszakban érkezett beadványok száma, típus szerinti bontásban is;

b/ a beadványok beérkezésének módja;
c/ a beadványok megválaszolásának átlagos időtartama;
d/ az elutasított beadványok száma, és azok okai;
e/ a válaszadás módja.

8. Az adatbiztonsági intézkedések (technikai és szervezési intézkedések) meghatározása és végrehajtása

80. Az adatbiztonsági szabályok kialakítása során különös gondot kell fordítani a beépített és az alapértelmezett adatvédelem elveinek (GDPR 25. cikk) betartására, valamint arra, hogy az Intézmény által alkalmazott adatbiztonsági intézkedések megfeleljenek a GDPR 32. cikkében írt követelményeknek.

81. Az Intézmény működése során betartandó adatbiztonsági szabályokat (GDPR 32. cikk) külön szabályzatok tartalmazzák, így különösen a mindenkor hatályos
a/ Adatvédelmi és Adatbiztonsági Szabályzat
b/ Szervezeti Integritást Sértő Események Kezelésének Eljárásrendje

82. Az adatbiztonsági szabályok tervezetének kialakításába – a véleményezésre vonatkozó egyéb szabályokat nem érintve – az adatvédelmi tisztviselőt be kell vonni.

83. Az adatbiztonsági intézkedéseket érintően az adatkezelésért felelős szervezeti egység adatkezelési megbízottja:
a/ a szakterületére vonatkozó információk szolgáltatásával közreműködik az érintett informatikai elemek védelmi osztályokba sorolásában;
b/ a szakterületére vonatkozó információk szolgáltatásával közreműködik az adatkezelés biztonságát fenyegető kockázatok felmérésében és meghatározásában;
c/ az informatikai rendszert üzemeltető szervezeti egységgel együttműködve közreműködik azon információbiztonságot érintő feladatok végrehajtásában, amelyek az adatbiztonsági követelmények megvalósulásához szükségesek;
d/ figyelemmel kíséri a belső adatvédelmi szabályok érvényre juttatását a szakterületen belül, felhívja a szakterületen dolgozók figyelmét a szabályok betartására, jelzi a szabályok megsértését az érintett munkavállaló felettesének, közreműködik a szakterületen dolgozók adatvédelmi tudatosságának növelésében.

84. Az adatbiztonság elveinek egy adatkezelés (lsd. **Hiba! A hivatkozási forrás nem található.**. pont) bevezetésének vagy személyes adatkezelést és/vagy -feldolgozást eredményező módosításának előkészítése során történő érvényesítése az informatikai szakterület vezetőjének feladata, akit az adatkezelési tevékenységet támogató nyilvántartási rendszerek kifejlesztésének, módosításának folyamatába kötelezően be kell vonni (lsd. **Hiba! A hivatkozási forrás nem található.**. pont).

85. Az adatbiztonsági intézkedések mindennapi működésben történő betartására az Intézmény minden alkalmazottja, valamint az Intézmény informatikai rendszereihez hozzáférő személy köteles.

9. A közös adatkezelői és az adatfeldolgozói szerződések megkötésének és végrehajtása ellenőrzésének szabályai

9.1. Közös adatkezelés

86. Közös adatkezelésnek minősül, ha az adatkezelés céljait és eszközeit az Intézmény egy vagy több másik adatkezelővel közösen határozza meg (GDPR 26. cikk).

87. A közös adatkezelésről szóló megállapodásban meg kell határozni különösen

a/ az adatkezelés célját, a kezelendő adatok körét, az adatkezelés időtartamát, az alkalmazandó adatbiztonsági intézkedéseket, az adatkezelés egyéb feltételeit, b/ azt, hogy a közös adatkezelésben érintett egyes adatkezelők

ba/mely adatkezelési műveleteket (pl. hozzájáruló nyilatkozatok felvétele, adatok tárolása, adatok felhasználása stb.) végzik,

bb/az érintett tájékoztatását hogyan végzik (pl. melyik adatkezelő készíti el az adatkezelési tájékoztatót és bocsátja az érintettek rendelkezésére stb.),

bc/ az érintett jogai gyakorlását hogyan biztosítják (pl. egyesített vagy elkülönített ügyfélszolgálat stb.),

bd/az esetleges jogellenes adatkezelés következményeit milyen arányban viselik; c/ az adatvédelmi incidens észlelése esetén követendő eljárást, különösen azt, hogy ca/ az adatvédelmi incidens tudomásra jutása esetén a másik adatkezelő adatvédelmi tisztviselőjét (adatvédelmi tisztviselő hiányában a kijelölt kapcsolattartót) haladéktalanul kötelesek értesíteni az adatvédelmi rendellenességről vagy incidensről,

cb/ egymással kötelesek együttműködni az adatvédelmi rendellenesség vagy incidens okának kiderítésében és következményeinek felszámolásában,

cc/ az egyes adatkezelőket mely adatvédelmi incidensek tekintetében terheli a bejelentési kötelezettség;

d/ kijelölnek-e kapcsolattartót az érintettek számára, és ha igen, a kapcsolattartó személyét és elérhetőségét naprakészen kell tartani,

e/ a megállapodásról az érintett rendelkezésére bocsátandó összefoglalót, aminek – a GDPR 13-14. cikkeiben írtakon túl – tartalmaznia kell az adatkezelők által végzett adatkezelési műveleteket, és azt, hogy az érintett hogyan gyakorolhatja jogait a közös adatkezelés tekintetében.

88. A közös adatkezelés szükségességét az adatkezelési megbízott az adatkezelés bevezetéséről való döntés előkészítése részeként az adatvédelmi tisztviselővel közösen [**Hiba! A hivatkozási forrás nem található.**. pont **Hiba! A hivatkozási forrás nem található.** alpont] vizsgálja meg.

89. Amennyiben a közös adatkezelésben érintett másik adatkezelő harmadik országbeli adatkezelő, először abban a kérdésben kell dönteni – a **Hiba! A hivatkozási forrás nem**

található.. fejezet megfelelő alkalmazásával –, hogy a harmadik országbeli adatkezelő képes-e a GDPR-nak megfelelő adatbiztonsági követelmények teljesítésére. Amennyiben a harmadik országbeli adatkezelő nem képes a GDPR által elvárt adatbiztonsági követelmények érvényesítésére, illetve nem tud a GDPR szerinti garanciákat nyújtani a személyes adatok kezelésére, az adatkezelővel nem köthető megállapodás közös adatkezelésre.

90. Amennyiben döntés születik a közös adatkezelés bevezetéséről, az illetékes adatkezelési megbízott(ak), az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselővel és egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a jogtanácsos bevonásával, továbbá az informatikai szakterülettel együttműködve közösen előkészíti a közös adatkezelésről szóló megállapodás tervezetét (benne a közös adatkezelőknek az érintettek számára kijelölendő kapcsolattartójának kijelölésével kapcsolatos döntést, valamint a közös adatkezelésre vonatkozó megállapodásnak az érintettek rendelkezésére bocsátható lényegi elemeit) és azt felterjeszti a szerződés megkötésére jogosult személynek.

91. A **Hiba! A hivatkozási forrás nem található.**. pont alkalmazásában a szerződés megkötésére jogosult személy az, aki – az Intézmény Szervezeti és Működési Szabályzata szerint – az érintett adatkezelés alapjául szolgáló tevékenységgel kapcsolatban döntésre jogosult, illetve – amennyiben a döntés testületi hatáskörbe tartozik – a testületi döntés előkészítéséért felelős. E szabály nem érinti az együttes aláírásra vonatkozó szabályokat.

92. Az adatkezelési megbízott a közös adatkezelői megállapodás megkötését követően e tényt és a további adatkezelő(k) adatait (név és cím, kapcsolattartó neve és elérhetősége) megküldi az adatvédelmi tisztviselőnek, aki az információkat rögzíti az Adatkezelési Nyilvántartásban.

9.2. Adatfeldolgozói szerződések

93. Amennyiben harmadik országbeli adatfeldolgozó igénybevétele merül fel, először abban a kérdésben kell dönteni – a **Hiba! A hivatkozási forrás nem található.**. fejezet megfelelő alkalmazásával –, hogy a harmadik országbeli adatfeldolgozó képes-e a GDPR-nak megfelelő adatbiztonsági követelmények teljesítésére. Amennyiben a harmadik országbeli adatfeldolgozó nem képes a GDPR által elvárt adatbiztonsági követelmények érvényesítésére, illetve nem tud a GDPR szerinti garanciákat nyújtani a személyes adatok kezelésére, az adatfeldolgozóval nem köthető szerződés.

94. Adatfeldolgozó igénybevétele esetén az adatfeldolgozóval kötendő szerződésnek tartalmaznia kell a GDPR 28. cikk (1)-(4) bekezdésében foglalt tartalmi elemeket a **Hiba! A hivatkozási forrás nem található.**. pontban foglalt kiegészítések és pontosítások szerint.

95. Az adatfeldolgozóval kötendő szerződésben

a/ a kellő részletességgel (pl. szabályzatra vagy szabványokra utalással) meg kell határozni az adatfeldolgozó, vagy az adatfeldolgozó által igénybe veendő további adatfeldolgozó (al-adatfeldolgozó) által betartandó adatbiztonsági szabályokat, amelyek nem lehetnek kevésbé szigorúak, mint az Intézmény által alkalmazott adatbiztonsági intézkedések, és az adatfeldolgozónak az adatbiztonsági intézkedések végrehajtásával kapcsolatos feladatait;

b/ rögzíteni kell az adatfeldolgozónak az érintettől származó kérelmek, panaszok megválaszolásában való közreműködésének eljárásrendjét;

c/ rögzíteni kell az adatfeldolgozó kötelezettségeit adatvédelmi incidens észlelése esetén, így különösen

ca/ az adatvédelmi incidens tudomásra jutása esetén az Intézmény adatvédelmi tisztviselőjét haladéktalanul köteles értesíteni az adatvédelmi incidensről, cb/ köteles együttműködni az Intézmény adatvédelmi tisztviselőjével és más

közreműködő szervezeti egységgel az adatvédelmi incidens okának feltárásban és következményeinek felszámolásában,

cc/ köteles együttműködni az adatvédelmi incidens bejelentésének teljesítésében,

d/ rögzíteni kell az adatfeldolgozó kötelezettségét az adatvédelmi hatásvizsgálat elvégzésében, illetve a hatásvizsgálatban azonosított kockázatok alakulásának figyelemmel kísérésében, az adatkezeléssel járó kockázatok változásának jelzésében, illetve az adatvédelmi hatásvizsgálatok utóellenőrzésben.

96. Az adatfeldolgozó igénybevételének szükségességét az adatkezelési megbízott az adatkezelés bevezetéséről való döntés előkészítése részeként [**Hiba! A hivatkozási forrás nem található.**. pont **Hiba! A hivatkozási forrás nem található.** pont] vizsgálja meg. Ezt a szabályt kell alkalmazni akkor is, ha az adatfeldolgozó igénybevételéről az adatkezelés folyamán születik döntés.

97. Az adatbiztonsági intézkedések megfelelőségének megítélése az informatikai szakterület hatáskörébe tartozik, beleértve azt is, hogy az adatfeldolgozó által egy magatartási kódexhez vagy tanúsítási mechanizmushoz való csatlakozás elegendő garanciát jelent-e az adatbiztonsági szabályok megfelelőségére.

98. Amennyiben döntés születik az adatfeldolgozó igénybevételéről, az adatkezelési megbízott az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselővel és egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a jogtanácsos bevonásával, továbbá informatikai szakterülettel együttműködve közösen előkészíti az adatfeldolgozóval kötendő szerződés tervezetét és azt felterjeszti a szerződés megkötésére a **Hiba! A hivatkozási forrás nem található.**. pont szerint jogosult személynek.

99. Az adatkezelési megbízott az adatfeldolgozói szerződés megkötését követően az adatfeldolgozó adatait (név és cím, kapcsolattartó neve és elérhetősége) megküldi az adatvédelmi tisztviselőnek, aki az információkat rögzíti az Adatkezelési Nyilvántartásban.

100. A **Hiba! A hivatkozási forrás nem található.**.-**Hiba! A hivatkozási forrás nem található.**. pont rendelkezéseit al-adatfeldolgozó igénybevétele esetén is megfelelően alkalmazni kell azzal, hogy az al-adatfeldolgozó igénybevételére vonatkozó hozzájáruló nyilatkozatnak az adatfeldolgozói szerződés megkötésre jogosult személy általi kiadása előtt az adatkezelési megbízott kikéri az adatvédelmi tisztviselő és rajta keresztül a jogtanácsos, továbbá az informatikai szakterület véleményét is.

10. Az Adatkezelési Nyilvántartás

101. Az adatvédelmi tisztviselő vezeti az Adatkezelési Nyilvántartást. Az Adatkezelési Nyilvántartás valamennyi, az Intézmény általi adatkezelés esetén tartalmazza: a/ az adatkezelés célját,

b/ az adatkezelés jogalapját,

c/ az érintettek körét,

d/ az érintettekre vonatkozó adatok leírását,

e/ az adatok forrását,

f/ az adatok kezelésének időtartamát,

g/ a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló, valamint nemzetközi szervezethez történő adattovábbításokat is, h/ az

adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét, i/ az alkalmazott adatfeldolgozási technológia jellegét;

j/ az adatkezelő szervezeti egység megnevezését,

k/ az adatkezelésért felelős szervezeti egység vezetője, az adatokhoz hozzáférésre jogosult személyek köre (munkakör),

l/ az adatkezelés módszere (manuális, számítógépes, vegyes),

m/ adatbiztonsági intézkedések, archiválás módja, gyakorisága, adattörlés ideje. n/ a kockázati besorolást.

102. Az Adatkezelési Nyilvántartás célja az Intézmény mint adatkezelő adatkezelési tevékenysége átláthatóságának biztosítása, és ezzel az esetleges felesleges, párhuzamos adatkezelések elkerülése.

103. Az adatvédelmi tisztviselő az Adatkezelési Nyilvántartásba való betekintést – a Hatóság képviselőin kívül – az Intézmény érintett szakterületei részére biztosítja.

104. Az adatkezelési megbízott az új adatkezelés bevezetését az adatkezelés megkezdése előtt 5 munkanappal bejelenti az adatvédelmi tisztviselőnek [vö. **Hiba! A hivatkozási forrás nem található.**. pont **Hiba! A hivatkozási forrás nem található.** alpont], aki azt az Adatkezelési Nyilvántartásba bejegyzi.

105. Az adatkezelési nyilvántartásba bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelési megbízott 5 munkanapon belül köteles bejelenteni az

adatvédelmi tisztviselőnek [vö. **Hiba! A hivatkozási forrás nem található.**. pont], aki ennek megfelelően módosítja az Adatkezelési Nyilvántartás adatait.

106. Az Adatkezelési Nyilvántartással összefüggésben az adatvédelmi tisztviselő: a/ biztosítja, hogy az adatkezelések bevezetését megelőző döntéselőkészítés során az érintett szakterületek az adatkezelési tevékenységek nyilvántartása adatait megismerhessék a felesleges, párhuzamos adatkezelések elkerülése, illetve az új adatkezelésnek a meglévő adatkezelésekhez való illeszkedése érdekében; b/ ellenőrzi az adatkezelések, illetve adatfeldolgozás adatainak az Adatkezelési Nyilvántartásba történő rögzítését és jelzi az adatkezelésért felelős szervezeti egység vezetőjének a hiányos, hibás vagy valószínűleg megváltozott adatokat, információkat; c/ a jogtanácsossal együttműködve figyelemmel kíséri az adatkezelést érintő jogszabályok változását és a szükséges módosításokra felhívja az adatkezelési megbízottak figyelmét; d/ az adatvédelmi felügyeleti hatóság megkeresésére adatot szolgáltat az Adatkezelési Nyilvántartásból.

11. Az adatvédelmi incidensek kezelése

11.1. Az adatvédelmi incidens minősítése

107. Adatvédelmi incidens csak akkor következik be, ha az adatbiztonsági intézkedések [**Hiba! A hivatkozási forrás nem található.**. fejezet] – akár vétlen, akár szándékos – megsértésének következtében bekövetkezik a személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés:

a/ súlyos incidens: olyan incidens (pl. adatvesztés, adatsérülés), mely valószínűsíthetően

magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve (pl.: a jogosulatlan hozzáféréssel érintett adatok esete; az olyan adatsérülés, adatvesztés, amelynél az adatok naplózott állományból nem állíthatóak helyre). Magas kockázatúnak minősül az az eset, amely fizikai, vagyoni vagy nem vagyoni károkat okozhat az érintetteknek, pl. az érintetteknek a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, pénzügyi veszteséget, jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok integritásának, illetve bizalmas jellegének sérülését eredményezheti,

b/ enyhe incidens: minden incidens, amely nem tartozik az a) pont alá (pl. átmeneti szolgáltatásleállás, -kiesés az Intézmény munkavállalói által használt olyan belső rendszerekben, amely nem jár adatsérüléssel vagy adatvesztéssel).

108. Az adatvédelmi incidensre vonatkozó szabályokat kell alkalmazni az Intézmény tulajdonát képező adathordozón, mobiltelefonon, laptopon, egyéb számítástechnikai eszközön tárolt adatokra, továbbá az Intézmény alkalmazottainak olyan saját tulajdonú

eszközein (adathordozó, mobiltelefon, laptop, egyéb számítástechnikai eszköz) tárolt adatokra, amely eszközöket munkavégzéshez, munkaköri feladatok ellátásához, hivatalos célból használhat. Az adatvédelmi incidensre vonatkozó szabályokat az Intézmény birtokában lévő papíralapú adathordozón lévő adatokra is alkalmazni kell.

109. Az elektronikus információs rendszereket érintő (biztonsági vagy egyéb) események adatvédelmi incidensnek is minősülnek, amennyiben személyes adatokra nézve következik be. A jelen Szabályzatnak az adatvédelmi incidens kezelésére vonatkozó rendelkezéseinek alkalmazása nem mentesít az elektronikus információs rendszerek érintő (biztonsági vagy egyéb) események kezelésére (bejelentésére, kivizsgálására stb.) vonatkozó szabályok betartása alól, azaz az elektronikus információs rendszereket érintő (biztonsági vagy egyéb) események kezelésére vonatkozó szabályokat jelen Szabályzat előírásaival párhuzamosan alkalmazni kell.

11.2. Az adatvédelmi incidens bejelentése

110. Az Intézmény irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező azon természetes személy (a munkavégzésre irányuló jogviszony jellegétől függetlenül), aki az Intézmény által kezelt vagy feldolgozott személyes adatokkal kapcsolatban, vagy az Intézmény szerződéses partnere által kezelt vagy feldolgozott személyes adataival kapcsolatban adatvédelmi incidenst vagy annak gyanúját észleli, köteles azt haladéktalanul bejelenteni az adatvédelmi tisztviselőnek a dpo@szivkorhaz.hu e-mail címen, vagy az intraneten erre a célra létrehozott űrlapot kitölteni, vagy az alábbi telefonszámon: 06 87 584 505. Az előbbieken túli egyéb bejelentő az Intézmény elektronikus elérhetőségén vagy az Intézmény honlapján elérhető űrlap kitöltésével jelentheti be az adatvédelmi incidenst.

111. Amennyiben az adatvédelmi incidens bejelentése szóban (telefonon vagy személyesen) történik (beleértve az Intézmény telefonos elérhetőségein tett közérdekű bejelentéseket is), azt a szóbeli közlést követő legfeljebb 1 napon belül – a **Hiba! A hivatkozási forrás nem található.**. pontban írottak figyelembevételével – írásban is meg kell erősíteni. Ilyen esetben a szóbeli közlés időpontját külön fel kell tüntetni.

112. Az adatvédelmi incidensről szóló bejelentésben ismertetni kell az adatvédelmi incidens

jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az adatvédelmi incidenssel érintett személyes adatok kategóriáit és hozzávetőleges számát, továbbá a bejelentő nevét és elérhetőségét.

113. A közös adatkezelésről szóló szerződésben [GDPR 26. cikk], illetve az adatfeldolgozóval kötendő szerződésben [GDPR 28. cikk] egyértelműen rendelkezni kell a másik adatkezelő, illetve az adatfeldolgozó azon kötelezettségéről, hogy az adatvédelmi incidensről az Intézményt a **Hiba! A hivatkozási forrás nem található.**. pontban meghatározott, adatvédelmi tisztviselő elérhetőségén köteles haladéktalanul, de legkésőbb az észlelést követő 24 órán belül értesíteni írásban és telefonon is. A szerződésnek tartalmaznia kell

továbbá a közös adatkezelő, illetve az adatfeldolgozó kötelezettségeit adatvédelmi incidens bejelentésében és kivizsgálásában [lsd. **Hiba! A hivatkozási forrás nem található.** pont].

11.3. Incidensprotokoll általában

114. Az érintett szakterület bevonásával a riasztásokban szereplő incidens gyanús esemény kezelésekor a következők szerint kell eljárni:

a/ figyelembe kell venni a különböző biztonsági szabályozásokban az incidens- gyanús események elhárítására vonatkozó rendelkezéseket;

b/ amennyiben a riasztás személyes adatot tartalmazó alkalmazás sérülékenységével kapcsolatban keletkezett, az incidens elhárítását végző személy az adatvédelmi tisztviselőt haladéktalanul tájékoztatja;

c/ amennyiben az Intézmény rendelkezik automatizált módszerrel az adott sérülés (incidens) elhárítására, akkor azt azzal az eszközzel azonnal el kell kezdeni; d/ ha az Intézmény – a mindenkor hatályos Adatvédelmi és Adatbiztonsági Szabályzatában, továbbá a Szervezeti Integritást Sértő Események Kezelésének Eljárásrendjében foglaltakkal összhangban – nem rendelkezik automatizált módszerrel az adott sérülés (incidens) elhárítására, akkor azt manuális módon kell azonnal elkezdeni;

e/ amennyiben a sérülés elhárítása belső erőforrásból nem kivitelezhető, akkor külső szakértőket kell bevonni az elhárítás folyamatába.

115. A nem papíralapon kezelt adattal kapcsolatos incidensek kezelésére az Intézmény mindenkor Adatvédelmi és Adatbiztonsági Szabályzatában, továbbá a Szervezeti Integritást Sértő Események Kezelésének Eljárásrendjében foglaltak is irányadóak. A papíralapon kezelt iratokkal kapcsolatban a jelen Szabályzat személyi hatálya alá tartozó személyek kötelesek a személyes adatokat tartalmazó iratokat a munkavégzés befejezését követően, ahol ennek feltételei biztosítottak, zárható szekrényben, zárral ellátott fiókban tárolni. Ahol a tárolás előbb nevesített feltételei nem adottak, az irodahelyiség ajtajának kulcsra zárásával kell a személyes adatok védelmét biztosítani abban az esetben, ha az irodahelyiségben senki sem tartózkodik. A Szabályzat személyi hatálya alá tartozó személyek kötelesek az Intézmény egyéb belső szabályzatai, így különösen az iratkezelés rendjéről, illetve a biztonsági előírásokról szóló mindenkor hatályos belső szabályzatnak megfelelően eljárni.

11.4. Az adatvédelmi incidens kivizsgálása

116. Adatvédelmi incidens (papíralapú és nem papíralapú adatokra vonatkozóak egyaránt) felmerülése esetén az Intézmény adatvédelmi tisztviselője a jogtanácsos és az informatikai szakterület, továbbá szükség esetén az adott szakterületért felelős szervezeti egység kijelölt

munkatársának (a továbbiakban együtt: incidensvizsgáló bizottság) közreműködésével megvizsgálja, és a **Hiba! A hivatkozási forrás nem található.**. pont szerint kategorizálja a bekövetkezett incidenst és meghatározza az esetleges elhárítás érdekében szükséges

további intézkedéseket. A bejelentőt – szükség esetén – további információk közlésére kell felkérni. Az incidensvizsgáló bizottságot az adatvédelmi tisztviselő hívja össze, az említett személyeknek szükség esetén munkaidőn kívül is rendelkezésre kell állniuk. Az incidensvizsgáló bizottság munkáját az adatvédelmi tisztviselő koordinálja, és képviseli az Intézmény egyéb szervezeti egységei felé.

117. Az incidensvizsgáló bizottság üléseiről emlékeztetőt, döntéseiről indoklást is tartalmazó jegyzőkönyvet, vizsgálatairól pedig intézkedési javaslatokat is tartalmazó jelentést kell készíteni. Az incidensvizsgáló bizottság munkáját tartalmazó dokumentumok kezelésére az Intézmény mindenkori iratkezelési szabályai az irányadók. Az incidensvizsgáló bizottság korlátozhatja a munkájáról szóló dokumentumokba betekintők körét.

118. Az adatvédelmi incidensről az adatvédelmi tisztviselő értesíti a főigazgatót, az orvos igazgatót, ápolási igazgatót, a gazdasági igazgatót, és az IT vezetőt

119. A bejelentés előzetes megvizsgálása során az alábbi szempontokat kell figyelembe venni:
a/ a bejelentés személyes adatot érint-e,
b/ amennyiben a bejelentés személyes adatot érint, megállapítható-e a személyes adatok köre,
c/ megállapítható-e az incidensben érintett személyek köre,
d/ a hatályos jogszabályok és belső szabályok alapján megállapítható-e, hogy személyes adat jogellenes kezelése vagy feldolgozása (beleértve a törlést/megsemmisítést is) történt,
e/ az incidens valószínűsíthetően magas kockázattal jár-e az érintettek jogaira és szabadságaira nézve,
f/ melyek az adatvédelmi incidensből eredő, valószínűsíthető következmények, g/ az Intézmény által alkalmazott technikai és szervezési védelmi intézkedések az incidensben érintett személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik-e az adatokat.

120. Ha a bejelentés előzetes megvizsgálása azzal az eredménnyel jár, hogy az elektronikus információs rendszereket érintő (biztonsági vagy egyéb) esemény nem érintett személyes adatokat, akkor a vizsgálatot az Intézmény mindenkor hatályos Adatvédelmi és Adatbiztonsági Szabályzatában, illetve a Szervezeti Integritást Sértő Események Kezelésének Eljárásrendjében, és a további, biztonsági előírásokat tartalmazó szabályokban foglaltak szerint kell folytatni.

121. Az incidensvizsgáló bizottság – az adatvédelmi tisztviselő útján – legkésőbb az incidens bejelentés vagy az incidensről való tudomásszerzés közül a korábbi időpontot követő 1 napon belül tájékoztatja a következő személyeket az előzetes vizsgálat eredményéről, a GDPR 33. cikkében írt hatósági bejelentés szükségességéről, az érintettek tájékoztatásának szükségességéről és módjáról, valamint arról, hogy szükséges-e az incidens részletes vizsgálata:
a/ az Intézmény főigazgatóját;

b/ informatikai rendszert is érintő incidens esetén az informatikai szakterület vezetőjét;
c/ a szakmailag illetékes szervezeti egység vezetőjét.

122. Az incidensvizsgáló bizottság javaslata alapján a főigazgató legkésőbb a bizottság javaslatának kézhezvételét követő 1 napon belül dönt a GDPR 33. cikkében írt adatvédelmi felügyeleti hatósági bejelentés szükségességéről. A főigazgató döntéséről az adatvédelmi tisztviselő értesíti a **Hiba! A hivatkozási forrás nem található.**. pontban meghatározott egyéb személyeket.

123. Az adatvédelmi incidens részletes vizsgálatának szükségességéről az incidensvizsgáló bizottság dönt. A részletes vizsgálatot a vizsgálat megkezdése után a lehető leghamarabb le kell zárni.

124. A vizsgálat során elsősorban az alábbi módszerek alkalmazhatóak: a/ személyes megbeszélés az adatvédelmi incidenst észlelő személyekkel, valamint az érintett szervezeti egységek munkatársaival és vezetőivel,
b/ írásbeli tájékoztatás kérése az érintett szervezeti egységektől,
c/ dokumentumok vizsgálata,
d/ informatikai rendszerek, hálózatok és eszközök vizsgálata, beleértve a naplóállományok vizsgálatát is.

125. Amennyiben az incidensvizsgáló bizottság a részletes vizsgálat során úgy ítéli meg, hogy azonnali intézkedések szükségesek annak biztosítására, hogy az adatvédelmi incidenssel azonos problémaforrásból eredő incidens a jövőben ne valósuljon meg, úgy a szükséges intézkedések megtétele érdekében haladéktalanul tájékoztatja az érintett szervezeti egységek vezetőit.

126. Az incidensvizsgáló bizottság a részletes vizsgálat megállapításairól, illetve a javasolt intézkedésekről a részletes vizsgálat befejezését követő 2 munkanapon belül vizsgálati jelentést készít. A vizsgálati jelentés tartalmazza az adatvédelmi incidens elhárításához és további incidens megelőzéséhez szükséges intézkedésekre vonatkozó, az illetékes vezető részére tett javaslatot is.

127. A részletes vizsgálatról szóló jelentést a **Hiba! A hivatkozási forrás nem található.**. pont a/-c/ alpontjában említett vezetőknek kell megküldeni.

128. A jelentés alapján a vizsgálatban érintett szervezeti egységek vezetői 15 napon belül a megvalósításhoz szükséges határidőre tett javaslatot is tartalmazó intézkedési tervet készítenek és azt megküldik az adatvédelmi tisztviselő útján az incidensvizsgáló bizottságnak.

129. Az intézkedési tervet és a megvalósításhoz szükséges határidőt tartalmazó szakterületi javaslatot az incidensvizsgáló bizottság a kézhezvételtől számított 3 munkanapon belül véleményezi, majd jóváhagyásra megküldi a főigazgató részére.

130. Az adatvédelmi incidens elhárítása és a további incidensek megelőzése céljából megvalósított egyes intézkedésekről az incidenssel érintett szervezeti egység vezetője tájékoztatást küld az adatvédelmi tisztviselő részére.

131. Az adatvédelmi tisztviselő az intézkedési tervben foglaltak végrehajtásáról, az összes intézkedés befejezését követő 3 munkanapon belül tájékoztatást küld a főigazgató részére.

11.5. Az érintett tájékoztatása a súlyos adatvédelmi incidensről

132. Súlyos adatvédelmi incidens esetén az Intézmény – az érintettel kapcsolatban rendelkezésére álló elérhetőségeken, ennek hiányában vagy alkalmazásuk lehetetlensége esetén (vö. GDPR 34. cikk) az Intézmény honlapján közzétett közlemény útján – indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. Az érintettek tájékoztatásának módjára az incidensvizsgáló bizottság javaslatot tesz. Az érintettek tájékoztatását – az érintett szervezeti egységek bevonásával – az adatvédelmi tisztviselő koordinálja.

133. Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az alábbi információkat és intézkedéseket:

a/ az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

b/ az adatvédelmi incidensből eredő, valószínűsíthető következményeket; c/ az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

134. Az érintettet nem kell tájékoztatni, amennyiben az incidens nem jár magas kockázattal, és a következő feltételek bármelyike teljesül:

a/ az Intézmény megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;

b/ az Intézmény az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az említett magas kockázat a továbbiakban valószínűsíthetően nem áll fenn;

c/ a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

135. Az Intézmény főigazgatójának döntése alapján az Intézmény az érintetteket az Intézmény honlapján vagy országos lefedettségű sajtótermékben közzétett hirdetmény útján is értesítheti.

11.6. Az adatvédelmi incidens bejelentése a Hatóságnak

136. Az adatvédelmi incidensről szóló bejelentést a Hatóság mindenkori kapcsolati pontjára kell eljuttatni.

137. A bejelentés összeállításának és beadásának felelőse az adatvédelmi tisztviselő. Az adatvédelmi incidensről szóló bejelentéshez szükséges információkat az adatvédelmi tisztviselő rendelkezésére kell bocsátani.

138. Az adatvédelmi incidensről szóló bejelentésben legalább:

a/ ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek

kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

b/ közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

c/ ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket; d/ ismertetni kell az Intézmény által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

139. Ha nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később (pl. a **Hiba! A hivatkozási forrás nem található.**. pont szerinti jóváhagyás után haladéktalanul) részletekben is közölhetők.

11.7. Az adatvédelmi és egyéb incidensek nyilvántartása

140. Az adatvédelmi incidensekről az adatvédelmi tisztviselő nyilvántartást vezet. E szabályzat nem érinti az egyéb jogszabályok szerint a biztonsági események kezelésével kapcsolatban vezetendő nyilvántartásokra vonatkozó szabályok alkalmazását.

141. A nyilvántartásban rögzíteni kell:

a/ az incidensben érintett személyes adatok körét; és számát,

b/ az adatvédelmi incidenssel érintettek körét, és számát,

c/ az adatvédelmi incidens tudomásszerzés időpontját,

d/ az adatvédelmi incidens körülményeit, hatásait,

e/ az adatvédelmi incidens elhárítására megtett intézkedéseket,

f/ az adatvédelmi incidenssel kapcsolatban adott tájékoztatások adatait.

142. Az Intézmény az adatvédelmi incidens kivizsgálásával kapcsolatos papíralapú és elektronikus dokumentumokat 10 évig köteles megőrizni. Az adatvédelmi incidensek