# GOTTSEGEN GYÖRGY
# ORSZÁGOS KARDIOLÓGIAI INTÉZET

# SZABÁLYZAT

## Adatkezelési és adatvédelmi szabályzat

| | | | | |
|---|---|---|---|---|
| **Készítette:** | **Nagy István<br>informatikai osztályvezető** | **2020.06.17<br>dátum** | **Dokumentum kódja:** | **SZ11** |
| | | | **Változatok száma:** | **6** |
| | | | **Oldalak száma:** | **57** |
| **Jóváhagyta:** | **Dr. Andréka Péter<br>mb. főigazgató főorvos** | **2020.06.22<br>dátum** | **Mellékletek száma:** | **6** |
| | | | **Érvénybelépés időpontja:** | **2020.06.22** |
| **Minőségügyi szempontból ellenőrizte:** | **Dohnál Erika<br>kontrolling, finanszírozási és minőségirányítási igazgató** | **2020.06.22<br>dátum** | **Felülvizsgálat időpontja:** | |

**MÓDOSÍTÁSOK JEGYZÉKE**

| Módosította Aláírás/dátum | Változat száma | Módosított oldalszám | Jóváhagyta Aláírás/dátum | Kibocsátás időpontja |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Az egyes példányok birtokosait a szétosztási lista tartalmazza sorszám szerint.**

### TARTALOMJEGYZÉK

## Tartalom

# I. ÁLTALÁNOS RÉSZ

## 1. A szabályzat célja

Jelen Belső adatvédelmi szabályzat (a továbbiakban: Szabályzat) célja, hogy biztosítsa a Gottsegen György Országos Kardiológiai Intézet (a továbbiakban: Intézmény) tevékenysége során

a) a személyes adatok védelméhez fűződő jog érvényesülését, a személyes adatok védelme elveinek érvényesülését,
b) az Intézmény szervezeti egységeinél vezetett, személyes adatokat tartalmazó nyilvántartások vezetésének és működtetésének jogszerű rendjét,
c) az adatbiztonsági követelmények (technikai és szervezési intézkedések) érvényesülését.

A Szabályzat meghatározza az Intézmény adatvédelmi tevékenysége irányításában és ellátásában résztvevő szervezeti egységeknek és személyeknek az adatkezelési tevékenységek ellátása során ellátandó feladatait.

A Szabályzat rendelkezéseit a Szabályzat tárgyi hatálya alá eső valamennyi adatkezelés (3. pont) során figyelembe kell venni.

Jelen Szabályzatnak az alábbi szabályzatok elválaszthatatlan részei:

- a mindenkor hatályos Vírusvédelmi szabályzat
- a mindenkor hatályos Iratkezelési szabályzat
- a mindenkor hatályos Incidenskezelési szabályzat

## 2. A szabályzat személyi hatálya

Jelen Szabályzat személyi hatálya kiterjed az Intézmény irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyekre (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 (adatfeldolgozók) esetén az erre a jogviszonyra az Intézmény által kötött szerződésben 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) 28. cikkének megfelelően rendelkezni kell arról, hogy az Intézmény által megbízott adatfeldolgozó a feladata ellátása során hogyan juttatja érvényre jelen Szabályzat rendelkezéseit.

## 3. A szabályzat tárgyi hatálya

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 4. pontjában felsorolt jogszabályok és az Intézmény belső szabályzatai szerint;
b) az egészségügyi ellátáson kívüli ügyfélkapcsolati jellegű adatkezelést valósítanak meg (az Intézménnyel kapcsolatba lépni szándékozó, kapcsolatban álló vagy kapcsolatban állt személyek, beleértve ezek meghatalmazottjait, képviselőit is);
c) foglalkoztatási jogviszonyhoz kapcsolódó adatkezelést valósítanak meg [az Intézménnyel közalkalmazotti jogviszonyban, munkaviszonyban vagy egyéb foglalkoztatási jogviszonyban (együtt: foglalkoztatási jogviszony) álló, állt, vagy foglalkoztatási jogviszonyba lépni szándékozó személyek) az adataira vonatkoznak.
d) az Intézménnyel szerződéses kapcsolatban álló társaságok képviselőinek, kapcsolattartóinak az adataira vonatkoznak.

## 4. Jogszabályi háttér

Az Intézmény adatkezelési tevékenységét megszabó jogszabályok különösen:

1. 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 (GDPR);
2. az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek (Infotv.) a GDPR hatálya alá eső adatkezelésekre alkalmazandó rendelkezései (lásd. Infotv. 2. § (2) bek.);
3. az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997 évi XLVII törvény (Eüak.);
4. az egészségügyről szóló 1997. évi CLIV. törvény (Eütv.);
5. az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről szóló 62/1997. (XII.21.) NM rendelet;
6. a kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény;
7. az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról szóló 39/2016.(XII. 21.) EMMI rendelet;
8. 2013. évi V. törvény a Polgári Törvénykönyvről (Ptk.)
9. a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996 évi XX. törvény;
10. a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény (Kjt.), és annak az egészségügyi ágazatban történő végrehajtására vonatkozó jogszabályok;
11. a Munka Törvénykönyvéről szóló 2012. évi I. törvény (Mt.).

Az Intézmény adatkezelési tevékenységével összefüggő speciális belső szabályzatok:

a) Incidenskezelési szabályzat (kiegészítve Jelen szabályzat 4.számú mellékletében találhatóü iratmintákkal)

b) A Gottsegen György Országos Kardiológiai Intézet informatikai eszközeinek és elektronikus levelező rendszerének használata

c) Vírusvédelmi szabályzat

d) GOKI Számítástechnikai vészhelyzetek intézkedési terve

e) Az intézet területén működő informatikai rendszerek adatvédelmi és adatmentési leírása az Infotörvény és a GDPR rendelet alapján

A Szabályzat hatálya alá tartozó személyek kötelesek az olyan tevékenységük során, amely szükségszerűen együtt jár személyes adatok kezelésével, az adott tevékenységre vonatkozó – az előző bekezdésben felsorolt – speciális belső 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.

## 5. Értelmező rendelkezések

**Adatállomány:** az egy nyilvántartásban kezelt adatok összessége[1];

**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;

**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[2];

**Adatkezelésért felelős szervezeti egység:** az Intézmény azon szervezeti egysége, amelynek feladatkörébe tartozik az Intézmény kezelésében lévő valamely nyilvántartási rendszer létrehozása, fenntartása, illetve üzemeltetése;

**Adatkezelő**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;[3]

**Adatkezelési Nyilvántartás:** jelen Szabályzat 18. pontjában meghatározott adattartalmú, folyamatosan karbantartott nyilvántartás;

**Adattovábbítás**: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele[4]

**Adattörlés**: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges [5]

[1] Infotv. 3. § 21. pont
[2] GDPR 4. cikk 2. pont
[3] GDPR 4. cikk 7. pont
[4] Infotv. 3. § 11. pont
[5] Infotv. 3. § 13. pont

Néhány esetben (pl. bíróság döntés) lehet adatokat fizikailag is törölni egy rendszerből. Ilyen esetekben szükséges egy üres „place-holder" elemet tárolni a hierarchiának ezen a pontján, hogy jelezze a törlést és azt, hogy az mikor és miért történt.

- Fizikai törlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk nem lehetséges.
- Logikai törlés: téves adatbevitel esetén lehetséges az adatokat logikailag törölni. A törlés ebben az esetben nem jelenti az adatok megsemmisülését. A törölt adatok, a törlés ténye, oka és az ehhez kapcsolódó adatok tárolásra kerülnek (ki, hol és miért). A törölt adatok, mint egy előző verzió az arra jogosultak számára elérhetőek.

**Adatvédelmi felügyeleti hatóság:** a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság);

**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;

**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.;

**Adatmegsemmisítés***:* az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése[6];

**Adatfeldolgozás:** az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége[7];

**Adatfeldolgozó:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel [8];

**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

[6] Infotv. 3. § 11. pont

[8] GDPR 4. cikk 8. pont

adatkezelésért felelős szervezeti egység felelősségi körébe tartozó részében gondoskodik az adatkezelőt terhelő feladatok elvégzéséről,

**Adatvédelem:** az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó olyan előírások, amelyek adatkezelések, adathozzáférések és adatfelhasználások jogszerűségeit szabályozzák;

**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;

**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[9];

**Beteg:** az egészségügyi szolgáltatásokat igénybe vevő vagy abban részesülő személy;[10]

**Betegellátó**: a kezelést végző orvos, az egészségügyi szakdolgozó, az érintett gyógykezelésével kapcsolatos tevékenységet végző egyéb személy, a gyógyszerész;[11]

**Bűnügyi személyes adat***:* a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;[12]

**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;

**Diagnosztikai vizsgálat:** az egészségügyi szolgáltatóhoz forduló beteg panasza okának feltárására irányuló vizsgálat[13]

**Dolgozói személyes adat:** az Intézménnyel foglalkoztatási jogviszonyban álló személyek adata;

**EGT állam:** az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam

[9] GDPR 4. cikk 5. pont
[10] Eütv. 3. § a) pont
[11] Eüak. 3. § g) pont
[12] Infotv. 3. § 4. pont
[13] Eütv. 3. § kb) pont

között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez[14]

**Egészségügyi adat:** egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

**Egészségügyi dokumentáció**: a gyógykezelés során a betegellátó tudomására jutott egészségügyi és személyazonosító adatokat tartalmazó feljegyzés(ek), nyilvántartás(ok), vagy bármilyen más módon rögzített adat vagy multimédiás információ, függetlenül annak hordozójától vagy formájától[15];

**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;[16]

**Egészségügyi ellátás***:* a beteg adott egészségi állapotához kapcsolódó egészségügyi szolgáltatások összessége;[17]

**Egészségügyi szolgáltató**: a tulajdoni formától és a fenntartótól függetlenül minden, egészségügyi szolgáltatás nyújtására az egészségügyi hatóság által kiadott működési engedély alapján jogosult jogi személy, jogi személyiség nélküli szervezet és minden olyan természetes személy, aki a szolgáltatást saját nevében nyújtja;[18]

**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;

**Érintett:** azonosított vagy azonosítható természetes személy; [19]

**Genetikai adat:** egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered;[20]

**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

[14] Infotv.3. § 23. pont
[15] Eütv. 3. § p) pont, és az Eüak. 3. § e) pont
[16] Eütv. 3. § d) pont
[17] Eütv. 3. § c) pont
[18] Eütv. 3. § f) pont
[19] GDPR 4. cikk 1. pont
[20] Infotv. 3. § 3a pont

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;[21]

**Harmadik fél:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;[22]

**Harmadik ország***:* minden olyan állam, amely nem EGT-állam;[23]

**Hozzájárulás:** az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;[24]

**Informatikai szakterület:** az informatikai rendszerek üzemeltetéséért, az informatikai biztonság ellátásáért felelős szervezeti egység vagy egységek, ideértve az Intézmény információbiztonsági felelősét is;

**Kezelést végző orvos**: a beteg adott betegségével, illetve egészségi állapotával kapcsolatos vizsgálati és terápiás tervet meghatározó, valamint ezek keretében beavatkozásokat végző orvos, aki a beteg gyógykezeléséért felelősséggel tartozik vagy abban közreműködő orvos (pl.: konzílium, telemedicina, stb.);[25].

**Kezelőorvos:** a beteg adott betegségével, illetve egészségi állapotával kapcsolatos vizsgálati és terápiás tervet meghatározó, továbbá ezek keretében beavatkozásokat végző orvos, illetve orvosok, akik a beteg gyógykezeléséért felelősséggel tartoznak;[26]

**Közeli hozzátartozó**: a házastárs, az egyeneságbeli rokon, az örökbe fogadott, a mostoha- és nevelt gyermek, az örökbe fogadó, a mostoha- és nevelőszülő, valamint a testvér és az élettárs[27];

**Közérdekű adat**: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat[28];

[21] Eüak. 3. § c) pont
[22] GDPR 4. cikk 10. pont
[23] Infotv. 3.§ 24. pont
[24] GDPR 4. cikk 11. pont
[25] Eüak. 3. § f) pont
[26] Eütv. 3. § b) pont
[27] Eütv. 3. § r) pont, Eüak.3. § j) pont
[28] Infotv. 3. § 5. pont

**Közérdekből nyilvános adat:** a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli[29];

**Közvetett adattovábbítás:** személyes adatnak valamely harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbítása útján valamely más harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítása;

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

**Nemzetközi szervezet:** a nemzetközi közjog hatálya alá tartozó szervezet és annak alárendelt szervei, továbbá olyan egyéb szerv, amelyet két vagy több állam közötti megállapodás hozott létre, vagy amely ilyen megállapodás alapján jött létre,

**Nyilvánosságra hozatal**: az adat bárki számára történő hozzáférhetővé tétele[30];

**Orvosi titok:** a gyógykezelés során az adatkezelő tudomására jutott egészségügyi és személyazonosító adat(ok), továbbá a szükséges, vagy folyamatban lévő, illetve befejezett gyógykezelésre vonatkozó, valamint a gyógykezeléssel kapcsolatban megismert egyéb adat.
Orvosi titok nem csak orvosnak juthat tudomására, illetve nem csak orvos kezelhet. Az orvosi titok megőrzése a jogszabály által előírt kivételektől eltekintve minden esetben kötelező[31];

**Sürgős szükség**: az egészségi állapotban hirtelen bekövetkezett olyan változás, amelynek bekövetkeztében azonnali egészségügyi ellátás hiányában az érintett közvetlen életveszélybe kerülne, illetve súlyos vagy maradandó egészségkárosodást szenvedne,[32]

**Személyes adat**: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;[33].

**Személyazonosító adat** (egészségügyi adat kezelése esetén): az olyan, 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

[29] Infotv. 3. § 6. pont
[30] Infotv. 3. § 12. pont
[31] Eüak. 3. § d) pont
[32] Eütv. 3. § i) pont, Eüak. 3. § k) pont
[33] GDPR 1. cikk 1. pont

egészségügyi dokumentáció részeként kezel ( családi és utóneve, születési családi és utóneve, születési helye, születési ideje és anyja születési családi és utóneve);[34]

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

**Titkosítás:** az adatok olyan átalakítása, melynek során az adat értelmezhetetlenné válik a megfelelő kulcs ismerete nélkül;

**Törlés:** az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása a továbbiakban már nem lehetséges. A törlés célja megvalósítható deperszonalizálással (anonimizálással) is;

## 6. Dokumentálási kötelezettség

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.

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.

## 7. Az adatvédelmi tevékenység szervezete és irányítása az Intézménynél

7.1. 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.

A főigazgató főorvos 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;

[34] 1996 évi XX. tv. 4. § 4) pont

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.

Az Intézmény szervezeti egységeinek vezetői az irányításuk alá tartozó szervezeti egység tekintetében:

a) betartják és betartatják az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírásokat; az adatvédelmi tisztviselővel, a jogi ügyekért felelős szervezeti egységgel, valamint az informatikai szakterülettel együttműködve gondoskodnak az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról;
b) kijelölik az irányításuk alá tartozó szervezeti egység adatkezelési megbízottját;
c) gondoskodnak arról, hogy az irányításuk alá tartozó szervezeti egységek felelősségi körébe tartozó nyilvántartási rendszerek naprakészek, megbízhatóak legyenek;
d) gondoskodnak arról, hogy az irányításuk alatt álló személyek az adatkezelés meghatározott feltételeinek megfelelően járjanak el [GDPR 32. cikk (4) bek.];
e) 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.

A sajtóval való kapcsolattartásért/ közönségkapcsolati feladatok ellátásáért felelős személy adatvédelmi incidens esetén közreműködik az érintettek tájékoztatásának módjáról és a tájékoztatás tartalmáról való döntés előkészítésében,

a) adatvédelmi incidens esetén – az adatvédelmi tisztviselő közreműködésével – szükség esetén sajtóközleményt bocsát ki és kizárólagos kapcsolatot tart a sajtó képviselőivel.

Az ügyfélkapcsolatokért működtetéséért felelős szervezeti egységek amely(ek) kérelmek, panaszok kivizsgálásáért felelős(ek) (igazgatói titkárságok, felnőtt és gyermek betegfelvételi irodák):

a) az adatvédelmi tisztviselő szükség szerinti közreműködésével ellátja az érintetti jogok gyakorlásával kapcsolatos beadványok megválaszolását a személyes adatok kezelését, illetve a GDPR szerinti jogaik gyakorlását érintő panaszok kivételével.

Az informatikai szakterület szervezeti egységei az Intézmény szervezeti és működési szabályzatában, valamint az Intézmény adatkezelési és adatvédelmi szabályzatában meghatározott feladatkörükben:

a) ellátják az informatikai biztonsági biztonsággal kapcsolatos feladatokat a folyamatos üzemeltetési feladatok kivételével, különösen az Intézmény adatkezelési és adatvédelmi szabályzatában meghatározott feladatokat;
b) ellátják 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 ellátják a személyes adatok kezelésével kapcsolatos technikai védelem megvalósítását, ellátják – az Intézmény adatkezelési és adatvédelmi szabályzatában meghatározott – hatáskörükbe tartozó információbiztonsági feladatokat, valamint rendelkezésre állási kontrollok biztosítását, a tárolt és továbbított személyes adatok bizalmasságának védelmét, az incidensfelderítési és -kezelési tevékenység támogatását,
d) az érintett szervezeti egységek vezetőivel együttműködve gondoskodnak az információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról.

A jogi ügyekért felelős személy:
a) szakmai támogatást nyújt az adatkezeléssel összefüggő, nem adatvédelmi jogszabályok értelmezésében,
b) az Intézmény belső szabályozók előkészítésére és kiadására vonatkozó szabályok szerint biztosítja, hogy az adatvédelmi tisztviselő véleményét kikérjék az Intézmény adatvédelmi tárgyú vagy adatvédelmi vonatkozású belső szabályzatainak előkészítése során,
c) 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.

Az osztályos adatkezeléssel megbízottak 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 adatkezelések nyilvántartásának 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 adatvagyon-felmérés elkészítésében,
h) közreműködik az Intézmény kezelésében lévő az adatok biztonsági osztályba sorolásában.

Adatkezelési megbízottat valamennyi a törvény és az ágazati magatartás kódex által előírt szintű szervezeti egységnél ki kell jelölni. Adatkezelési megbízottnak olyan személyt kell kijelölni, aki az adott szakterületet, üzleti/adminisztratív folyamato(ka)t, illetve – az informatikai szakterületen – a szakterületek tevékenységét támogató informatikai rendszereket illetően kellő ismeretekkel bír.

7.2. Az adatvédelmi tisztviselő

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/ jogi szakvizsgával vagy informatikai főiskolai (BSc) vagy egyetemi (MSc) szintű végzettséggel;
b/ az európai és hazai adatvédelemmel kapcsolatos főbb szabályozók, hatósági és bírósági határozatok, iránymutatások ismeretével;
c/ alapvető adatvédelmi és informatikai folyamatok ismeretével;
d/ legalább 10 év adatvédelmi területen szerzett gyakorlattal.

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

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 főigazgató főorvosnak tartozik felelősséggel.

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 – az Intézményi jogász és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – tartja a kapcsolatot.

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

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.

Az Intézményben nem lehet adatvédelmi tisztviselő az a természetes személy, aki az Intézményben az adatkezelési tevékenység céljainak, kereteinek, eszközeinek meghatározásáról

dönt, különösen a főigazgató főorvos, adatkezelésért felelős szervezeti egység vezetője (**Hiba! A hivatkozási forrás nem található.** pont) és a belső ellenőr.

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

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.

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 az Intézményi jogász bevonásával – a neki címzett panaszokat, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
d) az Intézményi jogásszal és az informatikai szakterülettel együttműködve elkészíti az adatvédelmi és adatbiztonsági szabályzatot;
e) az Intézményi jogásszal együttműködve gondoskodik az adatvédelmi ismeretek oktatásáról [elsősorban az intraneten közzétett segédanyagok útján];
f) az Intézményi jogásszal együttműködve személyes adatok kezelésére vonatkozó előírásokról tájékoztatást nyújt, tanácsot ad;
g) személyes adatot is kezelő új informatikai rendszer belső fejlesztéssel történő bevezetése során közreműködik az adatvédelmi hatásvizsgálatot lefolytatásában;
h) az adatvédelmi incidenskezeléssel kapcsolatban ellátja a jelen szabályzat szerinti feladatokat;
i) vezeti az Adatkezelési Nyilvántartást;
j) éves összefoglaló jelentést készít a főigazgató főorvosnak;
k) kapcsolatot tart és az Intézményi jogász és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – együttműködik a Hatósággal;
l) az Állami Egészségügyi Ellátó Központ számára adatszolgáltatást teljesít.

## 8. Adatkezelés bevezetésével, módosításával és megszüntetésével kapcsolatos feladatok

8.1. Adatkezelés bevezetésével kapcsolatos feladatok

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 a döntéselőkészítés rendjére vonatkozó belső szabályokat e fejezet rendelkezéseit figyelembe véve kell alkalmazni.

Adatkezelés bevezetése főigazgatói utasítással történik. A főigazgatói utasítás tartalmazza

a) az adatkezelésért felelős szervezeti egységnek és egyéb szervezeti egységeknek az adatkezeléssel kapcsolatos feladatait, így különösen:
   - az adatok felvételének, módosításának, törlésének rendje,
   - adatszolgáltatási kötelezettségek meghatározása az adatok naprakészen tartása érdekében,
   - a nyilvántartási rendszerből történő adattovábbítás, az ahhoz való hozzáférés rendje;
b) az adatkezelésre vonatkozó különös adatbiztonsági intézkedések meghatározása;
c) mellékletként
   - a GDPR-nak, az Infotv-nek és egyéb alkalmazandó jogszabálynak megfelelő adatkezelési tájékoztatót,
   - hozzájáruláson alapuló adatkezelés esetén a hozzájáruló nyilatkozat mintáját.

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

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 adatkezelési megbízottját/megbízottjait minden esetben be kell vonni a folyamatba. A fejlesztési igényt megfogalmazó szervezeti egység vezetője az egyéb területek adatkezelési megbízottjai bevonásának szükségességéről az érintett adatkezelési megbízottakat és az adatvédelmi tisztviselőt értesíti.

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

Az adatkezelés bevezetésével, az adatkezelés feltételeinek meghatározásával kapcsolatban a leendő adatkezelésért annak tárgya szerint felelős szakterület/szervezeti egység adatkezelési megbízottja (több érintett adatkezelési megbízott egymással együttműködve) 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), és ennek részeként

a) 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.];
b) amennyiben az adatkezelés jogalapja a jogos érdek lehet, elkészíti az érdekmérlegelési teszt dokumentumának tervezetét [GDPR 6. cikk (1) bek. f) pont];

c) az adatvédelmi tisztviselő véleményének kikérése után javaslatot tesz a döntésre jogosultnak adatvédelmi hatásvizsgálat elvégzésére; a döntésre jogosult erre vonatkozó pozitív döntése esetén – az informatikai fejlesztéseket, az informatikai architektúra tervezést, illetve az IT üzemeltetést végző szervezeti egységnél működő adatkezelési megbízott közreműködésével – elvégzi a hatásvizsgálatot, 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.];
d) előterjesztést tesz a döntésre jogosultnak arról, hogy az adatkezelést közös adatkezelésként indokolt-e ellátni, illetve indokolt-e adatfeldolgozót bevonni;
e) javaslatot tesz automatizált döntéshozatali módszer, illetve profilalkotási módszer alkalmazására [GDPR 22. cikk (1) bek.];
f) megszövegezi a hozzájáruló nyilatkozatot [GDPR 7. cikk (2) bek.], illetve a megfelelő szerződéses rendelkezéseket;
g) megfogalmazza az adatkezelésről szóló tájékoztatást (GDPR 13-14. cikk);
h) az informatikai szakterület közreműködésével gondoskodik az adatkezelésről szóló tájékoztatás könnyen hozzáférhető módon való közzétételéről [GDPR 12. cikk (1) bek.];
i) az adatkezelés bevezetéséről való döntést követően megküldi az adatvédelmi tisztviselőnek az új adatkezelésnek az Adatkezelési Nyilvántartásában történő rögzítéséhez szükséges információkat, illetve a nyilvántartott adatokban bekövetkezett valamennyi változást [GDPR 30. cikk (1) bek.]
j) amennyiben ennek szükségessége felmerül, egyedi esetben előterjesztést tesz a döntésre jogosultnak 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;
k) amennyiben ennek szükségessége felmerül, a 18. fejezet szabályait is figyelembe véve egyedi esetben előterjesztést tesz a döntésre jogosultnak arról, hogy személyes adatok harmadik országba továbbíthatók-e egyedi ügyekben [GDPR 49. cikk (1) bek.];

Az adatkezelés bevezetésével, az adatkezelés feltételeinek meghatározásával kapcsolatban az informatikai szakterület adatkezelési megbízottjai – szervezeti egységük feladatkörében – a személyes adatot kezelő rendszer fejlesztése és beszerzése során közreműködnek

a) a célhoz kötött adatkezelés és az adattakarékosság elvének megfelelően gyűjtött adatokra vonatkozóan a beépített és alapértelmezett adatvédelem elveinek dokumentált érvényesüléséről;
b) annak biztosításában, hogy az adathordozhatóság, adattörlés és adattisztítás célú módosítások szabályozott és dokumentált módon valósuljanak meg;
c) annak biztosításában, hogy az adatvédelmi tájékoztatók és nyilatkozatok könnyen elérhetők legyenek az ügyfelek számára,
d) annak biztosításában, hogy az adatkezeléssel kapcsolatos ügyfélrendelkezéseket visszakereshető formában tárolják;
e) 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;
f) az adott adatkezelés különös az Intézmény adatkezelési és adatvédelmi szabályzatában eltérő adatbiztonsági intézkedések meghatározásában;

g) az adatkezelés bevezetésével kapcsolatos – előző bekezdésben írt – döntések előkészítésében a feladatkörébe eső kérdésekben.

Az adatkezelés bevezetésével összefüggésben 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.

Az adatkezelés bevezetésével összefüggő döntések, javaslatok véglegesítése előtt ki kell kérni az adatvédelmi tisztviselő véleményét, úgy, hogy az adatvédelmi tisztviselőnek legalább 10 munkanapja legyen a vélemény adására.

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 az adatkezelések bevezetésével összefüggő egyéb döntési javaslatokat.

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 Intézet jogászának, valamint az informatikai szakterület véleményét;
b) megvizsgálja a véleményezésre megküldött dokumentumot/leírást
   - adatvédelmi jogi szempontból,
   - abból a szempontból, hogy azok milyen módon illeszthetők be az Intézmény informatikai rendszereibe, illetve nincs-e a tervezett adatkezeléssel azonos vagy hasonló adatkezelés.

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.

Az Intézet jogászának, valamint az informatikai szakterület a véleményét 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.

Amennyiben az adatkezelés feltételei kidolgozásában részt vevő adatkezelési megbízottak között véleményeltérés van, illetve az Intézet jogászának 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.

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.

8.2. Az adatkezelési megbízott feladatai az adatkezelés során

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 áttekinti a hatásvizsgálatban azonosított kockázatok alakulását, jelzi az adatvédelmi tisztviselőnek az adatkezeléssel járó kockázatok változását, közreműködik az adatvédelmi hatásvizsgálatok utóellenőrzésben [GDPR 35. cikk (11) bek.].

Az adatkezelés során (informatikai rendszerben kezelt adatok esetén az informatikai rendszer üzemeltetési szakaszában) az informatikai szakterület adatkezelési megbízottja(i) – a feladatkörükbe tartozó kérdésekben – gondoskodnak 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.

Amennyiben az adatkezelés feltételeinek módosítása válik szükségessé

a) megfelelően alkalmazni kell az adatkezelés bevezetésére vonatkozó rendelkezéseket (8.1. fejezet),
b) az adatkezelés megváltozott adatait – a változást elrendelő döntés után – át kell vezetni az Adatkezelési Nyilvántartásban.

8.3. Adatkezelés megszüntetésével kapcsolatos feladatok

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 tisztviselő és rajta keresztül az Intézeti jogász és az informatikai szakterület véleményének kikérése után – 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.

Az adatkezelés megszüntetésére vonatkozó döntés meghozatala során, illetve a döntés végrehajtása során:

a) megfelelően alkalmazni kell az adatkezelés bevezetésére vonatkozó rendelkezéseket (8.1. fejezet),
b) az Adatkezelési Nyilvántartásból az adatkezelést vagy az egyes adatfajtákat törölni kell,
c) az adatokat – attól függően, hogy az adatok archiválásáról vagy törléséről született döntés
   - az informatikai rendszerekben archiválni kell, illetve
   - az informatikai rendszerekből törölni kell, a papír alapú nyilvántartásban kezelt adatokat pedig – az Intézmény iratkezelési szabályzatáról szóló főigazgatói utasítás szerint – selejtezni kell.

## 9. Az érdekmérlegelési teszt elvégzésének módszertana

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.

Az érdekmérlegelési tesztet a tervezett adatkezelésért felelős szervezeti egység adatkezelési megbízottja végzi el. Az érdekmérlegelési tesztet írásban kell elvégezni. Az elkészült dokumentumot 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.

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.

Az érdekmérlegelési teszt részei:

- a tervezett adatkezelés leírása és az annak keretében kezelni tervezett személyes adatok meghatározása,
- az adatkezelő vagy azon harmadik fél jogos érdekének azonosítása, akinek az adatkezelés érdekében áll (Miért szükséges az adatkezelés?),
- az érintett érdekeinek, jogainak azonosítása (Arányban van-e az adatkezelés az érintett magánszférájának korlátozásával?),

- az adatkezelő (vagy harmadik fél) és az érintettek érdekeinek összevetése,
- az adatkezelés biztosítékainak leírása,
- az érdekmérlegelési teszt eredménye.

## 10. Az adatvédelmi hatásvizsgálat elvégzésének módszertana

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.

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

A hatásvizsgálat elvégzését a tervezett adatkezelésért felelős szervezeti egység adatkezelési megbízottja koordinálja. 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 úgy ítéli meg, hogy az adatkezelés nem jár magas kockázattal, úgy meg kell indokolnia és dokumentumokkal igazolnia a mellőzés okait. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

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.

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.

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).

A hatásvizsgálat első részében összefoglalóan le kell írni a tervezett adatkezelést, különösen:

- az adatkezelésért felelős szervezeti egységet és a tervezett adatfeldolgozó megjelölését;
- az adatkezelés jogalapját, célját (az adatkezeléstől várt előnyöket, az adatkezelés szükségességét), terjedelmét (időben és a kezelt adatok volumenében);
- az adatkezeléssel érintettek körét, a kezelendő adatok körét, az adatok megőrzésének tervezett idejét,
- azon adatkezelők megjelölését, akiknek az adatot továbbítani tervezik, és különösen, ha harmadik országba vagy nemzetközi szervezet felé tervezik az adattovábbítást;
- az adatkezelésre vonatkozó követelmények (jogszabályi követelmények vagy magatartási kódexből, szabványból eredő követelmények);

- az adatkezelés folyamatának a leírását.

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

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

A hatásvizsgálat negyedik része tartalmazza a tervezett adatkezelés értékelését:
a szempontok értékelését a tekintetben, hogy azok egyenként megfelelőek, további intézkedésekkel megfelelőek lehetnek, illetve nem megfelelőek;
a tervezett kiegészítő intézkedések végrehajtásának ütemtervét;
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.

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

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

## 11. Az adatkezelési tevékenység nyilvánossága

Az Intézmény a honlapján egy olyan, „Adatvédelem” nevű oldalt tart fenn, amely bármely oldalról közvetlenül elérhető. Az „Adatvédelem” oldalon közzé kell tenni:

a) Adatvédelmi alapadatok
b) Adatkezelési kérdésekkel kapcsolatos tájékoztató
c) Adatkezelési és védelmi tájékoztató
d) Adatkezelési Tájékoztatás a honlapon keresztül történő kapcsolatfelvételhez kapcsolódóan
e) Tájékoztató az EESZT-n keresztül megvalósuló adattovábbításról
f) az Intézet egyes adatkezelési tevékenységeihez kapcsolódó (különös) adatkezelési tájékoztatók, ide nem értve a munkavállalók, egyéb jogviszonyban foglalkoztatottak adatainak kezelésére vonatkozó tájékoztatókat;
g) közös adatkezelés esetén a közös adatkezelésben résztvevők közötti megállapodás lényegét, ha azt a különös adatkezelési tájékoztatók nem tartalmazzák;
h) tájékoztatást arról, hogy az érintett kihez fordulhat az adatkezelést érintő kérdéseivel, panaszaival (az adatkezelő és az adatvédelmi tisztviselő elérhetősége, az adatvédelmi felügyeleti hatóság elérhetősége).

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).

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 amennyiben létezik ilyen.

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

## 12. Az érintettől származó kérelmek, panaszok megválaszolásának rendje

12.1. Az adatvédelmi bejelentések típusai

Az érintettől a következő, személyes adatai Intézmény általi kezelését érintő beadványok érkezhetnek („adatvédelmi beadványok”):

a) bejelentheti az Intézmény által nyilvántartott adatok megváltozását;
b) tájékoztatást kérhet személyes adatai [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. §].

12.2. Az adatvédelmi beadványok kezelésének eljárásrendje

Az egyes belső szabályzatoknak, beleértve jelen Szabályzat Különös Részében írt szabályokat is, 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).

Az Intézményhez érkező adatvédelmi beadványokat az Intézmény beérkezett dokumentumok iktatási rendjében foglaltaknak megfelelően kell – a GDPR 12. cikkében írt határidők figyelembevételével – elintézni, az alábbi kiegészítésekkel és eltérésekkel:

a) a beadvány érkezési dátumát és időpontját pontosan rögzíteni kell;
b) a személyes adatok kezelését, illetve a GDPR szerinti jogaik gyakorlását érintő panasz [GDPR 77. cikk, 38. cikk (4) bek.] 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) az igazgatói titkárságok bármely beadvány esetén kérhetik az adatvédelmi tisztviselő véleményét a tekintetben, hogy a beadvány adatvédelmi beadványnak minősül-e, illetve, hogy az érintett kérte-e az adatkezelés korlátozását [zárolás, GDPR 18. cikk], 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 az adatvédelmi 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 az adatvédelmi beadványokra 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.

Az adatvédelmi beadványokról olyan ügyiratnyilvántartást kell vezetni, amely segítségével bármikor egyértelműen azonosíthatók e 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.

## 13. Az adatbiztonsági intézkedések (technikai és szervezési intézkedések) meghatározása és végrehajtása

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.

Az Intézmény működése során betartandó adatbiztonsági szabályokat (GDPR 32. cikk) külön szabályzatok tartalmazzák, így különösen a mindenkor hatályos

a) adatkezelési és adatvédelmi szabályzat,
b) vészhelyzeti intézkedési terv és informatikai üzletmenetfolytonossági szabályzat.

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

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.

Az adatbiztonság elveinek egy adatkezelés bevezetésének vagy személyes adatkezelést és/vagy -feldolgozást eredményező módosításának előkészítése során történő érvényesítése az informatikai szakterület adatkezelési megbízottjának (megbízottjainak) feladata, aki(ke)t az adatkezelési tevékenységet támogató nyilvántartási rendszerek kifejlesztésének, módosításának folyamatába kötelezően be kell vonni.

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

## 14. Közös adatkezelés

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

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
   - mely adatkezelési műveleteket (pl. hozzájáruló nyilatkozatok felvétele, adatok tárolása, adatok felhasználása stb.) végzik,
   - az érintett tájékoztatását hogyan végzik (pl. melyik adatkezelő készíti el az adatkezelési tájékoztatót és bocsátja az érintettek rendelkezésére stb.),
   - az érintett jogai gyakorlását hogyan biztosítják (pl. egyesített vagy elkülönített ügyfélszolgálat stb.),
   - az esetleges jogellenes adatkezelés következményeit milyen arányban viselik;
c) az adatvédelmi incidens észlelése esetén követendő eljárást, különösen azt, hogy
   - 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,
   - egymással kötelesek együttműködni az adatvédelmi rendellenesség vagy incidens okának kiderítésében és következményeinek felszámolásában,
   - 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.

A közös adatkezelés szükségességét az adatkezelési megbízott az adatkezelés bevezetéséről való döntés előkészítése részeként vizsgálja meg.

Amennyiben a közös adatkezelésben érintett másik adatkezelő harmadik országbeli adatkezelő, először abban a kérdésben kell dönteni, 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.

Amennyiben döntés születik a közös adatkezelés bevezetéséről, az illetékes adatkezelési megbízott(ök), az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő és egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében az ügyvéd közreműködésével, továbbá az informatikai szakterület véleményének kikérésével 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.

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.

Az adatkezelési megbízott a közös adatkezelői megállapodás megkötését követően – az adatkezelések nyilvántartására vonatkozó szabályok szerint – e tényt és a további adatkezelő(k) adatait (név és cím, kapcsolattartó neve és elérhetősége) rögzíti az Adatkezelési Nyilvántartásban.

## 15. Adatfeldolgozói megállapodások

Amennyiben harmadik országbeli adatfeldolgozó igénybevétele merül fel, először abban a kérdésben kell dönteni – a 18. 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.

Adatfeldolgozó igénybevétele esetén az adatfeldolgozóval kötendő szerződésnek tartalmaznia kell a GDPR 28. cikk (1)-(4) bekezdésében foglalt tartalmi elemeket az alábbi kiegészítések és pontosítások szerint: 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 az adatvédelmi incidens tudomásra jutása esetén az Intézmény adatvédelmi tisztviselőjét haladéktalanul köteles értesíteni az adatvédelmi incidensről; köteles együttműködni az Intézmény adatvédelmi tisztviselőjével és más közreműködő szervezeti egységgel az adatvédelmi incidens okának feltárásban és következményeinek felszámolásában; 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.

Az adatfeldolgozó igénybevételének szükségességét az adatkezelési megbízott az adatkezelés bevezetéséről való döntés előkészítése részeként vizsgálja meg. Ezt a szabályt kell alkalmazni akkor is, ha az adatfeldolgozó igénybevételéről az adatkezelés folyamán születik döntés.

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.

Amennyiben döntés születik az adatfeldolgozó igénybevételéről, az adatkezelési megbízott az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő és egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a [jogi ügyekért felelős szervezeti egység] közreműködésével, továbbá informatikai szakterület véleményének kikérésével előkészíti az adatfeldolgozóval kötendő szerződés tervezetét és azt felterjeszti a szerződés megkötésére.

Az adatkezelési megbízott az adatfeldolgozói szerződés megkötését követően – az adatkezelések nyilvántartására vonatkozó szabályok szerint – az adatfeldolgozó adatait (név és cím, kapcsolattartó neve és elérhetősége) rögzíti az Adatkezelési Nyilvántartásban.

Az adatfeldolgozásra vonatkozó rendelkezéseket 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 [jogi ügyekért felelős szervezeti egység], továbbá informatikai szakterület véleményét is.

## 16. Az adatkezelési nyilvántartás

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

- az adatkezelés célját,
- az adatkezelés jogalapját,
- az érintettek körét,
- az érintettekre vonatkozó adatok leírását,
- az adatok forrását,
- az adatok kezelésének időtartamát,
- a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló, valamint nemzetközi szervezethez történő adattovábbításokat is,
- az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét,
- az alkalmazott adatfeldolgozási technológia jellegét;
- az adatkezelő szervezeti egység megnevezését,
- az adatkezelésért felelős szervezeti egység vezetője, az adatokhoz hozzáférésre jogosult személyek köre (munkakör),
- az adatkezelés módszere (manuális, számítógépes, vegyes),
- adatbiztonsági intézkedések, archiválás módja, gyakorisága, adattörlés ideje.
- a kockázati besorolást.

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

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

A nyilvántartási célú adatállományt kezelő szervezeti egység vezetője az új adatállomány kialakítását a tevékenység megkezdése előtt 5 munkanappal bejelenti az adatvédelmi tisztviselőnek, aki azt az Adatkezelési Nyilvántartásba bejegyzi.

Az Adatkezelési Nyilvántartásba bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelésért felelős szervezeti egység vezetője 5 munkanapon belül köteles bejelenteni az adatvédelmi tisztviselőnek, aki ennek megfelelően módosítja az Adatkezelési Nyilvántartás adatait.

Az Adatkezelési Nyilvántartással összefüggésben az adatvédelmi tisztviselő:

- 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;
- 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;
- az ügyvéddel együttműködve figyelemmel kíséri az adatkezelést érintő jogszabályok változását és a szükséges módosításokra felhívja az adatkezelési megbízottak figyelmét;

- az adatvédelmi felügyeleti hatóság megkeresésére adatot szolgáltat az Adatkezelési Nyilvántartásból.

## 17. Adatvédelmi incidens-kezelés

Adatvédelmi incidens csak akkor következik be, ha az adatbiztonsági intézkedések – akár vétlen, akár szándékos – megsértésének következtében bekövetkezik a személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés:

- 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;
- 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).

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.

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.

**<u>Az adatvédelmi incidens bejelentése</u>**

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@kardio.hu e-mail címen, vagy az intraneten erre a célra létrehozott űrlapot

kitölteni, vagy az alábbi telefonszámon: +36-70-3820253. Az előbbieken túli egyéb bejelentő az Intézmény elektronikus elérhetőségén vagy az Intézmény honlapján elérhető űrlap kitöltésével jelentheti be az adatvédelmi incidenst.
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 írásban is meg kell erősíteni. Ilyen esetben a szóbeli közlés időpontját külön fel kell tüntetni.

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.

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 Intézmény adatvédelmi tisztviselőjét 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.

**Incidensprotokoll általában**

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

- figyelembe kell venni a különböző biztonsági szabályozásokban az incidens-gyanús események elhárítására vonatkozó rendelkezéseket;
- amennyiben a riasztás személyes adatot tartalmazó alkalmazás sérülékenységével kapcsolatban keletkezett, az incidens elhárítását végző személy az adatvédelmi tisztviselőt haladéktalanul tájékoztatja;
- amennyiben az Intézmény rendelkezik automatizált módszerrel az adott sérülés (incidens) elhárítására, akkor azt azzal az eszközzel azonnal el kell kezdeni;
- ha az Intézmény – a mindenkor hatályos információbiztonsági szabályzatában, továbbá a mindenkor hatályos Számítástechnikai vészhelyzetek intézkedési tervében foglaltakkal összhangban – nem rendelkezik automatizált módszerrel az adott sérülés (incidens) elhárítására, akkor azt manuális módon kell azonnal elkezdeni;
- amennyiben a sérülés elhárítása belső erőforrásból nem kivitelezhető, akkor külső szakértőket kell bevonni az elhárítás folyamatába.

A nem papíralapon kezelt adattal kapcsolatos incidensek kezelésére az Intézmény mindenkor hatályos Adatkezelési és adatvédelmi szabályzatában, továbbá a Számítástechnikai vészhelyzetek intézkedési tervében 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.

**Az adatvédelmi incidens kivizsgálása**

Adatvédelmi incidens (papíralapú és nem papíralapú adatokra vonatkozóak egyaránt) felmerülése esetén az Intézmény adatvédelmi tisztviselője az ügyvéd és az informatikai szakterület kijelölt munkatársának (a továbbiakban együtt: incidensvizsgáló bizottság) közreműködésével megvizsgálja, és 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 össze kell hívni, 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.

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.

Az adatvédelmi incidensről az adatvédelmi tisztviselő értesíti az Intézmény felsővezetőit és – szükség esetén – az Intézmény Titkárságát.

A bejelentés előzetes megvizsgálása során az alábbi szempontokat kell figyelembe venni:

- a bejelentés személyes adatot érint-e,
- amennyiben a bejelentés személyes adatot érint, megállapítható-e a személyes adatok köre,
- megállapítható-e az incidensben érintett személyek köre,
- a hatályos jogszabályok és belső szabályok alapján megállapítható-e, hogy személyes adat jogellenes kezelése vagy feldolgozása (beleértve a törlést/megsemmisítést is) történt,
- az incidens valószínűsíthetően magas kockázattal jár-e az érintettek jogaira és szabadságaira nézve,
- melyek az adatvédelmi incidensből eredő, valószínűsíthető következmények,
- 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.

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 információbiztonsági szabályzatában, illetve a Számítástechnikai vészhelyzetek intézkedési terve foglaltak szerint kell folytatni.

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:

- az Intézmény főigazgatóját;
- ügyvédet;
- informatikai rendszert is érintő incidens esetén az informatikai szakterület vezetőjét;
- a szakmailag illetékes szervezeti egység vezetőjét;
- a Titkárság vezetőjét.

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.

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

A vizsgálat során elsősorban az alábbi módszerek alkalmazhatóak:

- személyes megbeszélés az adatvédelmi incidenst észlelő személyekkel, valamint az érintett szervezeti egységek munkatársaival és vezetőivel,
- írásbeli tájékoztatás kérése az érintett szervezeti egységektől,
- dokumentumok vizsgálata,
- informatikai rendszerek, hálózatok és eszközök vizsgálata, beleértve a naplóállományok vizsgálatát is.

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.

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.
A részletes vizsgálatról szóló jelentést azoknak a vezetőknek kell megküldeni, akiket az adatvédelmi incidensről is értesítettek.

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.
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.

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.

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

**Az érintett tájékoztatása a súlyos adatvédelmi incidensről**

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.

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

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

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

- 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;
- 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;
- 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.

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

**Az adatvédelmi incidens bejelentése a Hatóságnak**

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

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

Az adatvédelmi incidensről szóló bejelentésben legalább:

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

Ha nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

**Az adatvédelmi és egyéb incidensek nyilvántartása**

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.

A nyilvántartásban rögzíteni kell:

- az incidensben érintett személyes adatok körét és számát,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens észlelésének és tudomásszerzésének időpontját,
- az adatvédelmi incidens körülményeit, hatásait,
- az adatvédelmi incidens elhárítására megtett intézkedéseket,
- az adatvédelmi incidenssel kapcsolatban adott tájékoztatások adatait.

Az Intézmény az adatvédelmi incidens kivizsgálásával kapcsolatos papíralapú és elektronikus dokumentumokat 10 évig köteles megőrizni. Az adatvédelmi incidensek vizsgálata során keletkezett iktatott dokumentumokat az adatvédelmi tisztviselő az incidens vizsgálatának lezárásától számított minimálisan 10 évig őrzi meg, illetéktelenek számára hozzá nem férhető zárt helyen.

## 18. Harmadik országba irányuló adattovábbítás különös szabályai

Amennyiben személyes adatnak harmadik országba történő továbbításának szükségessége merül fel, az érintett szervezeti egység köteles az adatvédelmi tisztviselő véleményét kérni az adattovábbítás megengedhetőségéről, illetve az adattovábbítás lehetséges módjáról, figyelembe véve a GDPR szabályait és az aktuális országbesorolást.

Az adatvédelmi tisztviselő – szükség esetén az Intézeti jogtanácsos és az informatikai szakterület véleményének kikérése után – javaslatot tesz az adattovábbítás módjára, az adatátadás során alkalmazandó biztosítékok körére.

## II. KÜLÖNÖS RÉSZ

A Szabályzat Általános Részének rendelkezéseit az e Részben szabályozott esetekben csak annyiban kell alkalmazni, amennyiben e Rész eltérő rendelkezéseket nem tartalmaz.

### A) Az egészségügyi és a hozzá kapcsolódó személyes adatok kezelése

### 19. Az adatvédelemért felelős személyek és feladataik az Eüak. alapján

Az egészségügyi intézményen belül az egészségügyi és személyazonosító adatok védelméért, a nyilvántartás megőrzéséért az Intézmény vezetője a felelős.

**Az Intézményben az egészségügyi és személyazonosító adatok kezelésére jogosultak**

- a betegellátó,
- az intézményvezető,
- az adatvédelmi tisztviselő,

A fenti körbe nem tartozó személyek adatkezelést az Intézményvezetőtől vagy az adatvédelmi tisztviselőtől kapott megbízás alapján végezhetnek.

### 19.1. Az intézményvezető tevékenysége során[35]

Az Intézményvezető tevékenysége során

a. gondoskodik az adatvédelmi szabályok betartásáról,
b. ellenőrzi az adatkezelők és adatfeldolgozók adatkezeléssel, illetve adatfeldolgozással összefüggő tevékenységét,
c. kezdeményezi az adatvédelem, illetve az adatbiztonság területén kifejlesztett új technológiák és eszközök alkalmazását,
d. biztosítja az adatkezeléssel és adatfeldolgozással foglalkozó személyek adatkezelési oktatását,
e. tudományos kutatás esetén [21. § (1) bekezdés] engedélyezi az egészségügyi dokumentációba való betekintést,
f. kijelöli az adatvédelmi tisztviselőt,
g. ellenőrzi az adatvédelmi tisztviselő tevékenységét,
h. gondoskodik az intézmény adatvédelmi szabályzatának elkészítéséről,
i. dönt a kötelező nyilvántartási időt követően a nyilvántartott adatok további tárolásáról vagy megsemmisítéséről.

Az *a)-e)* pontok szerinti tevékenységet az adatvédelmi tisztviselő is elláthatja.

### 19.2. Az Intézmény, mint adatkezelő feladatai

Az Intézményi munkavállalóival kapcsolatos megállapítás: az Intézmény munkavállalói nem adatkezelők, hanem a GDPR 29. cikke szerinti adatkezelő irányítása alatt eljáró személyek.
Az adatkezelő

1) Köteles megtenni minden olyan technikai és szervezési intézkedést, amelyek szükségesek az adatvédelmi és titokvédelmi jogszabályok érvényre jutásához,

[35] Eüak. 32§ (2)

2) Védi az adatokat különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás, törlés, sérülés vagy megsemmisülés ellen.

Az adatkezelő a személyes és különleges adatokkal kapcsolatosban a GDPR, az Infotv. valamint a jelen Szabályzat előírásait, és az orvosi titkot köteles megtartani az Eüak.7. § (2) bekezdésben foglalt kivétellel.

Az Intézmény irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek (a munkavégzésre irányuló jogviszony jellegétől függetlenül) ismerniük kell a jelen Szabályzatban foglalt adatkezelésre vonatkozó szabályokat:

a) gondoskodniuk kell arról, hogy az általuk kezelt adatokhoz és adathordozókhoz illetéktelenek ne juthassanak hozzá,

b) a munkájuk során tudomásukra jutott egészségügyi információkat a jogosultak kivételével, senkivel nem közölhetik,

c) Az Eüak. 7. § (2) bekezdése alapján mentesül a titoktartási kötelezettség alól, ha

- az egészségügyi és személyazonosító adat továbbítására az érintett, illetve törvényes képviselője írásban hozzájárult, az abban foglalt korlátozásokon belül, valamint
- az egészségügyi és személyazonosító adat továbbítása törvény előírásai szerint kötelező.

d) a titoktartási kötelezettség a közalkalmazotti jogviszony, megbízási jogviszony vagy munkaviszony megszűnése után is fennmarad.

## 20. Az Intézményben folytatott adatkezeléssel érintett szervezeti egységek

Az Intézményben egészségügyi adatkezelés az alábbi szervezeti egységekben történik:

1. Főigazgatóság
2. Gazdasági igazgatóság és kapcsolódó osztályai
3. Ápolási igazgatás
4. Betegfelvételi és betegirányítási iroda (fekvő járóbeteg ellátás), porta
5. Gyermek kardiológia
6. Felnőtt kardiológia
7. Gyermek szívsebészet
8. Felnőtt szívsebészet
9. Gyermek Intenzív osztályok
10. Felnőtt Intenzív osztályok
11. Érsebészet
12. Központi laboratórium
13. Radiológiai osztály
14. Katéter terápiás osztály (Hemodinamika – Elektrofiziológia és PM részleg)
15. Diagnosztikus laboratóriumok (Echo, Ergo, Angiológia, Holter)
16. Klinikai farmakológia osztály
17. Intézeti gyógyszertár
18. Informatikai osztály
19. Kontrolling, finanszírozási és minőségirányítási igazgatóság

## 21. Az egészségügyi adatkezelés célja

1, Az egészségügyi és személyazonosító adat kezelésének célja[36]:

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

2. Egészségügyi és személyazonosító adatot az alábbi célokból lehet kezelni az orvosi titoktartást nem szem elől tévesztve[37]:

a) egészségügyi szakember-képzés,

b) orvos-szakmai és epidemiológiai vizsgálat, elemzés, az egészségügyi ellátás tervezése, szervezése, költségek tervezése,

c) statisztikai vizsgálat,

d) hatásvizsgálati célú anonimizálás és 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, valamint a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról szóló törvény szerinti rendvédelmi egészségkárosodási ellátás megállapítása,

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, valamint a társadalombiztosítási ellátások megállapítása, kifizetése és a kifizetett ellátások visszafizetése, megtérítése érdekében,

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, kormányzati szolgálati, politikai szolgálati,

[36] Eüak. 4 § (1) bekezdés
[37] Eüak. 4 § (2) bekezdés

biztosi vagy közszolgálati jogviszony, hivatásos szolgálati viszony vagy egyéb jogviszony keretében történik,

p)köznevelés, szakképzés, illetve felsőoktatás 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. A fenti céloktól eltérő célra is lehet az érintett, illetve törvényes vagy meghatalmazott képviselője (a továbbiakban együtt: törvényes képviselő) - megfelelő tájékoztatáson alapuló önkéntes, egyértelműen kifejezett akaratot tartalmazó, és a szabályszerű nyilatkozat megtételét hitelt érdemlően bizonyító módon tett - hozzájárulásával egészségügyi adatot kezelni teljes körűen vagy egyes adatkezelési tevékenységre kiterjedően

4. A 1.-2. szerinti adatkezelési célokra csak annyi és olyan egészségügyi, illetve személyazonosító adat kezelhető, amely az adatkezelési cél megvalósításához elengedhetetlenül szükséges.

5. Az egészségügyi ellátó hálózaton belül az egészségügyi és személyazonosító adat kezelésére – amennyiben e törvény másként nem rendelkezik – jogosult

*a)* a betegellátó,

*b)* az intézményvezető, valamint

*c)* az adatvédelmi felelős,

6. A közegészségügyi-járványügyi veszélynek kitett személy, az ilyen személlyel kapcsolatban álló vagy kapcsolatba került és ezért közegészségügyi-járványügyi szempontból veszélyeztetett személy, valamint az ilyen személyekkel kapcsolatos egészségügyi és személyazonosító adatot

kezelő az egészségügyi és személyazonosító adatot, illetve telefonos vagy más elektronikus elérhetőséget

*a)* az érintett kezelését végző orvos,

*b)* az egészségügyi államigazgatási szerv keretében dolgozó tisztiorvos,

*c)* a közegészségügyi-járványügyi felügyelő,

*d)* a közegészségügyi-járványügyi célból adatkezelésre jogosult más személy vagy szerv, valamint

*e)* az Egészségügyi Világszervezet 2009. évi XCI. törvénnyel kihirdetett Nemzetközi Egészségügyi Rendszabályai (NER) végrehajtása körében a NER végrehajtásában közreműködő szerv feladatkörrel rendelkező alkalmazottja részére - kérésükre - a közegészségügyi-járványügyi cél által indokolt körben köteles haladéktalanul és ingyenesen átadni.

7. Az egészségügyi és személyazonosító adatok kezelése és feldolgozása során biztosítani kell az adatok biztonságát véletlen vagy szándékos megsemmisítéssel, megsemmisüléssel, megváltoztatással, károsodással, nyilvánosságra kerüléssel szemben, továbbá, hogy azokhoz illetéktelen személy ne férjen hozzá[38].

**Amennyiben az adatkezelés célja** az egészség megőrzésének, fenntartásának elősegítése, az érintett egészségi állapotának nyomon követése, vagy közegészségügyi és járványügyi érdekből szükséges, abban az esetben az adat kezelés a kóros szenvedélyre és szexuális szokásokra is kiterjed (ebben az esetben az Intézmény vezetője saját hatáskörében különleges adathozzáférési jogosultságok kialakítását engedélyezheti).

### B) A betegek jogai a 1997. évi CLIV. törvény alapján

A betegek jogait az 5. számú melléklet tartalmazza.
A beteg és hozzátartozói jogainak gyakorlása nem sértheti az egészségügyi dolgozóknak törvényben foglalt jogait.
A betegjogok gyakorlásának módját – e törvény keretei között, ideértve a leletkiadás rendjét is - a szolgáltató működési rendje (gyógyintézet házirendje) szabályozza.

### C) Adatkezelés gyógykezelés céljából és a felvett adatok biztonságára vonatkozó előírások

A gyógyítás sikere és az adatkezelési eljárás sérthetetlensége, bizalmassága érdekében törekedni kell arra, hogy a kezelt személyes adatok pontosak, teljesek és időszerűek legyenek.

Az adatok tárolását biztosító rendszernek támogatniuk kell:

- a számítógépes adatrögzítési eljárások és adatrögzítési hibák felderítését, javítását;
- az adatkezelési folyamatba beépített egyeztető kontrollokat;
- az adatok tetszőleges összeállítás szerinti visszakereshetőségét és a gyors visszakeresés centrikus adattárolást,
- a különböző egészségügyi adatokra tárolási és láthatósági szabályok és jogosultságok kialakíthatóságát;

[38] Eüak. 6. §

- azt, hogy a kezelt személyes adatokkal az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani (törlés a kezelés után),
- a különböző adattípusok tárolási módját, feltételeit (szöveg, adat, dátum, kulcsszó, kulcs-értékpár, stb.).

A fenti elvárásokat az informatikai rendszer beszerzése kapcsán az elvárások között fel kell tüntetni és az átadás átvételi folyamatok, valamint az üzemeltetés kapcsán folyamatosan ellenőrizni.

Az egészségügyi adatok felvétele a gyógykezelés része. Az egészségügyi és a személyazonosító adatoknak a gyógykezelt személy részéről történő szolgáltatása – az egészségügyi ellátás igénybevételéhez kötelezően előírt személyazonosító kivételével – önkéntes. Abban az esetben, ha a gyógykezelt személy önként fordul a kórházhoz, a gyógykezeléssel összefüggő egészségügyi és személyazonosító adatainak kezelésére szolgáló hozzájárulását – ellenkező nyilatkozat hiányában – megadottnak kell tekinteni, és erről az érintettet (törvényes képviselőjét) tájékoztatni kell. Sürgős szükség, valamint a gyógykezelt személy belátási képességének hiánya esetén az önkéntességet vélelmezni kell.

Az adatfelvétel során a gyógykezelés alatt az egészségügyi dokumentációban rögzíteni kell a szakmai szabályoknak megfelelően felvett adatokat. A kezelést végző orvos dönti el, hogy a szakmai szabályoknak megfelelően – a kötelezően felveendő adatokon kívül – mely egészségügyi adat felvétele szükséges.

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 (ilyen adat lehet például a beteg családi állapota, foglalkozása).

A kóros szenvedélyre, illetve a szexuális életre vonatkozó adatok csak akkor rögzíthetők, ha azok az adott betegség ellátásához orvos-szakmai szempontból szükségesek. Az így felvett adatokat különös gondossággal kell kezelni. Ezen adatokat elsősorban az intézményen belüli egészségügyi dokumentációban lehet felhasználni, továbbításuk a zárójelentésben csak kivételes okból megengedett. Ilyen adat például a nemi identitásra, nemi betegségekre, illetve a drogfogyasztásra vonatkozó adat, az alkoholizmus, illetve dohányzás szokása. Hasonlóan gondosan kell kezelni pl. a művi abortuszra vonatkozó adatokat, a Wassermann-teszt vizsgálati eredményét, stb.

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.

A lázlapok nem tarthatók a betegágy végén vagy másutt a kórteremben, illetve szabadon hozzáférhetően nem tárolhatják, kivéve a vizit idejét. A beteg nevét nem lehet a kórtermek ajtajára kifüggeszteni. A kórlapokat nem lehet a nővérpulton vagy másutt úgy tárolni, hogy a személyazonosító adatok a helyiségben tartózkodók, a beteg ellátásában részt nem vevők számára hozzáférhető legyen.

A gyógykezelés céljából rögzített adatokkal kapcsolatban biztosítani szükséges az alábbiakat:

- Bizalmasságot:
  A rendszerben kezelt adatot csak az arra jogosultak és csak a jogosultságuk szerinti mértékben ismerhessék meg, használhassák fel, illetve rendelkezhessenek a felhasználásáról.
- Rendelkezésre állást:

Biztosítani kell, hogy a rendszerben rögzített adatok, illetve az informatikai rendszer elemeit az arra jogosultak számára a szükséges időpontban és időtartamra rendelkezésre álljanak.

- Sértetlenség (védelem):

Az adatok tárolását végző eszközök minden elemének védelme szükséges.

### D) Adatkezelés közegészségügyi, járványügyi célból

A közegészségügyi és járványügyi célból történt adatkezelés az Intézmény közegészségügyi és járványügyi szabályzata szerint történik.

### E) Adatkezelés tudományos kutatási, statisztikai célból

## 22. Adatkezelés tudományos kutatási, statisztikai célból

### 22.1. Tudományos kutatási célú adatkezelés Eüak. szerinti szabályai

Tudományos kutatás céljából az intézményvezető vagy az adatvédelmi tisztviselő engedélyével a tárolt adatokba be lehet tekinteni, azonban tudományos közleményben nem szerepelhetnek egészségügyi és személyazonosító adatok oly módon, hogy az érintett személyazonossága megállapítható legyen. Tudományos kutatás során a tárolt adatokról nem készíthető személyazonosító adatokat is tartalmazó másolat.
A tárolt adatokba betekintett személyekről, a betekintés céljáról és időpontjáról nyilvántartást kell vezetni. A nyilvántartás kötelező megőrzési ideje 10 év.
A kutatási kérelem megtagadását az intézményvezető vagy az adatvédelmi tisztviselő köteles írásban megindokolni. A kérelem megtagadása esetén a kérelmező bírósághoz fordulhat. A per megindítására és az eljárás lefolytatására az információs önrendelkezési jogról és az információszabadságról szóló törvénynek a közérdekű adat megismerése iránti igény elutasítása esetén megindítható perre vonatkozó szabályai az irányadóak. [Eüak. 21.§]

### 22.2. Statisztikai célú adatkezelés

A kötelező adatkezelés keretében kezelt személyes adatokat – ha törvény eltérően nem rendelkezik – a Központi Statisztikai Hivatal statisztikai célból egyedi azonosításra alkalmas módon átveheti és törvényben meghatározottak szerint kezelheti.
A statisztikai célra felvett, átvett vagy feldolgozott személyes adatok - ha törvény eltérően nem rendelkezik - csak statisztikai célra kezelhetők. A személyes adatok statisztikai célra történő kezelésének részletes szabályait külön törvény határozza meg.

**F) Adatkezelés a kórház eredményes gyógykezelési tevékenységének elősegítése céljából**

A kórház eredményes gyógykezelési tevékenységének elősegítése, az ellátás tervezése, szervezése, költségek tervezése céljából a 1997. évi CLIV. törvény 24 §. alapján a beteg jogosult megismerni a róla készült egészségügyi dokumentációban szereplő adatait, illetve joga van ahhoz, hogy – az Eütv. 135. §-ban[39] foglaltak figyelembevételével – egészségügyi adatairól tájékoztatást kérjen.
A tárolt adatokhoz a hozzáférés nem korlátozott, azzal a kitétellel, hogy az adatokról személyazonosításra alkalmas másolat nem készíthető. A fenti célból az adatkezelés engedélyezett:

- az Intézményvezető,
- az adatvédelmi tisztviselő
- a minőségbiztosítási csoport tagjai részére, előzetesen írásban indokolt cél érdekében, annak eléréséig,
- illetve más olyan személy részére, akit az Intézményvezető vagy adatvédelmi tisztviselő e célból írásban megbíz. A megbízások megadott ideig érvényesek. A fenti céllal végzett adatkezelésről nyilvántartást kell vezetni.

Az egészségügyi ellátás finanszírozásához szükséges adatlapok elkészítése érdekében az osztályok kódoló orvosai jogosultak az érintettek az osztályukon történt gyógykezelésével kapcsolatos valamennyi tárolt adatba betekinteni, időbeni korlátozás nélkül. Az adatokról másolat nem készíthető. A jogosultság a kódolási megbízás tartamára szól, melyet minimum évente felül kell vizsgálni.

**G) Egészségügyi dokumentáció**

Az Eütv. 136. §-a szerint az egészségügyi dokumentáció részét képezi:

- a beteg személyazonosító adatai,
- cselekvőképes beteg esetén az értesítendő személy, valamint - ha a beteg kéri - a támogatott döntéshozatalról szóló törvény szerinti támogató nevét, lakcímét, elérhetőségét, továbbá kiskorú, illetve gondnokság alatt álló beteg esetében a törvényes képviselő neve, lakcíme, elérhetősége,
- a kórelőzmény, a kórtörténete,
- az első vizsgálat eredménye,
- a diagnózis(ok) és a gyógykezelési tervet megalapozó vizsgálat eredménye, a vizsgálatok elvégzésének időpontjai,
- az ellátást indokoló betegség megnevezése, a kialakulásának alapjául szolgáló betegség, a kísérőbetegségek és szövődmények,
- egyéb, az ellátást közvetlenül nem indokoló betegség, illetve a kockázati tényezők megnevezése,
- az elvégzett beavatkozások ideje és azok eredménye,
- a gyógyszeres és egyéb terápia, annak eredménye,
- a beteg gyógyszer-túlérzékenységére vonatkozó adatok,
- a bejegyzést tevő egészségügyi dolgozó neve és a bejegyzés időpontja,

[39] **1997. évi CLIV. törvény - az egészségügyről**

- a betegnek illetőleg tájékoztatásra jogosult más személynek nyújtott tájékoztatás tartalmának rögzítése,
- a beleegyezés, illetve visszautasítás ténye, valamint ezek időpontja,
- minden olyan egyéb adat és tény, amely a beteg gyógyulására befolyással lehet. Ide tartozik az orvosi dekurzus, illetve az ápolási dokumentáció.

Fekvőbeteg esetén a kórlapot az egészségügyi dokumentáció részei alkotják, együtt a beteg lázlapjával, dekurzusával. A kórlapba a kezelés befejezése után a zárójelentés egy példányát be kell illeszteni.

## H) Orvosi titok védelme

Az Intézmény irányítása alatt eljáró természetes személyeket (a munkavégzésre irányuló jogviszony jellegétől függetlenül) a beteg egészségi állapotával kapcsolatos adat, továbbá a munkavégzéssel kapcsolatosan tudomására jutott egyéb adat vonatkozásában időbeni korlátozás nélkül titoktartási kötelezettség terheli[40]. A titoktartási kötelezettség független attól, hogy az adatokat milyen módon ismerte meg.

A titoktartási kötelezettség tehát nemcsak a kezelőorvost, illetve az ápolószemélyzetet köti, hanem az intézmény minden dolgozóját. Ilyen személyek lehetnek például a betegszállítók vagy a beteg diétáját készítő konyhai dolgozók.

A betegellátót – a gyógykezelt személy választott háziorvosa, valamint az igazságügyi orvos szakértő 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.

A titoktartási kötelezettség alól írásban felmentést adhat a beteg, vagy jogszabályi kötelezettség teljesítése.

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.

## I) A gyógykezelés során jelen lévő személyek

A gyógykezelés során a kezelést végző orvos és a betegellátásban részt vevő más személyek lehetnek jelen.
Jelen lehet továbbá:

- más személy, ha a gyógykezelés rendje több beteg egyidejű ellátását igényli (Ilyen eset például az intenzív osztályokon történő kezelés, vagy más olyan osztályokon, ahol a beteg vagy a betegtársak mobilizálása állapotromlás veszélyével járhat.),
- fogva tartott vagy szabadságelvonással büntetett személy esetében a rendőrség hivatásos állományú tagja vagy a büntetés-végrehajtási szervezet jogviszonyban álló tagja. (Fenti

[40] Eüak. 7. §

esetekben a gyógykezelt személy hozzájárulására nincs szükség, de a beteg emberi jogait és méltóságát tiszteletben kell tartani.),
- más személy, ha a gyógykezelt személy ehhez hozzájárult.

Ezen túlmenően jelen lehet az:
- aki a beteget az adott betegség miatt már kezelte,
- akinek az orvos igazgató vagy az adatvédelmi megbízott szakmai ok miatt engedélyt adott. A gyógykezelt személy kifejezett tiltakozásának ebben az esetben helyt kell adni.

Kórházunkban egészségügyi szakemberképzés céljából – oktatókórház jellegére tekintettel – jelen lehet:
- orvos, orvostanhallgató,
- egészségügyi szakdolgozó, egészségügyi főiskola, középiskola vagy szakiskola hallgatója, feltéve, hogy a megjelölt személy képzésére a kórház ki van jelölve. Ebben az esetben a gyógykezelt személy hozzájárulására nincs szükség, de a betegtájékoztatóban a kórház oktató jellegéről és a szakemberképzésről a gyógykezelteket tájékoztatni kell.

Fentieken kívül olyan személy lehet jelen, akinek a jelenlétéhez a gyógykezelt személy hozzájárul (pl.: szülő, gyerek, más közeli hozzátartozó, stb.). A hozzájárulást a gyógykezelt személy szóban is megteheti a kezelőorvosnak.

**J) Adattovábbítások**

Amennyiben az egészségügyi és személyazonosító adat kezelésének célja az egészség megőrzésének, fenntartásának előmozdítása, a betegellátó eredményes gyógykezelési tevékenységének elősegítése, az érintett egészségi állapotának nyomon követése vagy közegészségügyi és járványügyi érdek abban az esetben az egészségügyi ellátóhálózaton belül az

- egészségügyi és személyazonosító adatok továbbíthatók, illetve összekapcsolhatók. A különböző forrásból származó egészségügyi és személyazonosító adatokat csak addig az időpontig és olyan mértékig lehet összekapcsolni, ameddig az a megelőzés, a gyógykezelés, a közegészségügyi-járványügyi intézkedések megtétele érdekében feltétlenül szükséges,
- érintett betegségével kapcsolatba hozható minden olyan egészségügyi adat továbbítható, amely a gyógykezelés érdekében fontos, kivéve, ha ezt az érintett írásban kifejezetten megtiltja.

Sürgős szükség esetén a kezelést végző orvos által ismert, a gyógykezeléssel összefüggésbe hozható minden egészségügyi és személyazonosító adat továbbítható az érintett hozzájárulása nélkül is. A sürgős szükség tényét a beteg dokumentációjában hitelt érdemlően dokumentálni szükséges.

## 23. Adattovábbítás az intézményen belül

Az adatok akkor továbbíthatók, valamint a különböző adatkezelések akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy törvény azt megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek.

A gyógykezelt személy betegségével kapcsolatba hozható minden egészségügyi adat továbbítható az intézményen belül, amely a gyógykezelés érdekében fontos. A beteg az Intézménybe történt felvételkor vagy később rendelkezhet arról, hogy ezt megtiltsa. A beteget a rendelkezés lehetőségéről tájékoztatni kell. A tiltás nem érvényes akkor, ha az adattovábbítást jogszabály írja elő.
Nem továbbítható ugyanakkor a gyógykezelt személy hozzájárulása nélkül olyan adat, mely a fennálló betegséggel össze nem függő, korábbi betegségre vonatkozik[41].

## 24. Adatkommunikáció más rendszerekkel

Adatkommunikációt más rendszerekkel csak zárt módon API (application programming interface) kommunikáció kialakításával szabad megvalósítani. A kommunikáció lehet file vagy port kommunikáció.
A kommunikációs protokollokat írásban rögzíteni szükséges. Ilyen módon működik például a labor, ultrahang és a PACS kommunikáció.
A kommunikáció indítása során próbaüzemet kell tartani és rendszeres időközönként ellenőrizni kell a kommunikáció validitását.

## 25. Adattovábbítás az intézményen kívülre

Egészségügyi és személyazonosító adatokat is tartalmazó elektronikus dokumentum az intézményen kívülre kizárólag deperszonalizálás után kerülhet kivéve, ha az adattovábbítás a GDPR 6. cikk szerinti jogalappal történik.. Ebben az esetben az adatok akkor továbbíthatók, valamint a különböző adatkezelések akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy törvény azt megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek.
Jelen Szabályzat (Különös Rész) 42. fejezete szabályozza az ágazati informatikai rendszerbe (EESZT) történő továbbítást.

Személyes adat az országból – az adathordozótól vagy az adatátvitel módjától függetlenül – külföldi adatkezelő részére csak akkor továbbítható, ha az érintett ahhoz hozzájárult, vagy törvény azt lehetővé teszi, feltéve hogy az adatkezelés feltételei a külföldi adatkezelőnél minden egyes adatra nézve teljesülnek.

## 26. Társadalombiztosítási ellátás és az ellátás finanszírozása céljából történő adattovábbítás

A társadalombiztosítási igazgatási szervek részére abban az esetben továbbítható egészségügyi és személyazonosító adat, amennyiben

- arra az érintettnek járó társadalombiztosítási ellátások megállapítása, folyósítása céljából van szükség, és az egészségi állapot alapján történik, valamint
- az a társadalombiztosítási alapok kezelői gazdálkodásának, továbbá a társadalombiztosítási ellátások folyósításának ellenőrzése céljából indokolt.

A társadalombiztosítási igazgatási szervek által lefolytatott ellenőrzés során a társadalombiztosítás szerveinek csak orvos, illetve gyógyszerész végzettségű alkalmazottja ismerheti meg a gyógykezelt személy összekapcsolt egészségügyi és személyazonosító adatait.

[41] 1997. évi XLVII. tv. 10. § (1)

Az egészségügyi ellátást finanszírozó szervek részére a betegforgalmi összesítéseket az Informatikai Osztály továbbítja.

## 27. Elektronikus adattovábbítással kapcsolatos előírások

Elektronikus adattovábbítás esetén az adatkezelő, illetve az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. 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.
Elektronikus adattovábbítás esetén az alábbi műszaki paraméterek vizsgálata és minősítése szükséges az adattovábbítás megkezdése előtt:

- Átviteli vonalkárosodás, megszakadás
- A hálózati szoftver és hardver manipulálhatósága
- Az adó és a fogadó hiányzó azonosítása
- Függés az átvitel sorrendjétől
- Valamely adattovábbítás elküldésének, kézhezvételének hiányzó bizonyítása

## 28. Adattovábbítás megnevezett hivatalos szervek részére

Az egyes szervek részére adat írásbeli megkeresés alapján adható ki. A megkeresésnek tartalmaznia kell a megismerni kívánt adat megnevezését és az adatkezelés pontos célját. Csak annyi és olyan adat továbbítható, mely az adatkezelési cél megvalósulásához elengedetlenül szükséges. A következő szervek igényelhetik a gyógykezelt személy egészségügyi és személyazonosító adatait:

- büntetőügyben a nyomozó hatóság, az ügyészség, a bíróság, az igazságügyi orvos szakértő, polgári és közigazgatási ügyben az ügyészség, a bíróság, az igazságügyi orvos szakértő,
- szabálysértési eljárás során az eljárást lefolytató szervek,
- hadköteles személy esetén az illetékes jegyző, a hadkiegészítő parancsnokság, illetve a katonai egészségügyi alkalmasságot megállapító bizottság,
- a nemzetbiztonsági szolgálatok, a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben meghatározott feladatok ellátása érdekében, az abban kapott felhatalmazás körében.

## 29. Bűncselekményből eredő sérülés esetén adattovábbítás

A kezelőorvos a gyógykezelt személy első ellátása során a rendőrségnek haladéktalanul bejelenti a gyógykezelt személy személyes adatait, ha gyógykezelt személy 8 napon túl gyógyuló sérülést szenvedett, és a sérülés feltehetően bűncselekmény következménye. 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.

## 30. Adattovábbítás egyéb célból és az adattovábbítási nyilvántartás

Daganatos eredetű betegség észlelése esetén a gyógykezelt személy egészségügyi és személyazonosító adatait a Nemzeti Rákregiszternek kell továbbítani. A Nemzeti Rákregisztert az Országos Onkológiai Intézet vezeti. Az adattovábbítást az informatikai osztály végzi. Más betegség esetén személyazonosításra alkalmas módon adat epidemiológiai céllal nem továbbítható.

Egészségügyi és személyazonosító adatot akkor lehet továbbítani, ha az adattovábbításnak van a GDPR 6. cikk szerinti jogalapja.

## 31. Adattovábbítási nyilvántartás

Az Intézmény az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából adattovábbítási nyilvántartást vezet, amely tartalmazza az általa kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

## 32. Az Elektronikus Egészségügyi Szolgáltatás Tér

Az Elektronikus Egészségügyi Szolgáltatás Tér (a továbbiakban: EESZT) egy európai uniós forrásból létrehozott egységes informatikai környezet, ami az egészségügyi ágazat hatékony és biztonságos információáramlását valósítja meg. Az EESZT önállóan és az egészségügyi ellátó hálózat informatikai rendszereihez csatlakozva tölti be központi szerepét.
Az EESZT emellett lehetővé teszi, hogy az Érintettek átláthassák és felügyeljék az egészségügyi adataik EESZT rendszeren belüli kezelését. Az EESZT szolgáltatásainak működésére vonatkozó részletes leírás a http://www.e-egeszsegugy.gov.hu weboldalon található.
Az adatok kezelője (a továbbiakban: EESZT Adatkezelő vagy Működtető) az Állami Egészségügyi Ellátó Központ, ide nem értve azokat a szolgáltatásokat, melyek esetében kifejezetten adatfeldolgozónak minősül.
Az ÁEEK adatkezelőként való megjelölése az Állami Egészségügyi Ellátó Központról szóló 27/2015. (II. 25.) Korm. rendelet 6. § (4)-(6) bekezdésein alapul, mely az EESZT működtetőjének, az EESZT-hez kapcsolódó önrendelkezési nyilvántartás vezetőjének és az EESZT-ben használt kapcsolati kódot kezelő szervnek az Állami Egészségügyi Ellátó Központot jelölte ki. A Kormányrendelet az intézmény e feladatokra történő kijelölését az Eüak. 38. § (2) bekezdésében kapott felhatalmazás alapján végezte.

Az adatfeldolgozó feladatait a központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről szóló 7/2013. (II. 26.) NFM rendelet – mely 1. számú melléklete 1.23. és 1.24. pontja szerint kizárólagos joggal rendelkezik az EESZT rendszer üzemeltetésében - valamint a Működtetővel kötött szerződés alapján végzi. Az adatfeldolgozó elsődleges feladata információtechnológiai infrastruktúra biztosítása. Az adatfeldolgozó a nemzeti vagyonról szóló 2011. évi CXCVI. törvény alapján átlátható szervezetnek minősül.

### 32.1. Adatbiztonság

Az EESZT adatkezelője különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás elleni adminisztratív, fizikai és logikai védelmi intézkedéseket tesz.
A jogosulatlan hozzáférés megakadályozására az adatok titkosított tárolása mellett az azokhoz való hozzáférés kizárólag megbízható azonosítás (tanúsítvány alapú, vagy kétfaktoros azonosítás) után lehetséges. Az EESZT tekintetében minden üzleti és rendszeresemény naplózásra, az adminisztrációs tevékenységek a módosítást ellehetetlenítő módon rögzítésre kerülnek. A külső hozzáférés megakadályozása érdekében a rendszert tűzfalak védik, valamint a rendszer bizonyos felületei (pl. adminisztrációs felületek) kizárólag belső hálózatból érhetők el.
Az adatok véletlen megsemmisülésének, sérülésének megakadályozása érdekében az adatállományok rendszeresen mentésre, földrajzilag elkülönülő helyen kerülnek tárolásra.
Az EESZT adatkezelője fokozott figyelmet fordít arra, hogy megakadályozza az Érintettek adatainak helytelen rögzítését, valamint azt is, hogy az Érintettek adati más Érintetthez kerüljenek rögzítésre. Az Érintett azonosítását szolgáló adatkezelések mind azt a célt szolgálják, hogy a kezelés biztonságossága, megbízhatósága biztosított legyen.

## K. Az Érintett adatkezeléssel kapcsolatos jogai

### 33. Tájékoztatás kérése

Az Érintett bármikor jogosult tájékoztatást kérni az Intézmény által kezelt, rá vonatkozó személyes adatokról.
Az Intézmény az Érintett kérésére tájékoztatást ad a rá vonatkozó, általa kezelt adatokról, az általa vagy rendelkezése szerint megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, továbbá az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá - az Érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről. Az Intézmény a kérelem benyújtásától számított 1 hónapon belül írásban adja meg a kért tájékoztatást. Az Intézmény az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az Érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az Érintett személyes adatok körét, az adatvédelmi incidenssel Érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.
Az Érintett bármely, az adatkezeléssel kapcsolatos kérdéssel, illetve észrevétellel az EESZT adatvédelmi tisztviselőjéhez is fordulhat.

### 34. Személyes adat helyesbítése, törlése, korlátozása

Az érintett bármikor jogosult a helytelenül rögzített adatainak helyesbítését vagy azok törlését kérni az Intézmény által megjelölt elérhetőségek valamelyikén. Az Intézmény a kérelem beérkezésétől számított 5 munkanapon belül törli az adatokat, ez esetben azok nem lesznek újra helyreállíthatók. A törlés nem vonatkozik a jogszabály alapján kötelezően előírt adatkezelésekre,

azokat az Intézmény a jogszabályban előírt időtartamig megőrzi. Az Érintett kérheti továbbá adatainak korlátozását. Az Intézmény korlátozza a személyes adatot, ha az alábbi feltételek valamelyike teljesül:

- az Érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;
- az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását; vagy az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;
- az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

A helyesbítésről, a korlátozásról és a törlésről az Érintettet, továbbá mindazokat értesíteni kell, akiknek korábban az adatot adatkezelés céljára továbbították. Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az Érintett jogos érdekét nem sérti.
Ha az Intézmény az Érintett helyesbítés, korlátozás vagy törlés iránti kérelmét nem teljesíti, a kérelem kézhezvételét követő 1 hónapon belül írásban közli a helyesbítés, zárolás vagy törlés iránti kérelem elutasításának ténybeli és jogi indokait.

## 35. Jogorvoslati lehetőségek

Az Érintett – amennyiben álláspontja szerint az adatkezelés nem felel meg a jogszabályi követelményeknek, illetőleg az Intézmény megsértette személyes adataihoz fűződő jogait – a

**Nemzeti Adatvédelmi és Információszabadság Hatósághoz**
**(székhely: 1125 Budapest Szilágyi Erzsébet fasor 22/C;**
**postacím: 1530 Budapest, Pf. 5,**
**telefon: +36 (1) 391-1400,**
**e-mail: ugyfelszolgalat@naih.hu,**
**web: http://naih.hu)**

fordulhat, vagy a Bíróság előtt érvényesítheti jogait.

A jogérvényesítés az Infotv., valamint a Ptk. alapján lehetséges.
A Nemzeti Adatvédelmi és Információ Hatóságnál bejelentéssel bárki vizsgálatot kezdeményezhet arra hivatkozással, hogy személyes adatok kezelésével kapcsolatban jogsérelem következett be vagy annak közvetlen veszélye fennáll.
Az érintett adatvédelmi hatósági eljárás megindítása iránti kérelmet nyújthat be a Nemzeti Adatvédelmi és Információ Hatósághoz, ha megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti e rendeletet.
A bírósági jogérvényesítés esetén az ügyben soron kívül jár el. A per elbírálása az Adatkezelő székhelye szerinti, azaz a

**Fővárosi Törvényszék**
**(1055 Budapest, Markó u. 27,**
**levelezési cím: 1363 Pf. 16.,**

**tel.: +36-1-354-6000)**

hatáskörébe tartozik, de a per - az Érintett választása szerint - az Érintett lakóhelye vagy tartózkodási helye szerinti törvényszék előtt is megindítható.
Az Érintett a jogainak megsértése esetén közvetlenül az Intézmény adatvédelmi tisztviselőjéhez is fordulhat.
Az adatvédelmi tisztviselő neve: Nagy István
e-mail: dpo@kardio.hu
Telefonszám munkaidőben: 06-1-2151220

## L. Tájékoztatással kapcsolatos ismeretek

### 36. A beteg joga a tájékoztatáshoz

A beteget felvételkor tájékoztatni kell a kórház adatvédelmi rendjéről. Abban az esetben, ha az érintett önként fordul az egészségügyi ellátó hálózathoz, a gyógykezeléssel összefüggő egészségügyi és személyazonosító adatainak kezelésére szolgáló hozzájárulását – ellenkező nyilatkozat hiányában – megadottnak kell tekinteni, és erről az érintettet (törvényes képviselőjét) tájékoztatni kell [Eüak.12. § (2)]. A beteg tájékoztatása a kórházi adatvédelemről a felvevő orvosnak 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.

A gyógykezelt személy gyógykezelésével kapcsolatos tájékoztatást a beteg kezelőorvosa vagy a betegellátó osztály vezetője adja meg. A beteg gyógykezelésének ápolási vonatkozásairól az őt ellátó diplomás ápoló is felvilágosítást adhat. Ápoló, illetve más dolgozó a beteg gyógykezeléséről tájékoztatást nem adhat, kivéve, ha a beteg kezelőorvosa erre az adott beteg esetében felhatalmazta. A tájékoztatás személyesen történik.

Telefonon a beteg gyógykezeléséről érdemi tájékoztatás nem adható. A kezelőorvos, az osztály más orvosa, illetve ápoló a beteg kórházi kezelésének tényét – a beteg ellenkező értelmű nyilatkozata hiányában – megerősítheti. Ezen túlmenően a beteg általános állapotára vonatkozó információt orvos megadhat azon közeli hozzátartozóknak, akiket azonosítani tud és a beteg erre az általános tájékoztató keretén belül feljogosítja.

### 37. A gyermekek tájékoztatáshoz való jogának biztosítása

Az Intézmény szervezeti egységeinek vezetői az adatkezelési megbízottak közreműködésével 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.

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

Az Intézmény szervezeti egységeinek vezetői az adatkezelési megbízottak közreműködésével 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.

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

Az Intézmény szervezeti egységeinek vezetői az adatkezelési megbízottak 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.

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

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.

### 40. Hozzátartozó és más személy tájékoztatása

A beteg a kórházba történt felvételkor vagy később rendelkezhet arról, hogy egyes közeli hozzátartozóit kizárja a tájékoztatásra jogosultak köréből. A beteget a rendelkezés lehetőségéről tájékoztatni kell. Az ehhez használatos nyilatkozat mintája a jelen Szabályzat 4. számú mellékletében található. Ennek hiányában a közeli hozzátartozók tájékoztatásához a beteg hozzájárulása megadottnak tekinthető.

A beteg a kórházba történt felvételkor vagy később rendelkezhet arról is, hogy valamennyi személyt kizár a tájékoztatásra jogosultak köréből. A beteget a rendelkezés lehetőségéről tájékoztatni kell. Ebben az esetben intézkedni kell, hogy a beteg tájékoztatási tiltása megjelenjék az informatikai rendszerből lekérhető listákon is.

Más hozzátartozók és egyéb személyek csak a gyógykezelt személy írásos felhatalmazása alapján kaphatnak tájékoztatást.

### 41. Egészségügyi dokumentációval kapcsolatos tájékoztatás

A beteg (törvényes képviselője) – képességeit is figyelembe véve – jogosult tájékoztatást kapni a rá vonatkozó személyazonosító és egészségügyi adatokról, betekinthet az egészségügyi dokumentációba, illetve azokról saját költségére másolatot kérhet.

Megkezdett, de még nem befejezett ellátás esetén a tájékoztatást az adott ellátással kapcsolatban a kezelőorvos adja meg. Folyamatban levő ellátás esetén a beteg a dokumentációról másolatot saját költségére kaphat a kezelőorvos által.

Távozott beteg esetén a dokumentációba betekintést és másolat kiadását a törvényi feltételek vizsgálata mellett az irattározással megbízott személy biztosítja. A tájékoztatásról nyilvántartást kell vezetni.

### 42. Elhunyt beteggel kapcsolatos tájékoztatás

A gyógykezelt beteg személy halála esetén a halál okával összefüggésbe hozható, továbbá a halál bekövetkeztét megelőző gyógykezeléssel kapcsolatos adatokat megismerheti az elhunyt

- törvényes képviselője,
- közeli hozzátartozója,
- örököse,

a jogcím hiteles igazolását követően.

A megjelölt személyek a fenti adatokról – saját költségükre – másolatot kaphatnak. A másolat kiadása az Igazgatóságon történik.

**Közeli hozzátartozó**: a házastárs, az egyeneságbeli rokon, az örökbe fogadott, a mostoha- és nevelt gyermek, az örökbe fogadó, a mostoha- és nevelőszülő, valamint a testvér és az élettárs[42];

## M) Az adatok biztonságos kezelése

Az egészségügyi és személyazonosító adatok kezelése során biztosítani kell az adatok biztonságát véletlen vagy szándékos megsemmisítéssel, megsemmisüléssel, megváltoztatással, károsodással, nyilvánosságra kerüléssel szemben, továbbá, hogy azokhoz illetéktelen személy ne férjen hozzá.

### 43. Adatfelvétel

Az adatfelvétel során az egészségügyi dokumentációban rögzíteni kell az adatfelvétel időpontját és az adatfelvevő személyét. A gyakorlatban a beteg dokumentációjába történt minden feljegyzést, beírást aláírással vagy kézjeggyel, és ha szükséges, dátummal hitelesíteni kell.
Az osztályokon a dolgozók aláírás mintáját nyilvántartásban kell rögzíteni. A nyilvántartás vezetéséért az osztályvezető felelős.

### 44. Adatmódosítás

Ha tévesztés, vagy más ok miatt a beírt adatot módosítani kell, ez csak úgy végezhető, hogy az eredeti adat megállapítható legyen. Módosításnál is kézjeggyel el kell látni a módosítást.

[42] Eütv. 3. § r) pont, Eüak.3. § j) pont

## 45. Eljárás az adatok sérülése esetén

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 pótlására annak a szervezeti egységnek a vezetője felelős, ahol a sérülés bekövetkezett. Az adatpótlásba be kell vonni azon betegellátó osztályok vezetőit, ahol a beteget kezelték és a kezelésről az adatok megsérültek. A pótolt adatokon a pótlás tényét fel kell tüntetni. A Pótlásról jegyzőkönyvet kell felvenni, amit az Igazgatónak kell hitelesítenie.

## 46. Egészségügyi dokumentáció megőrzése

| Sorsz. | Egészségügyi dokumentum leírása | Megőrzési időtartam |
|---|---|---|
| 1 | Zárójelentés | legalább 50 évig |
| 2 | Képalkotó diagnosztikai eljárással készült felvételt az annak készítésétől számított | 10 évig |
| 3 | A képalkotó diagnosztikai felvételről készített lelet | A felvétel készítésétől számított 30 évig |
| 4 | A gyógyszer, gyógyászati segédeszköz és gyógyászati ellátás kiszolgáltatója vagy nyújtója a papíralapú vényeket, illetve elektronikus vény kiváltásakor az emberi felhasználásra kerülő gyógyszerek rendeléséről és kiadásáról szóló rendelet szerint nyomtatott kiadási igazolást | 5 évig |
| 5 | Elektronikus vénynyilvántartás az EESZT-ben | Vény visszavonásától, felhasználásától vagy felhasználási idejének lejártától számított 5 év |
| 6 | Gyógyászati segédeszköz szaküzletben kiszolgáltatott olyan gyógyászati segédeszköz esetén, amelynek kihordási ideje 5 évnél hosszabb, a papíralapú vény, valamint a kiadási igazolás megőrzési ideje. | a kihordási idővel azonos |
| 7 | Az EESZT-hez informatikai rendszere útján csatlakozásra köteles gyógyszertár az egyes vényekre vonatkozó adatokat a vény visszavonásától, felhasználásától vagy felhasználási idejének lejártától számítva. | 30 év |
| 8 | Önrendelkezési nyilvántartás az EESZT rendszerében | az érintett halálát követő 5 év |
| 9 | Központi eseménykatalógus az EESZT-ben | az érintett halálát követő 5 év |
| 10 | Egészségügyi dokumentáció az EESZT-ben | Az Eüak. egészségügyi dokumentáció megőrzésére vonatkozó szabályai szerint |
| 11 | Egészségügyi profil az EESZT-ben | az érintett halálát követő 5 év |

| | | |
|---|---|---|
| 12 | Elektronikus beutalók és foglalások az EESZT-ben<br>A beutaló visszavonásától, felhasználásától vagy felhasználási idejének lejártától számítva | 5 év<br>(Ebtv. 18/A. § (3)) |
| 13 | Digitális képtovábbítás | az érintett halálát követő 5 év<br>(Eüak. 35/M. (1)) |
| 14 | Adatkezelési napló (adattovábbítási nyilvántartás) | 25 év |
| 15 | Nemzeti Szívinfarktus Regiszter | 50 év |
| 16 | Protézis Regiszter | 50 év |
| 17 | Egészségbiztosítási szerv | 50 év |
| 18 | A gyógyszer, gyógyászati segédeszköz és gyógyászati ellátás kiszolgáltatója vagy nyújtója a papíralapú vényeket, illetve elektronikus vény kiváltásakor az emberi felhasználásra kerülő gyógyszerek rendeléséről és kiadásáról szóló rendelet szerint nyomtatott kiadási igazolás | 5 év |

Az egészségügyi dokumentáció részeként meg kell őrizni:

- az egyes vizsgálatokról készült leleteket,
- a gyógykezelés és a konzílium során keletkezett iratokat,
- az ápolási dokumentációt,
- a képalkotó diagnosztikus eljárások felvételeit illetve az azokról készült leleteket

Az egészségügyi dokumentáció részét képező iratok megőrzéséért a betegellátó osztály és a titkárság vezetője a felelős az alábbi szabályozás szerint.

Az elektronikus adatok megőrzéséért a számítástechnikai osztály vezetője az írott anyagok kórlaptárba történő megőrzéséért a titkárság vezetője a felelős az érvényes kórlaptári szabályzat szerint.
A diagnosztikus eljárások felvételeinek megőrzéséért annak az osztálynak a vezetője a felelős, ahol a felvétel keletkezett.
A kötelező nyilvántartási időt követően gyógykezelés vagy tudományos kutatás érdekében - amennyiben indokolt - az adatok továbbra is nyilvántarthatók. Ha a további nyilvántartás nem indokolt - a[43] (3) bekezdés kivételével - a nyilvántartást meg kell semmisíteni. (1997.évi XLVII törvény 30§).

## 47. Egészségügyi és személyes adatok megsemmisítése

A 30, illetve 50 éves őrzés után az egészségügyi dokumentációt ezt követően meg kell semmisíteni. A megsemmisítés alól kivételt képeznek azok a dokumentumok, amelyek:

- a gyógykezelt személy 30 évnél korábbi kezelésével kapcsolatba hozhatók, vagy
- tudományos jelentőségük van.

[43] Amennyiben az egészségügyi dokumentációnak tudományos jelentősége van, a kötelező nyilvántartási időt követően át kell adni a Semmelweis Orvostörténeti Múzeum, Könyvtár és Levéltár részére

Tudományos jelentőségük lehet a dokumentumoknak a betegség vagy a kezelés jellege, a gyógykezelt személy, személyi vagy általános kultúrtörténeti okok miatt. Fentiek alapján a tudományos jelentőség elbírálására a kórház tudományos bizottsága jogosult.

A megsemmisítés alóli kivételre a betegellátó osztály vagy részleg vezetője tesz javaslatot az orvosigazgatónak. Amennyiben az egészségügyi dokumentációnak tudományos jelentősége van, a kötelező nyilvántartási időt követően át kell adni a Semmelweis Orvostörténeti Múzeum, Könyvtár és Levéltár részére. A megsemmisítés elbírálását, illetve a megsemmisítési eljárást valamennyi, a kórházban tárolt dokumentáció esetében le kell folytatni a dokumentációs szabályzat alapján.
**A megsemmisítési eljárást az intézményi dokumentációs szabályzat szabályozza.**
A megsemmisítés során is biztosítani kell az adatvédelmet. Ha a megsemmisítés az intézményen belül történik, a dokumentumokat olyan eljárással kell megsemmisíteni, ami lehetetlenné teszi a dokumentumok rekonstruálását. A megsemmisítésre vállalkozó szervezetnél is az adatvédelmet biztosítani kell.

### 48. Diagnosztikai vizsgálatok leleteinek megőrzése

A diagnosztikai vizsgálatok leleteinek megőrzése a diagnosztikai egységben történik. A kórházi informatikai rendszerben tárolt adatok esetében helyszíni adattárolás nem szükséges.

### N) közérdekű kérelmekkel, panaszokkal és bejelentésekkel kapcsolatos eljárás

A panasz, illetőleg a közérdekű bejelentés alapján - ha alaposnak bizonyul - gondoskodni kell:
a) a jogszerű, illetőleg a közérdeknek megfelelő állapot helyreállításáról vagy az egyébként szükséges intézkedések megtételéről;
b) a feltárt hibák okainak megszüntetéséről;
c) az okozott sérelem orvoslásáról, továbbá;
d) indokolt esetben a felelősségre vonás kezdeményezéséről.

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 30. § (6) bekezdés, valamint az államháztartásról szóló törvény végrehajtásáról szóló 368/2011. (XII.31.) Korm. rendelet 13. § (2) bekezdés h) pontjának előírásai alapján Gottsegen György Országos Kardiológiai Intézetnél a közérdekű adatok megismerésére irányuló kérelmek intézésének, továbbá a kötelezően közzéteendő adatok nyilvánosságra hozatalának rendje a „Közzétételi szabályzat” című szabályzatban került szabályozásra.

## III. MELLÉKLETEK

A szabályzat 4 mellékletet tartalmaz:
1. számú melléklet: GDPR szerinti adatkezelési elvek
2. számú melléklet: Az intézet területén működő számítógépes rendszerek adatvédelmi és adatmentési előírásai
3. számú melléklet: Várólisták
4. számú melléklet: Iratminták
5. számú melléklet: A beteg jogai az 1997. évi CLIV. törvény alapján
6. számú melléklet: EESZT