4845-001/2021

Dél-pesti Centrumkórház – Országos Hematológiai és Infektológiai Intézet	SZ-39

ADATVÉDELMI ÉS ADATKEZELÉSI SZABÁLYZAT

Készítette: ..... **Dátum:** 2021.04.01.
Berenczei Rezső
informatikai igazgató

Minőségügyi szempontból ellenőrizte: ..... **Dátum:** 2021.04.01.
Dohnál Erika
minőségirányítási irodavezető

Jogi szempontból ellenőrizte és jóváhagyta: ..... **Dátum:** 2021.04.01.
Dr. Ujvári Györgyi
jogi és igazgatási osztályvezető

Jóváhagyta: ..... **Dátum:** 2021.04.01.
Dr. Vályi-Nagy István
főigazgató

A dokumentum kódja	SZ-39
Változat száma	09
File név	SZ-39
Oldalak száma	75
Mellékletek száma	7
Hatálybalépés időpontja	2021.04.08.

Nyilvántartott példány: ☒ Munkapéldány: ☐

A példány sorszáma: 01

Ezen dokumentum továbbadása, sokszorosítása írásos engedélyhez kötött.

MÓDOSÍTÁSOK JEGYZÉKE

Módosította Aláírás/Dátum	Változat száma	Módosított oldalszám	Jogi szempontból ellenőrizte és jóváhagyta Aláírás/Dátum	Jóváhagyta Aláírás/Dátum	Kibocsátás időpontja
Berenczei Rezső 2021.10.15.	09	3, 10, 12, 16, 22, 43-44, 46-47, 54-57	Dr. Ujvári Györgyi 2021.10.15.	Dr. Vályi-Nagy István 2021.10.15.	2021.10.20.
Berenczei Rezső 2022.01.13.	09 02	5, 10-12 M01	Dr. Ujvári Györgyi 2022.01.13.	Dr. Vályi-Nagy [illegible] 2022.01.17.	2022.01.17.

TARTALOMJEGYZÉK

1. A SZABÁLYZAT CÉLJA 5

1.1. BEVEZETŐ RENDELKEZÉSEK 5
1.2. AZ ÁLTALÁNOS SZABÁLYOZÁS CÉLJA 6

2. ALKALMAZÁSI TERÜLET 7

2.1. AZ ÁLTALÁNOS SZABÁLYOZÁS SZEMÉLYI HATÁLYA 7
2.2. AZ ÁLTALÁNOS SZABÁLYOZÁS TÁRGYI HATÁLYA 7

3. AZ ILLETÉKESSÉG ÉS FELELŐSSÉG MEGHATÁROZÁSA 8

4. FOGALMAK, DEFINÍCIÓK 8

5. A SZABÁLYZAT LEÍRÁSA 13

5.1. DOKUMENTÁLÁSI KÖTELEZETTSÉG 13
5.1.1. Az adatkezelés bevezetéséhez, módosításához, megszüntetéséhez kapcsolódó dokumentálási kötelezettség 13
5.1.2. A hozzájárulások dokumentálása és tárolása 14
5.1.3. Az érintettek tájékoztatásának dokumentálása 14
5.1.4. Az Adatkezelői Nyilvántartás 15
5.2. AZ ADATVÉDELMI TEVÉKENYSÉG SZERVEZETE ÉS IRÁNYÍTÁSA AZ INTÉZMÉNYNÉL: AZ ADATVÉDELMI TEVÉKENYSÉG ELLÁTÁSÁBAN RÉSZTVEVŐK 15
5.3. ADATKEZELÉS BEVEZETÉSÉVEL, MÓDOSÍTÁSÁVAL ÉS MEGSZÜNTETÉSÉVEL KAPCSOLATOS FELADATOK. 23
5.3.1. Adatkezelés bevezetésével kapcsolatos feladatok 23
5.3.2. Adatkezelés megszüntetésével kapcsolatos feladatok 27
5.3.3. Az érdekmérlegelési teszt elvégzésének módszertana 27
5.3.4. Az adatvédelmi hatásvizsgálat elvégzésének módszertana 29
5.4. AZ ÉRINTETTI JOGOK GYAKORLÁSÁNAK ELŐSEGÍTÉSE 33
5.4.1. Az adatkezelési tevékenység nyilvánossága 33
5.4.2. A gyermekek tájékoztatáshoz való jogának biztosítása 34
5.4.3. Korlátozottan cselekvőképes és cselekvőképtelen (gondokság alatt álló) személyek tájékoztatáshoz való jogának biztosítása 34
5.4.4. Gyermekek és gondokság alatt álló személyek személyes adatainak kezelése hozzájáruló nyilatkozat alapján 35
5.4.5. Hozzátartozók tájékoztatása 35
5.5. AZ ÉRINTETTŐL SZÁRMAZÓ KÉRELMEK, PANASZOK MEGVÁLASZOLÁSÁNAK RENDJE 35
5.5.1. Az adatvédelmi bejelentések típusai 35
5.5.2. Az adatvédelmi beadványok kezelésének eljárásrendje 36
5.6. AZ ADATBIZTONSÁGI INTÉZKEDÉSEK (TECHNIKAI ÉS SZERVEZÉSI INTÉZKEDÉSEK) MEGHATÁROZÁSA ÉS VÉGREHAJTÁSA 42
5.7. A KÖZÖS ADATKEZELÉSI ÉS AZ ADATFELDOLGOZÁSI MEGÁLLAPODÁSOK MEGKÖTÉSÉNEK ÉS VÉGREHAJTÁSA ELLENŐRZÉSÉNEK SZABÁLYAI 43
5.7.1. Közös adatkezelési megállapodások 43
5.7.2. Adatfeldolgozási megállapodások 44
5.8. AZ ADATKEZELŐI NYILVÁNTARTÁS 46
5.9. AZ ADATVÉDELMI INCIDENSEK KEZELÉSE 48
5.9.1. Általános szabályok 48
5.9.2. Külső kommunikáció 48
5.10. AZ ADATVÉDELMI FELÜGYELETI HATÓSÁGOKKAL VALÓ KAPCSOLATTARTÁS 48
5.11. HARMADIK ORSZÁGBA IRÁNYULÓ ADATTOVÁBBÍTÁS KÜLÖNÖS SZABÁLYAI 51
5.12. BELSŐ ADATVÉDELMI ELLENŐRZÉSI ELJÁRÁS 52
5.13. EGÉSZSÉGÜGYI ADATVÉDELMI SZABÁLYOZÁS 54
5.13.1. Az egészségügyi szabályozás célja 54
5.13.2. Az általános szabályozás és az egészségügyi szabályozás kapcsolata 54
5.13.3. Az egészségi állapotra vonatkozó alapfogalmak 54
5.14. EGÉSZSÉGÜGYI ADATVÉDELEM 56

5.14.1. Az egészségügyi adatkezelés célja 56
5.14.1.1. Az egészségügyi és személyazonosító adat kezelésének célja 56
5.14.1.2. Az 5.14.1.1. pontban meghatározottakon túl - törvényben meghatározott esetekben - az alábbi célból lehet adatot kezelni 56
5.14.2. Egészségügyi adatkezelésre jogosultak köre 58
5.14.3. Titoktartási kötelezettség 58
5.14.4. A tájékoztatáshoz, valamint az önrendelkezéshez való jog, illetve kötelezettség 58
5.14.5. A gyógykezelés során jelenlévő személyek 60
5.14.6. Adatszolgáltatás az érintett részéről 60
5.14.7. A gyógykezelés céljából történő adatkezelés 61
5.14.8. Adattovábbítás az egészségügyi intézmény részéről jogszabály alapján 62
5.14.9. Közegészségügyi, járványügyi célból történő adatkezelés 63
5.14.10. Népegészségügyi célból történő adatkezelés 64
5.14.11. Az intézmény, mint betegségregisztert vezető szerv adatkezelése 64
5.14.12. Statisztikai célú adatkezelés 65
5.14.13. Tudományos kutatás céljából történő adatkezelés 65
5.14.14. Az egészségügyi és személyazonosító adatok nyilvántartása 67
5.14.15. Az egészségügyi dokumentáció megőrzése 68
5.14.16. Egészségügyi adatok, betegdokumentáció kérés, kiadás 68
5.14.17. Dokumentáció és adattárolás 69
5.14.18. Egészségügyi és személyazonosító adatok megsemmisítése 70
5.14.19. Adatfelvétel és módosítása 71
5.14.20. Adatvédelem az elektronikus adatkezelés során 71
5.15. AZ ÉRINTETT JOGAI 71
5.15.1. A hozzáféréshez való jog 71
5.15.2. A helyesbítéshez való jog 72
5.15.3. A törléshez való jog 72
5.15.4. A zároláshoz (adatkezelés korlátozásához) való jog 72
5.15.5. A tiltakozáshoz való jog 72
5.15.6. Az adathordozhatósághoz való jog 72
5.15.7. Hatósági és bírósági jogérvényesítéshez való jog 72
5.16. A SZABÁLYZATOKHOZ KAPCSOLÓDÓ JOGSZABÁLYOK, BELSŐ SZABÁLYZATOK 73
5.17. ZÁRÓ RENDELKEZÉSEK 74
6. HIVATKOZÁSOK 74
7. MELLÉKLETEK, ADATLAPOK JEGYZÉKE 75

679-001/2022

1. A SZABÁLYZAT CÉLJA

1.1. BEVEZETŐ RENDELKEZÉSEK

A Dél-pesti Centrumkórház- Országos Hematológiai és Infektológiai Intézet (a továbbiakban: Intézmény) jelen általános szabályozásban (a továbbiakban: Általános Szabályozás) határozza meg a tevékenységének ellátása, szolgáltatásának nyújtása során rendelkezésre bocsátott, vagy egyéb módon tudomására jutott személyes adatok kezelésével kapcsolatos egyes lényeges rendelkezéseket, különösen az adatvédelmi tevékenység irányításában, az adatvédelmi tevékenység ellátásában résztvevő szervezeti egységek feladatait és együttműködésük kereteit, valamint a természetes személyek személyes adatainak kezelésével és védelmével kapcsolatos irányelveket.

Az Általános Szabályozás hatálya alá tartozó személyek kötelesek a tevékenységük során az Intézmény kezelésében lévő személyes adatokat a mindenkori jogszabályi rendelkezéseknek megfelelően, így különösen a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679/EU európai parlamenti és tanácsi rendelet (a továbbiakban: GDPR), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) alkalmazandó rendelkezései, az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997 évi XLVII törvény (Eüak.), valamint az Intézményre irányadó egyéb hatályos magyar illetőleg európai uniós jogi normák rendelkezései szerint kezelni. Az Intézmény a személyes adatok kezelésével járó tevékenysége során érvényre juttatja a GDPR alapelveit, így különösen:

a) jogszerűség, tisztességes eljárás és átláthatóság elve: a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni;
b) célhoz kötöttség elve: a személyes adatok rögzítése csak meghatározott, egyértelmű és jogszerű célból történik, és azokat az Intézmény nem kezeli ezekkel a célokkal össze nem egyeztethető módon;
c) adattakarékosság elve: a kezelt személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk;
d) pontosság elve: a kezelt személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük, minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;
e) korlátozott tárolhatóság elve: a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé;
f) integritás és bizalmas jelleg: a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok

jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve;

g) beépített adatvédelem elve: olyan megfelelő technikai és szervezési intézkedések végrehajtása, amelyek már az adatkezeléssel járó folyamatok tervezésétől (az adatkezelés módjának meghatározásától) kezdődően az adatkezelés megszüntetéséig terjedő időszakban azt célozzák, hogy az adatvédelmi elvek hatékony megvalósítása, illetve a GDPR-ban foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépüljenek az adatkezelés folyamatába;

h) alapértelmezett adatvédelem elve: olyan technikai és szervezési intézkedések végrehajtása, amelyek biztosítják, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek, továbbá, hogy a gyűjtött személyes adatok mennyisége, kezelésük mértéke, tárolásuk időtartama és hozzáférhetőségük is csak az adatkezelési cél szempontjából szükséges mértékre korlátozódjon. Különösen azt kell biztosítani, hogy a személyes adatok alapértelmezés szerint természetes személy beavatkozása nélkül arra illetéktelen személyek számára ne válhassanak hozzáférhetővé.

Az Általános Szabályozás hatálya alá tartozó személyek kötelesek az olyan tevékenységük során, amely szükségszerűen együtt jár személyes adatok kezelésével, az adott tevékenységre vonatkozó – az 5.16. fejezetben felsorolt – speciális belső szabályzatokban foglalt rendelkezések mellett az Általános Szabályozás rendelkezései szerint eljárni.

Az Intézmény működése, tevékenységének ellátása, szolgáltatásának nyújtása során rendelkezésére bocsátott, vagy egyéb módon tudomására jutott személyes adatokat bizalmasan kezeli és a biztonságos adatkezelést elősegítő minden szükséges intézkedést megtesz.

1.2. Az Általános Szabályozás célja

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

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

Az Általános Szabályozás további célja, hogy meghatározza az Intézmény szervezeti egységeinél vezetett, személyes adatokat tartalmazó nyilvántartások vezetésének és működtetésének jogszerű rendjét, megőrzési időtartamát, valamint biztosítsa a személyes adatok védelme elveinek és az adatbiztonság követelményeinek érvényesülését.

Az Általános Szabályozásban hivatkozott szabályozó dokumentumok különösen:

a) Szervezeti és működési szabályzat (SZ-01)
b) Belső ellenőrzési szabályzat (SZ-53)
c) Az Intézmény Rendészeti és vagyonvédelmi szabályzata (SZ-30)
d) Informatikai biztonsági szabályzat (SZ-66)
e) Informatikai felhasználói szabályzat (SZ-41)
f) Az iratkezelés rendje – Iratkezelési szabályzat (SZ-48)
g) A postai küldemények fogadásáról és kezeléséről – Iratkezelési szabályzat (SZ-48)
h) Munkavédelmi szabályzat (SZ-14)
i) A panaszbejelentések kezelésének rendje – Panaszkivizsgálási szabályzat (SZ-13)
j) Az Intézmény humánkockázat kezelésének és humánbiztonsági intézkedéseinek rendje – Kockázatkezelés eljárásrendje (SZ-79)

2. ALKALMAZÁSI TERÜLET

2.1. AZ ÁLTALÁNOS SZABÁLYOZÁS SZEMÉLYI HATÁLYA

Az Általános Szabályozás személyi hatálya kiterjed az Intézmény részéről, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek (a munkavégzésre irányuló jogviszony jellegétől függetlenül), továbbá azon természetes személyekre (a továbbiakban: érintett), akik személyes adatait az Általános Szabályozás hatálya alá tartozó adatkezelések tartalmazzák, továbbá azon érintettekre, akik jogait vagy jogos érdekeit az adatkezelés érinti, továbbá az adatkezelési vagy adatfeldolgozási tevékenységet végző személyekre, partnerekre, továbbá az Intézmény adatkezelési tevékenységéhez eszközöket, számítástechnikai programokat szállító más személyekre is.

Az Intézmény megbízásából személyes adatok kezelését vagy feldolgozását végző személyekre.

2.2. AZ ÁLTALÁNOS SZABÁLYOZÁS TÁRGYI HATÁLYA

Az Általános Szabályozás 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 az 5.16. fejezetben felsorolt jogszabályok és belső szabályzatok szerint;
b) az egészségügyi ellátáson kívüli ügyfélkapcsolati jellegű adatkezelést valósítanak meg (az Intézménnyel kapcsolatba lépni szándékozó, kapcsolatban álló vagy kapcsolatban állt személyek, beleértve ezek meghatalmazottjait, képviselőit is);
c) foglalkoztatási jogviszonyhoz kapcsolódó adatkezelést valósítanak meg [az Intézménnyel egészségügyi szolgálat jogviszonyban, munkaviszonyban vagy egyéb

foglalkoztatási jogviszonyban (együtt: foglalkoztatási jogviszony) álló, állt, vagy foglalkoztatási jogviszonyba lépni szándékozó személyek);

d) az Intézménnyel szerződéses kapcsolatban álló természetes személyek, alapítványok, hatóságok, egyéb költségvetési szervek, stb. képviselőinek, kapcsolattartóinak az adataira vonatkoznak.

3. AZ ILLETÉKESSÉG ÉS FELELŐSSÉG MEGHATÁROZÁSA

A szabályzatban megfogalmazott tevékenységek végrehajtásában az alábbiak illetékesek, illetve felelősek.

▪ A szabályzat készítéséért:	informatikai igazgató.
▪ A szabályzat alkalmazásáért:	intézeti dolgozók.
▪ A szabályzat alkalmazásának ellenőrzéséért:	munkáltatói jogkör gyakorlók, informatikai igazgató, szervezeti egységek vezetői.
▪ A szabályzat szétosztásáért:	minőségirányítási dokumentáció-felelős.

4. FOGALMAK, DEFINÍCIÓK

Az Általános Szabályozás alkalmazása során az alábbi fogalmakat kell alkalmazni:

adat: az adatfajta értéke egy adott személy esetén; az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;

adatcsoport/adattípus: azonos ismérvekkel jellemezhető több adat együttesen (pl. személyazonosító adatok, jövedelmi adatok, stb.);

személyes adat: azonosított vagy azonosítható természetes személyre (érintett) vonatkozó bármely információ;

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;

adatfajta: a kezelt adatok típusának legkisebb egysége (pl. név, születési név, lakcím, telefonszám, havi jövedelem, stb.), ami a nyilvántartási rendszer felhasználói felületén egy rekordon belül rendszerint egy mezőt képez;

adathordozhatóság: hozzájáruláson vagy szerződésen alapuló, automatizált módon történő adatkezelés [GDPR 6. cikk (1) bek. a) és b) pont, 9. cikk (2) bek. a) pont] esetén az érintett azon joga, hogy a rá vonatkozó, általa az adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá azokat egy másik adatkezelőnek továbbítsa;

Adatkezelői Nyilvántartás: Az Általános Szabályozás 5.8. fejezetében meghatározott adattartalmú, folyamatosan karbantartott nyilvántartás;

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

adatgazda: intézményi szinten az Intézmény vezetője továbbá az egyes szervezeti egységek szintjén az SZMSZ és munkaköri leírás alapján felelős szervezeti egység vezetők, igazgatók, osztályvezetők, osztályvezető főorvosok;

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;

adatkezelési cél: az a pontosan meghatározott, jogszerű cél, amelynek elérése érdekében a személyes adatokon az adatkezelő az adatkezelési műveleteket végzi;

adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza. Az Intézmény szervezeti egységei által elhatározott vagy jogszabály rendelkezése alapján ellátott adatkezelések tekintetében az Intézmény minősül adatkezelőnek;

adatkezelésért felelős szervezeti egység (ld. még adatgazda): az Intézmény azon szervezeti egysége, amelynek feladatkörébe tartozik az Intézmény kezelésében lévő valamely nyilvántartási rendszer létrehozása, fenntartása, üzemeltetése, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik;

Adatkezelési megbízott: az adatgazda által kijelölt, az adatkezelésről rendelkező szervezeti egységhez tartozó, e feladatkör ellátására kijelölt, az Intézménnyel munkavégzésre irányuló jogviszonyban lévő személy. Az adatkezelésről rendelkező szervezeti egység felelősségi körébe tartozó adatkezelések tekintetében, vagy az adatkezeléseknek az adatkezelésről rendelkező szervezeti egység felelősségi körébe tartozó részében az adatkezelőt terhelő, az Általános Szabályozásban, illetve az adott adatkezelést szabályozó belső rendelkezésekben meghatározott feladatokat végzi;

Adatkezelésről rendelkező szervezeti egység: az a szervezeti egység, amely az Általános Szabályozás 5.3.1., 5.3.2. fejezetében foglalt rendelkezésekkel kapcsolatos döntési folyamatot kezdeményezi;

adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele[1]. Az Intézmény egyes szervezeti egységei közötti, illetve az adatfeldolgozónak történő adatátadás nem minősül adattovábbításnak;

adatvédelem: a személyes adatok jogszerű kezelését és feldolgozását, az adatok biztonságát, valamint az érintett személyek magánszférájának és személyhez fűződő jogainak védelmét

[1] Infotv. 3. § 11. pont

biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök, technikai és szervezeti intézkedések és módszerek összessége;

az adatvédelemért felelős szervezeti egységek: az Általános Szabályozás 5.2. fejezetében felsoroltak;

adatvédelmi esemény: az adatvédelmi rendellenesség és az adatvédelmi incidens;

adatvédelmi felelős: e feladatkör ellátására kijelölt, az Intézmény alkalmazásában álló személy, aki az Információbiztonsági és Adatvédelmi Osztály keretében, az adatvédelmi operatív tevékenységek ellátásán túl az Intézmény adatkezelési megbízottak közötti együttműködést koordinálja;

adatvédelmi felügyeleti hatóság: a Nemzeti Adatvédelmi és Információszabadság Hatóság - NAIH (a továbbiakban: Hatóság);

adatvédelmi hatásvizsgálat: olyan vizsgálat, amelyet az adatkezelésért felelős szervezeti egység kijelölt dolgozója (adatkezelési megbízott) köteles elvégezni, amennyiben valamely tervezett adatkezelés – figyelemmel annak jellegére, hatókörére, körülményeire és céljaira, ideértve különösen az új technológiák alkalmazásának esetét – személyekhez ezt a személyes adatot nem lehet kapcsolni;

adatvédelmi rendellenesség: az Intézmény Incidenskezelési Szabályzatának (Sz-83) rendelkezései szerint adatvédelmi incidensnek nem minősülő adatvédelmi esemény;

biometrikus adat: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai (ujjnyomat) adat;

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;

dolgozó: az Intézménnyel egészségügyi szolgálat jogviszonyban, illetőleg munkavégzésre irányuló egyéb jogviszonyban álló természetes személy

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

egyéb személyazonosító adatok: a személyes adatok bármely olyan kombinációja, amely alkalmas egy természetes személy azonosítására, vagyis más természetes személyektől való egyértelmű megkülönböztetésére;

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; 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;

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

harmadik ország: minden olyan állam, amely nem tagja az Európai Gazdasági Térségnek (EGT). Az EGT államai: az EU tagállamai, valamint Izland, Lichtenstein és Norvégia;

harmadik fél: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, aki, vagy 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;

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;

informatikai szakterület: az informatikai rendszerek üzemeltetéséért felelős szervezeti egység vagy egységek;

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

jogosultságkezelés: a személyes adatokhoz, informatikai rendszerekhez vagy egyéb erőforrásokhoz való hozzáférés kezelésének folyamata és módszere, beleértve különösen a jóváhagyásokat, szerepköröket, összeférhetetlenségi kontrollokat;

közérdekű adat: közfeladatot ellátó szerv 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;

személyes közreműködő: az egészségügyi szolgáltatás nyújtásában részt vevő olyan személy vagy szervezet, aki vagy amely a közreműködést igénybe vevő szolgáltató nevében, a közreműködést igénybe vevő szolgáltató szervezeti egysége által ellátott betegek részére személyesen nyújt egészségügyi szolgáltatást a közreműködést igénybe vevő szolgáltató szervezeti egysége által nyújtott szakmában, akként, hogy a felek között létrejött közreműködői szerződés alapján a feladat ellátásához szükséges tárgyi feltételeket kizárólag a

közreműködőt igénybe vevő szolgáltató biztosítja, a személyes közreműködő pedig kizárólag személyi feltételeket biztosít; (96/2003. (VII. 15.) Korm. rendelet 2. § (1) bekezdés n) pont).

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, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére, vagy szexuális irányultságára vonatkozó személyes adatok;

magatartási kódex: a GDPR 40. cikke alapján a GDPR rendelkezései hatékony és helyes alkalmazásának az elősegítése érdekében létrehozott, és az esettől függően a Nemzeti Adatvédelmi- és Információszabadság Hatóság vagy az Európai Bizottság által jóváhagyott előírások összessége, amely figyelembe veszi az ágazaton belüli adatkezelés sajátosságait;

munkavállalói személyes adat: az Intézménnyel foglalkoztatási jogviszonyban álló személyek adata;

munkavégzésre irányuló egyéb jogviszony: a munkavégzési kötelezettséggel járó vállalkozási és megbízási szerződés;

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

profilalkotás: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;

személyazonosító adat: a személyes adatok közül azok, amelyek szükségesek és elégségesek egy természetes személy más természetes személytől való egyértelmű megkülönböztetésére (azonosítására), melyen belül megkülönböztetünk természetes és egyéb személyazonosító adatokat;

természetes személyazonosító adatok: az 1996. évi XX. törvény szerinti adatok (az érintett családi és utóneve, születési családi és utóneve, születési helye, születési ideje és anyja születési családi és utóneve);

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. amely megvalósulhat adat szintjén, adatcsoport szintjén, egy személyhez kapcsolódó valamennyi adat szintjén, adatbázis/nyilvántartási rendszer része vagy egésze szintjén. A törlés célja megvalósítható deperszonalizálással (anonimizálással) is;

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

5. A SZABÁLYZAT LEÍRÁSA

5.1. DOKUMENTÁLÁSI KÖTELEZETTSÉG

Az Intézmény részéről illetőleg érdekében eljáró valamennyi személy köteles a személyes adatok kezelésére vonatkozó alapelveket [GDPR 5. cikk (1) bek.] betartani. Az Intézménynek, mint adatkezelőnek 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 nyilvántartás elektronikus módon az Országos Kórházi Főigazgatóság (a továbbiakban: OKFŐ) által biztosított az Ágazati Tudásközpont által felügyelt szoftvertermék használatával történik.

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 és az **Incidenskezelési szabályzat**nak **(SZ-83)** megfelelően – nyilvántartást vezet a bekövetkezett incidensekkel kapcsolatos tényekről és intézkedésekről az OKFŐ által biztosított az Ágazati Tudásközpont által felügyelt szoftvertermék használatával.

Az adatkezelési tájékoztatók elkészítéséről az adatvédelmi felelős az adatkezelési megbízottak közreműködésével, gondoskodik. Az adatkezelési tájékoztatókat rendszeresen, legalább évente egyszer az adatvédelmi tisztviselő az adatvédelmi felelős bevonásával felülvizsgálja. Adatkezelő törekszik a felülvizsgálatot az intézeti működéssel kapcsolatos audittal összekötni.

5.1.1. Az adatkezelés bevezetéséhez, módosításához, megszüntetéséhez kapcsolódó dokumentálási kötelezettség

Az Intézmény az adatkezelést érintő minden tevékenységről, beleértve az adatkezelés megkezdésére, megváltoztatására irányuló bármely és valamennyi igényt, szándékot, az adatkezelést érintő valamennyi és bármely döntést írásban, dokumentálható és visszakereshető formában rögzíti és tárolja az OKFŐ által biztosított az Ágazati Tudásközpont által felügyelt szoftvertermék nyilvántartási rendszerében. Ennek során rögzíteni kell az adatkezelés megkezdésére és megváltoztatására irányuló igény, szándék felmerülésének, valamint az adatkezelést érintő valamennyi és bármely döntés, illetve az adatkezelést érintő minden további tevékenység időpontját, célját, továbbá annak a szakterületnek és adatgazdának a megnevezését, ahol az adott igény felmerült, illetve annak a szakterületi vezetőnek a megnevezését és aláírását, aki az adott adatkezelési igényt megfogalmazta.

Amennyiben adatkezelésre érdekmérlegelési teszt elvégzését követően jogos érdek alapján kerül sor, az Intézmény írásban, dokumentálható és visszakereshető formában rögzíti és tárolja az érdekmérlegelési teszt megállapításait, eredményét és az arról készült egyéb dokumentációt. Az érdekmérlegelési teszt elvégzésére vonatkozó részletszabályokat az Általános Szabályozás 5.3.3. fejezete tartalmazza.

Amennyiben adatkezelésre hatásvizsgálat elvégzését követően kerül sor, Intézmény az írásban, dokumentálható és visszakereshető formában rögzíti és tárolja a hatásvizsgálat megállapításait, eredményét és az arról készült egyéb dokumentációt. A hatásvizsgálat elvégzésére vonatkozó részletszabályokat az Általános Szabályozás 5.3.4. fejezete tartalmazza.

5.1.2. A hozzájárulások dokumentálása és tárolása

Amennyiben a személyes adat kezelésének jogalapjai (GDPR 6. cikk) valamint az Info tv. az adatkezelés jogalapja és általános feltételeiről szóló rendelkezései az adott személyes adat kezelését az érintett hozzájárulása alapozza meg, az Intézménynek képesnek kell lennie annak igazolására, hogy az érintett a személyes adatainak kezeléséhez hozzájárult. Amennyiben az adatkezelés során kétség merül fel az érintett hozzájárulásának kérése tekintetében, a szükséges iránymutatás érdekében az adatvédelmi felelőshöz kell fordulni. Az érintetteknek az Intézmény egyes adatkezelési tevékenységeihez hozzájáruló valamennyi – írásban, online felületen, elektronikus üzenet, illetve videochat útján és egyéb úton tett – nyilatkozatát, továbbá az Intézmény minden, ezzel kapcsolatos nyilatkozatát dokumentálható és visszakereshető formában kell rögzíteni, nyilvántartani és tárolni. A hozzájáruló nyilatkozatokat abban az ügyben kell rögzíteni az iratkezelési szabályok figyelembevételével, amelyben a személyes adatok kezeléséhez az érintett hozzájárult. A hozzájáruló nyilatkozatokkal kapcsolatos feladatok (rögzítés, nyilvántartás, tárolás, megsemmisítés stb.) ellátását valamennyi érintett szakterületnek a saját feladatai elvégzése során, saját hatáskörben kell elvégeznie.

Az érintett hozzájárulásának visszavonását a hozzájárulás megadásával azonos módon kell biztosítani, dokumentálni és a visszavonásról szóló nyilatkozatot tárolni.

Amennyiben az adatkezelés jogalapja az érintett hozzájárulása, úgy a hozzájárulás visszavonása esetén az Intézmény a hozzájárulás alapján kezelt adatokat a GDPR 17. cikke és az Infotv. személyes adatok törlésére vonatkozó rendelkezései figyelembevételével törli.

Az Intézmény a hozzájáruló nyilatkozatokat és a hozzájárulás visszavonását tartalmazó nyilatkozatokat az adott adatkezelésre vonatkozó tájékoztatóban meghatározott ideig megőrzi. A megőrzési időt követően a nyilatkozatokat megsemmisíti.

5.1.3. Az érintettek tájékoztatásának dokumentálása

Az Intézmény megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó valamennyi szükséges információt és minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és

közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében.

Az érintettnek címzett tájékoztatás rendelkezésre bocsátását dokumentálható és visszakereshető formában a tájékoztatást nyújtó szervezeti egységnél rögzíteni kell.

5.1.4. Az Adatkezelői Nyilvántartás

Az Intézmény valamennyi adatkezelési tevékenységéről és adatfeldolgozási tevékenységéről az Általános Szabályozás 5.8. fejezetben meghatározottak szerint nyilvántartást vezet. (a továbbiakban: Adatkezelői Nyilvántartás)

Az adatkezelői nyilvántartás napra készen tartása az Általános Szabályozás 5.8. fejezetben meghatározottak szerint az adatkezelési megbízottak feladata az adatvédelmi felelős felügyelete mellett.

Az Adatkezelői Nyilvántartásban szereplő adatokat illetően az Intézmény az egyes adatkezelések vonatkozásában tett megkeresésekre az Általános Szabályozás 5.5. fejezet rendelkezései szerint nyújt tájékoztatást.

5.2. AZ ADATVÉDELMI TEVÉKENYSÉG SZERVEZETE ÉS IRÁNYÍTÁSA AZ INTÉZMÉNYNÉL: AZ ADATVÉDELMI TEVÉKENYSÉG ELLÁTÁSÁBAN RÉSZTVEVŐK

Az az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv) .és végrehajtására kiadott jogszabályok, a szervezeteknek az elektronikus információs rendszereik védelmét biztosító kötelezettségei között felsorolt előírásainak (ld: szerepkörök), valamint az **Informatikai biztonsági szabályzat** (SZ-66) rendelkezéseinek megfelelően az adatvédelmi tevékenység irányításában és ellátásában az Intézmény döntési jogosultsággal rendelkező vezetői, illetőleg szervezeti egységei – az Intézmény Szervezeti és működési szabályzatában meghatározott feladatkörükön belül – az alábbiak szerint vesznek részt.

A főigazgató
(intézményi szintű adatgazda) felelős azért, hogy az Intézmény – mint adatkezelő, illetve adatfeldolgozó – működése az adatvédelmi szabályoknak megfeleljen. Ennek érdekében:

a) gondoskodik az adatvédelmi tevékenység irányításában és ellátásában résztvevő szervezeti egységek kijelöléséről, feladataik, az adatvédelmi tárgyú ügyekkel kapcsolatos döntési jogkörök meghatározásáról, az egyes adatkezelési döntési szintek kialakításáról;
b) biztosítja az adatvédelmi tevékenység irányításához és ellátásához, valamint az érintett jogai gyakorlásához szükséges személyi és tárgyi feltételeket;
c) gondoskodik az adatvédelmi tevékenység során esetleg előforduló, feltárt hiányosságok megszűntetéséről, szükség szerint a felelősségre vonásról;
d) kinevezi az Intézmény adatvédelmi tisztviselőjét, és az adatvédelmi tisztviselő nevét és elérhetőségét bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak,
e) megbízást ad az Intézmény adatvédelmi felelősének a feladatai ellátására;
f) munkajogi értelemben vett közvetlen felettese az adatvédelmi tisztviselőnek.

Az Orvosigazgató
az Intézmény szakmai működését vezeti, ennek keretein belül az adatvédelmi tisztviselő, valamint adatvédelmi felelős javaslatai alapján ellátja az érintetti jogok gyakorlásával kapcsolatos beadványok megválaszolását (5.5.2. pont) a személyes adatok kezelését, illetve a GDPR szerinti jogaik gyakorlását érintő panaszok (5.5.1. pont j) alpont) kivételével.

Az adatkezelésért felelős szervezeti egység vezetője (adatgazda)
az irányítása alá tartozó szervezeti egység tekintetében:

a) betartja és betartatja **Adatvédelmi és adatkezelési- (SZ-39)**, az **Informatikai biztonsági (SZ-66)**, valamint **Informatikai felhasználói szabályzatok (SZ-41)** előírásait; az adatvédelmi tisztviselővel, az adatvédelmi felelőssel, információbiztonsági felelőssel, a Jogi és Igazgatási Osztállyal, valamint az Információbiztonsági és Adatvédelmi Osztály információbiztonsági szakterületével együttműködve gondoskodik e szabályzatok megismertetéséről, rendszeres oktatásáról;
b) ellenőrzi, hogy a szervezeti egység által foglalkoztatottak rendelkeznek-e aláírt az Adatvédelmi, információbiztonsági, titokvédelmi követelmények tudomásul vételéről szóló nyilatkozattal, amennyiben nem, megteszi a megfelelő intézkedéseket eziránt és gondoskodik azok megküldéséről a Bérszámfejtési, Munkaügyi és Humánpolitikai Osztály részére,
c) kijelöli az irányítása alá tartozó szervezeti egység adatkezelési megbízottját és értesíti az adatvédelmi felelőst, illetve az adatvédelmi tisztviselőt az adatkezelési megbízott nevéről, elérhetőségéről és az általa felügyelt adatkezelésről. Utasítja az adott szakmai terület adatkezelési megbízottját, hogy az értesítéssel egyidejűleg az Adatkezelői Nyilvántartást – 5.8. fejezet – megfelelően módosítsa, gondoskodik az adatkezelési megbízotti feladatok ellátásának személyi és tárgyi feltételeiről;
d) gondoskodik arról, hogy az irányítása alá tartozó szervezeti egységek felelősségi körébe tartozó nyilvántartási rendszerek naprakészek, megbízhatóak legyenek;
e) gondoskodik arról, hogy az irányítása alatt álló személyek az adatkezelés meghatározott feltételeinek megfelelően járjanak el [GDPR 32. cikk (4) bek.];
f) az adatkezelési megbízott előterjesztésére – az Intézmény döntés-előkészítésre vonatkozó szabályainak megfelelően – dönt az Adatvédelmi és adatkezelési szabályzatban, illetve az adatkezeléssel járó folyamatot szabályozó egyéb belső szabályzatokban a feladat- és hatáskörébe utalt kérdésekben.

Az adatkezelési megbízott
a feladatkörébe tartozó adatkezelések tekintetében:

a) az Intézmény általános biztonsági szabályairól szóló **SZ-30 Rendészeti és vagyonvédelmi szabályzat**ban írottak figyelembevételével megfogalmazza az adott szakterület egyedi, a személyes adatok kezelésével járó munkafolyamatok biztonsági és fizikai hozzáférés-védelmi szabályait és eljárásait;
b) az **SZ-66 Informatikai biztonsági szabályzat**ban foglaltak szerint megfogalmazza a személyes adatokhoz történő, hozzáférésre vonatkozó specifikus szabályokat és eljárásokat;

c) betekinthet mindazon belső eljárásba és dokumentumokba (pl. kockázatfelmérés, üzletmenet-folytonossági terv, kármértékek meghatározása), amelyek az adatok biztonsági osztályba sorolásához, az adatkezelési feltételek meghatározásához szükségesek;
d) köteles az adatvédelmi és információbiztonsági szakirányítás mellett, évente legalább egyszer, az adatkezelési megbízotti feladatok ellátásához szükséges ismeretek naprakészsége érdekében tartott képzésen, továbbképzésen részt venni;
e) előkészíti az adatkezeléssel kapcsolatos, az adatkezelőt terhelő döntéseket, illetve abban közreműködik a végrehajt (at) ásukban;
f) az adatvédelmi felelős szakmai támogatása mellett gondoskodik az adatkezeléshez kapcsolódó adminisztratív teendők ellátásáról, az abban való közreműködésről (az adatkezeléssel összefüggő döntések dokumentálása, adatkezelői nyilvántartás karbantartása, közreműködés az érdekmérlegelési teszt elvégzésében, közreműködik a hatásvizsgálat lefolytatásában, az adatkezeléssel összefüggő szerződések előkészítésében, stb.);
g) együttműködik az ugyanazon adatkezelésben érintett más szakterületek adatkezelési megbízottjaival;
h) az információbiztonsági felelős szakmai támogatása mellett az erre vonatkozó szabályzatok szerint előkészíti az információbiztonsági szakértelmet nem igénylő adatbiztonsági intézkedéseket, közreműködik az Intézmény kezelésében lévő az adatok biztonsági osztályba sorolásában;
i) Az Információbiztonsági és Adatvédelmi Osztály támogatása mellett közreműködik az adatvagyon-felmérésben, jogosultságkezelés felülvizsgálatban;
j) az adatvédelmi tisztviselő és az adatvédelmi felelős támogatásával közreműködik az érintettek jogai gyakorlásának biztosításában, adatvédelmi incidens következményeinek elhárításában, adatvédelmi vizsgálatokban;
k) amennyiben az Intézmény adatfeldolgozóként jár el, közreműködik a feladatkörébe tartozó adatkezelési tevékenység tekintetében az adatfeldolgozót terhelő adminisztratív kötelezettségek ellátásában;
l) közreműködik az adatkezeléssel kapcsolatos oktatások megszervezésében.

Adatkezelési megbízotti feladatokra kizárólag az Intézménnyel határozatlan idejű munkavégzésre irányuló jogviszonyban álló személy jelölhető ki. Az adatkezelési megbízottaknak informatikai szakképesítéssel nem kötelező rendelkeznie, azonban a feladatok természete miatt haladó számítógépes felhasználói tudás indokolt. Egy munkatárs egyidejűleg több folyamat adatkezelési megbízottja is lehet.

Amennyiben a munkafolyamat több szakterületet érint, a szakterületet felügyelő igazgatók közös megegyezéssel döntenek az adatkezelési megbízott kijelöléséről. A döntéshozatal előtt az adatvédelmi felelős és az információbiztonsági felelős véleményét ki kell kérni.

Az adatkezelési megbízotti feladatokat ellátó munkatárs áthelyezése vagy munkaviszonyának megszüntetése esetén új adatkezelési megbízottat kell kijelölni. Az új adatkezelési megbízott

kijelöléséről az áthelyezést vagy a munkaviszony megszűnését követően, legkésőbb 15 napon belül gondoskodni kell.

Az adatkezelési megbízotti feladatok munkaköri leírásban szerepeltetését az adatkezelési megbízott kijelöléssel egyidejűleg a kijelölő vezető kezdeményezi.

Az adatkezelési megbízotti feladatok ellátásával kapcsolatos felelősségre a munkajogi szabályok az irányadók. Az adatkezelési megbízotti feladatokat ellátó munkatárs 15 munkanapot meghaladó távolléte esetén helyettesítéséről gondoskodni kell.

Egy vagy több adatkezelési megbízottat kell kijelölni a következő szervezeti egységeknél: Főigazgató közvetlen alárendelt szervezetei, Orvosigazgatóság, Gazdasági Igazgatóság, Ápolási Igazgatóság, Stratégiai Igazgatóság, Informatikai Igazgatóság és Országos Hematológiai és Infektológiai Intézet. Egy adatkezelési megbízott több igazgatóságra is kijelölhető. A kijelölést a szakmai, szervezeti és személyi szempontok szem előtt tartásával úgy kell végrehajtani, hogy minden szakterület megfelelően lefedésre kerüljön adatvédelmi szempontból. A kijelölés az igazgatóságok élén álló igazgatók jogkörébe és felelősségébe tartozik.

Adatkezelési megbízottnak olyan személyt kell kijelölni, aki az adott szakterületet, adminisztratív folyamato(ka)t, illetve – az informatikai szakterületen – a szakterületek tevékenységét támogató informatikai rendszereket illetően kellő ismeretekkel bír (adott szakterület vezetője döntése alapján egy adatkezelési megbízott több osztály adatkezelési feladatait is elláthatja).

Az információbiztonsági és informatikai szakterület szervezeti egységei
az Intézmény **SZ-01 Szervezeti és működési szabályzat**ában, valamint az Intézmény **SZ-66 Informatikai biztonsági szabályzat**ában meghatározott feladatkörükben

a) ellátják az informatikai biztonsággal kapcsolatos feladatokat a folyamatos üzemeltetési feladatok kivételével, különösen az Intézmény **Informatikai biztonsági szabályzat**ában (**SZ-66**) 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 érintett szervezeti egységek vezetőivel együttműködve gondoskodnak az információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról.
d) az informatikai rendszerek üzemeltetése területén ellátják a személyes adatok kezelésével kapcsolatos technikai védelem megvalósítását, ellátják – az Intézmény **Informatikai biztonsági szabályzat**ában (**SZ-66**) – hatáskörükbe tartozó információbiztonsági feladatokat (beleértve a káros külső behatások elleni védelmet és a jogosultságkezelés általa felügyelt területeit), valamint rendelkezésre állási kontrollok biztosítását, a tárolt és továbbított személyes adatok bizalmasságának

védelmét (pl. tesztadatbázisok álnevesítése vagy deperszonalizálása, különleges adatok maszkolása/titkosítása), az incidensfelderítési és -kezelési tevékenység támogatását,

Az információbiztonsági felelős (elektronikus információs rendszer biztonságáért felelős személy[2])
az Informatikai Biztonsági Szabályzatban foglalt tevékenységén túl az adatkezelési megbízottak munkáját az alábbiak szerint támogatja:

a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról;
b) elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését;
c) előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot
d) Az Adatvédelmi és adatkezelési szabályzatban és az **SZ-66 Informatikai biztonsági szabályzat**ban írottak figyelembevételével meghatározza az adatok címkéit (személyes adat, üzleti titok, stb.), valamint azok osztályba sorolásának keretrendszerét, biztonsági osztályok jellemzőit bizalmasság, sértetlenség, rendelkezésre állás szempontjából;
e) előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását;
f) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit
g) Az **SZ-66 Informatikai biztonsági szabályzat** előírásai figyelembevételével megfogalmazza az adatátviteli (kódolási és szállítási) feltételeket, szabályokat és eljárásokat (pl. csak titkosított adatátvitel lehetséges);
h) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal

Az információbiztonsági szakterület adatkezelési megbízottja
Az adatkezelés során (informatikai rendszerben kezelt adatok esetén az informatikai rendszer üzemeltetési szakaszában) – a feladatkörébe tartozó kérdésekben – gondoskodik arról, hogy az adatkezelés általános adatbiztonsági kontrolljainak működtetése az erre vonatkozó eljárásrendeknek és az információbiztonsági 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.

[2] https://nki.gov.hu/hatosag/tartalom/gyik/

Bérszámfejtési, Munkaügyi és Humánpolitikai Osztály
A dolgozók személyi anyagait őrzi az adatvédelmi, információbiztonsági és titokvédelmi nyilatkozatokkal együtt (**M01** melléklet).

A Jogi és Igazgatási Osztály:

a) szakmai támogatást nyújt az adatkezeléssel összefüggő, nem adatvédelmi jogszabályok értelmezésében,
b) az Intézmény belső szabályozók előkészítésére és kiadására vonatkozó szabályai szerint biztosítja, hogy az adatvédelmi felelős, valamint tisztviselő a Jogi és Igazgatási Osztály véleményét és jóváhagyását kikérje az Intézmény adatvédelmi tárgyú vagy adatvédelmi vonatkozású belső szabályzatainak előkészítése során,
c) Adatvédelmi jogsértés gyanúja esetén a NAIH hivatalból történő, illetőleg az érintetti megkeresés folytán lefolytatott vizsgálatában, és az abban való együttműködés során történő kapcsolattartásban való közreműködés
d) véleményezi az adatvédelmi felelős valamint tisztviselő hatáskörébe tartozó általuk előkészített dokumentumok tervezeteit;
e) az adatvédelmi jogi szempontok kivételével a jogi megfelelőség szempontjából véleményezi az adatkezeléssel összefüggő szabályzatok, tájékoztatók, nyilatkozatok, szerződések tervezeteit, valamint az adatkezelésekkel kapcsolatban készített javaslatok, előterjesztések tervezeteit;

Az Információbiztonsági és Adatvédelmi Osztály:

a) biztosítja az adatvédelmi felelős valamint tisztviselő feladatainak ellátásához szükséges személyi és tárgyi feltételeket;
b) közreműködik az adatvédelmi felelőshöz valamint tisztviselőhöz érkezett adatvédelmi bejelentések megválaszolásában, illetve az adatvédelmi események kivizsgálásában;
c) ellátja az Általános Szabályozásban és egyéb szabályzatokban meghatározott információbiztonsági, incidenskezelési feladatokat.
d) ellátja az adatkezelési megbízottak adatvédelemmel és adatbiztonsággal összefüggő szakmai felügyeletét.

Az Intézmény megbízott kommunikációs vezetője

a) adatvédelmi incidens esetén közreműködik az érintettek tájékoztatásának módjáról és a tájékoztatás tartalmáról való döntés előkészítésében,
b) adatvédelmi incidens esetén – az adatvédelmi tisztviselő közreműködésével – szükség esetén sajtóközleményt bocsát ki és kizárólagos kapcsolatot tart a sajtó képviselőivel.

Az adatvédelmi felelősre és tisztviselőre vonatkozó közös szabályok

a) Az adatvédelmi tisztviselőt/felelőst az Intézmény Főigazgatója nevezi ki/ bízza meg az olyan, az Intézménnyel munkavégzésre irányuló foglalkoztatási jogviszonyban álló természetes személyek közül, aki ismeri az Intézmény működését, feladatait, munkafolyamatait és rendelkezik:
    aa) jogi szakvizsgával vagy informatikai főiskolai (BSc) vagy egyetemi (MSc) szintű végzettséggel;

ab) az európai és hazai adatvédelemmel kapcsolatos főbb szabályozók, hatósági és bírósági határozatok, iránymutatások ismeretével;
ac) alapvető adatvédelmi és informatikai folyamatok ismeretével;
ad) legalább 2 év adatvédelmi területen szerzett gyakorlattal.

b) Az Intézményben nem lehet adatvédelmi felelős valamint tisztviselő az a természetes személy, aki az Intézményben az adatkezelési tevékenység céljainak, kereteinek, eszközeinek meghatározásáról dönt, különösen a főigazgató, adatkezelésért felelős szervezeti egység vezetője és a belső ellenőr.

c) Az Intézmény elősegíti az adatvédelmi felelős valamint tisztviselő megfelelő szakmai feladatellátását, ennek érdekében az Intézmény biztosítja különösen az adatvédelmi felelős valamint tisztviselő feladatai végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáférést, valamint a szakértői szintű ismereteinek fenntartásaihoz szükséges továbbképzések biztosítását, elegendő idő biztosítását feladatai ellátásához:

ca) 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;
cb) a felügyeleti hatósággal történő együttműködés során, amellyel az adatvédelmi tisztviselő – az adatvédelmi felelős, a Jogi és Igazgatási Osztály és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – tartja a kapcsolatot.

d) Az adatvédelmi tisztviselőt valamint felelőst tisztségük fennállása alatt és annak megszűnését követően titoktartási kötelezettség terheli a tevékenysége során tudomására jutott, nem közérdekűnek illetőleg nem közérdekből nyilvános adatnak minősülő információk kapcsán.

Adatvédelmi felelős

a) szükség esetén szakmai fórum indítását kezdeményezi az adatvédelmi követelményeknek való megfelelés biztosítása érdekében;
b) az Intézmény adatvédelmi szabályozási tevékenységének ellátása, a Jogi és Igazgatási Osztállyal és az információbiztonsági szakterülettel együttműködve szabályozó dokumentumok, normatívák, különösen az Adatvédelmi és Adatkezelési Szabályzat kidolgozása és karbantartása;
c) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
d) asszisztenciát nyújt az adatvédelmi tisztviselőnek, szakmai támogatást az adatkezelési megbízottaknak, illetve az Intézmény szervezeti egységeinek a személyes adatok kezelésével és védelmével kapcsolatos szabályok alkalmazásáról,
e) ellenőrzi az adatvédelemre és az adatkezelésre vonatkozó jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;

f) az érintett szakterületek és a Jogi és Igazgatási Osztály bevonásával kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
g) vezeti a belső adatvédelmi nyilvántartást;
h) gondoskodik az adatvédelmi ismeretek oktatásáról.
i) az adatvédelmi tisztviselő szakmai irányítása mellett

ia) közreműködik az Info tv. által meghatározott feladatok ellátásában, az Általános Adatvédelmi Rendelet (GDPR,2016/679/EU) követelményeinek érvényre juttatásában;

ib) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;

ic) ellenőrzi a GDPR, az Info tv. és az adatkezelésre vonatkozó más jogszabályok, valamint a Szabályzat, továbbá az Intézmény egyéb belső szabályzatai rendelkezéseinek a megtartását, belső adatvédelmi ellenőrzési eljárást folytat le;

id) a Jogi és Igazgatási Osztállyal együttműködve személyes adatok kezelésére vonatkozó előírásokról tájékoztatást nyújt, tanácsot ad;

ie) személyes adatot is kezelő új informatikai rendszer belső fejlesztéssel történő bevezetése során közreműködik az adatvédelmi hatásvizsgálat lefolytatásában;

if) az adatvédelmi incidenskezeléssel kapcsolatban ellátja az Általános Szabályozás szerinti feladatokat.

Az adatvédelmi felelős véleményét – az Általános Szabályozás rendelkezései szerint – ki kell kérni az adatkezelést érintő döntések, szerződések és belső szabályzatok tervezetéről.

Az adatvédelmi tisztviselő feladatai (DPO):

a GDPR 39. cikke valamint az Info tv. adatvédelmi tisztviselőre vonatkozó rendelkezései szerinti, illetve az Adatvédelmi és adatkezelési szabályzatban meghatározott feladatok ellátásával elősegíti az Intézmény adatvédelmi megfelelőségének biztosítását, így különösen

a) kapcsolatot tart és – az adatvédelmi felelős, a Jogi és Igazgatási Osztály és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – együttműködik a Hatósággal;
b) az OKFŐ számára adatszolgáltatást teljesít.
c) felügyeli az adatvédelmi tevékenység irányításában és ellátásában részt vevő szervezeti egységek adatvédelemmel összefüggő tevékenységét, az ugyanazon adatkezelésben érintett szakterületek közötti vita esetén javaslatot tesz a nézetkülönbségek feloldására;
d) szakmai irányítást gyakorol az Intézmény, különösen az adatvédelmi felelős adatvédelmi tevékenysége felett;
e) a Jogi és Igazgatási Osztállyal, valamint az Információbiztonsági és Adatvédelmi Osztállyal elősegíti az Intézmény alkalmazottai adatvédelmi tudatosságának növelését (rendszeres, évente legalább egyszer képzés, szakmai fórum, hírlevél stb.),
f) éves összefoglaló jelentést készít az Intézmény főigazgatójának;

Az adatvédelmi tisztviselő független, függetlensége biztosítása érdekében szakmai feladatai ellátása során utasítást nem fogadhat el, szakmai feladatai ellátásával összefüggésben nem bocsátható el. Az Általános Szabályzatban foglalt tevékenysége ellátása során autonóm, szakmai ügyekben kizárólag az Intézmény főigazgatójának tartozik felelősséggel.

Az adatvédelmi tisztviselő az adatvédelmi tisztviselői feladatokon kívül az Intézmény főigazgatója 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.

5.3. ADATKEZELÉS BEVEZETÉSÉVEL, MÓDOSÍTÁSÁVAL ÉS MEGSZÜNTETÉSÉVEL KAPCSOLATOS FELADATOK

5.3.1. 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 döntés-előkészítés rendjére vonatkozó belső szabályokat e fejezet rendelkezéseit figyelembe véve kell alkalmazni.

(1) A leendő adatkezelésért annak tárgya szerint felelős adatgazda az adatkezelési megbízott útján – az adatkezelési tevékenységhez kapcsolódó szakterület adatgazdájával, a többi érintett adatkezelési megbízottal illetőleg az adatvédelmi felelőssel együttműködve

az adatkezelési igény felmerülésekor:

a) meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, a személyes adatok továbbítására (címzettek, harmadik országba továbbítás), tárolására (pl. elektronikus, papíralapú), archiválására, törlésére, megsemmisítésére vonatkozó szabályokat és eljárásokat, valamint az adatkezelés egyéb feltételeit (különösen hatásvizsgálat/érdekmérlegelési teszt elvégzése, adatfeldolgozó/közös adatkezelő bevonása, automatizált döntéshozatali/profilalkotási módszer, hozzájáruló nyilatkozat, harmadik személy létfontosságú érdekének azonosítása, stb.) és ilyen tartalmú javaslatot készít a döntésre jogosultnak (GDPR 4. cikk 7. és 16. pont)

b) kezdeményezi, végrehajtja a belső szabályzatokban leírt előkészítő folyamatot (fejlesztési igény megfogalmazása, szakmai, informatikai, adatvédelmi szakértői, információbiztonsági vélemények bekérése, stb.)

c) meglévő adatkezelés esetében 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.];

d) megfogalmazza az adatkezelésről szóló tájékoztatást (GDPR 13-14. cikk) és az informatikai szakterület közreműködésével gondoskodik annak könnyen hozzáférhető módon való közzétételéről [GDPR 12. cikk (1) bek.];

az adatkezelés bevezetéséről való döntést követően:

e) megküldi az adatvédelmi felelősnek az új adatkezelésnek az Adatkezelői Nyilvántartásban történő rögzítéséhez szükséges információkat, illetve a nyilvántartott adatokban bekövetkezett valamennyi változást [GDPR 30. cikk (1) bek.]

f) amennyiben ennek szükségessége felmerül, az adatvédelmi tisztviselővel és a adatvédelmi felelőssel történő egyeztetést követően kezdeményezi az érintett jogainak védelmét biztosító intézkedések megtételét;

g) gondoskodik az érintettek jogainak védelmét biztosító intézkedések nyilvánosan hozzáférhetővé tételéről [GDPR 14. cikk (5) bek.];

h) képviseli az adatkezelőt az adatfeldolgozó felé vagy – közös adatkezelés esetén – a többi, a közös adatkezelésben résztvevő adatkezelő felé (amennyiben releváns);

i) 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;

j) új adatkezelés bevezetése esetén a kapcsolódó szabályzatok szintjén is 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.];

k) 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 (1) a) alkalmazása során döntésre jogosultnak minősül az személy, aki – az Intézmény **SZ-01 Szervezeti és működési szabályzata** szerint – az érintett adatkezelés alapjául szolgáló tevékenységgel kapcsolatban döntésre jogosult.

(2) Az információbiztonsági, 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 **Informatikai biztonsági szabályzat**ától (**SZ-66**) eltérő) adatbiztonsági intézkedések meghatározásában;
g) az adatkezelés feltételeinek kialakítását, adatvédelmi hatásvizsgálat elvégzését, adatfeldolgozó/közös adatkezelő bevonását, automatizált döntéshozatali/profilalkotási módszert, az adatkezelésről szóló tájékoztatást, harmadik országba történő adattovábbítást érintő döntések előkészítésében.

(3) Az információbiztonsági, informatikai szakterület adatkezelési megbízottját/megbízottjait minden esetben be kell vonni az adatkezelés feltételeinek kidolgozása folyamatába. A fejlesztési igényt megfogalmazó szervezeti egység vezetője az egyéb területek adatkezelési megbízottjai bevonásának szükségességéről az érintett adatkezelési megbízottakat és az adatvédelmi felelőst valamint tisztviselőt értesíti.

Az (1) pontban meghatározott döntések, javaslatok véglegesítése előtt ki kell kérni az adatvédelmi felelős véleményét, úgy, hogy az adatvédelmi felelősnek legalább 10 munkanapja legyen a vélemény adására. Az adatvédelmi felelős 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 (1) pontban meghatározott egyéb döntési javaslatokat.

(4) Az adatkezelés vonatkozásában az adatvédelmi felelős adatvédelmi jogi támogatást nyújt az adatkezelési megbízott által előkészített, megszövegezett, adatkezeléshez kapcsolódó dokumentumok elkészítésében és közreműködik azok véglegesítésében, melynek során szükség szerint konzultál az adatvédelmi tisztviselővel.

Ennek keretében
a) beszerzi a Jogi és Igazgatási Osztály, valamint az az információbiztonsági szakterület véleményét;
b) megvizsgálja a véleményezésre megküldött dokumentumot/leírást adatvédelmi jogi szempontból, valamint abból a szempontból, hogy azok milyen módon illeszthetők be az Intézmény informatikai rendszereibe, illetve nincs-e a tervezett adatkezeléssel azonos vagy hasonló adatkezelés;
c) koordinálja az adatkezelés feltételeinek kidolgozásában érintett személyek/szervezeti egységek tevékenységét.

A fentiekben felsorolt szervezeti egységek a véleményüket az adatvédelmi felelősnek küldik meg az adatvédelmi felelős által meghatározott határidőben, amely nem lehet kevesebb 5 munkanapnál. A véleményeket az adatvédelmi felelős összesíti és véglegesíti, szükség esetén az adatkezelési megbízottakkal és a véleményezőkkel való konzultáció után.

A végleges dokumentumok szakmai megfelelőségéért a dokumentum létrehozását kezdeményező adatkezelési megbízott, az adatvédelmi megfelelőségéért az adatvédelmi felelős, az informatikai, információbiztonsági megfelelőségért pedig az információbiztonsági 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 felelős vagy az információbiztonsági szakterület semmilyen felelősséggel nem tartozik.

Amennyiben az adatkezelés feltételei kidolgozásában részt vevő adatkezelési megbízottak között véleményeltérés van, illetve a Jogi és Igazgatási Osztály vagy az információbiztonsági szakterület kifogást fogalmaz meg, az adatvédelmi felelős – szükség esetén az adatkezelési megbízottakkal, adatvédelmi tisztviselővel és a véleményezőkkel való konzultáció után – javaslatot tesz a lehetséges megoldásra.

Az adatbesorolást és az adatkezelési feltételeket, valamint az adatvédelmi felelős és az információbiztonsági felelős véleményét tartalmazó dokumentumokat – az adatkezelést elrendelő szervezeti egység vezetője hagyja jóvá. Amennyiben az új adatkezelés, vagy a meglévő adatkezelés (munkafolyamat, eljárás) módosítása több szakterületet érint, vagy a tervezett változás stratégiai jelentőségű, vagy felügyeleti szerv határozata alapján szükséges, a jóváhagyást a főigazgató adja meg. A jóváhagyás dokumentálását az adatbesorolást és adatkezelési feltételeket tartalmazó dokumentumon kell elvégezni.

(5) Az adatvédelmi felelős véleményét az adatkezeléssel kapcsolatos szabályok és intézkedések bevezetéséről való döntést kezdeményező előterjesztésben ismertetni kell. Az adatvédelmi felelős véleményétől való eltérést az előterjesztésben részletesen meg kell indokolni.

Adatkezelés bevezetése (végrehajtása) az Adatkezelői Nyilvántartásból kinyomtatott adatkezelési tájékoztató főigazgatói jóváhagyásával történik. A főigazgatói jóváhagyás tartalmazza az adatkezelésért felelős szervezeti egységnek és egyéb szervezeti egységeknek az adatkezeléssel kapcsolatos feladatait, így különösen:

a) az adatok felvételének, módosításának, törlésének rendjét,

b) adatszolgáltatási kötelezettségek meghatározását az adatok naprakészen tartása érdekében,

c) a nyilvántartási rendszerből történő adattovábbítás, az ahhoz való hozzáférés rendjét;

d) -az adatkezelésre vonatkozó különös adatbiztonsági intézkedések meghatározását;

e) a GDPR-nak, az Infotv-nek és egyéb alkalmazandó jogszabálynak megfelelő adatkezelési tájékoztatót,

f) hozzájáruláson alapuló adatkezelés esetén a hozzájáruló nyilatkozat mintáját.

5.3.2. 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 Információbiztonsági és Adatvédelmi Osztályon keresztül az adatvédelmi felelős, a Jogi és Igazgatási Osztály és az információbiztonsági 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 megszüntetése esetén

a) megfelelően alkalmazni kell az adatkezelés bevezetésének releváns rendelkezéseit
b) az Adatkezelői Nyilvántartásból az adatkezelést vagy az egyes adatfajtákat törölni kell,
c) a korábbi nyilvántartás-változatokat meg kell őrizni
d) az adatokat – az a) és b) pontokban tett megkülönböztetés szerint –
    da) az informatikai rendszerekben archiválni kell, illetve
    db) az informatikai rendszerekből törölni kell, a papír alapú nyilvántartásban kezelt adatokat pedig – az Intézmény iratkezelési szabályzata szerint – selejtezni kell.

5.3.3. 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. Különösen akkor lehet rá hivatkozni, ha az érintett az adatkezelő ügyfele vagy dolgozója, illetőleg, ha az adatkezelésre csalások megelőzése miatt kerül sor.

Az érdekmérlegelési teszt tervezetét a tervezett adatkezelésért felelős szervezeti egység adatkezelési megbízottja készíti el az adatvédelmi felelős támogatásával. Az érdekmérlegelési tesztet írásban kell elvégezni. Az elkészült dokumentumot – az (4) pont szerint – az adatvédelmi felelősnek kell megküldeni, aki azt szakmai szempontból véleményezi. A jogos érdeken alapuló adatkezelés kizárólag az érdekmérlegelési teszt elvégzését és az adatvédelmi felelős véleményének beszerzését követően kezdhető meg. A (5) pont rendelkezéseit jelen esetben is alkalmazni kell.

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) az adatkezelés leírása és az annak keretében kezelni tervezett személyes adatok meghatározása. Ezen belül azt is meg kell vizsgálni, hogy

aa) a tervezett művelethez, folyamathoz valóban szükség van-e a személyes adatok kezelésére?

ab) van-e olyan alternatív megoldás, ami nem jár személyes adatok kezelésével?

b) Az adatkezelő vagy harmadik fél, akinek az adatkezelés érdekében áll, jogos érdekének azonosítása (Miért szükséges az adatkezelés? – Szükségességi teszt):

ba) Mi a célja az adatkezelésnek?

bb) Az Intézmény mely céljaihoz szükséges az adatkezelés?

bc) Valamely harmadik fél céljaihoz szükséges az adatkezelés?

bd) A GDPR vagy valamelyik hazai jogszabály jogos érdek alapján végzendő adatkezelésnek tekinti-e az adatkezelést? Ha jogszabály nem rendelkezik az adatkezelésről, mely a jog által elismert, védett (pl. üzleti, munkáltatói) érdek, vagy jogszabályból következő feladat áll az adatkezelés mögött?

be) Más módon elérhető-e az adatkezelés célja?

c) Az érintett érdekeinek, jogainak azonosítása (Arányban van-e az adatkezelés az érintett magánszférájának korlátozásával – Arányossági teszt):

ca) Az adatkezelés annak az érintettnek az érdekében áll, akinek a személyes adatai kezelésére kerül sor?

cb) Az adatkezelés az érintett jogát hátrányosan érinti?

cc) Az érintett számíthat-e arra, hogy személyes adatai kezelésére kerül sor? Az érintett számíthat-e arra, hogy az adatait a kívánt célra felhasználják?

cd) Korlátozza, befolyásolja az adatkezelés az érintett jogait?

ce) A felhasználni kívánt adatot közvetlenül az érintettől vagy valaki mástól szerezte meg az adatkezelő?

cd) Az adatkezelés módosítható (pl. az adatkör szűkítésével, az időtartam rövidítésével, adatbiztonsági intézkedések szigorításával, stb.) annak érdekében, hogy csökkenthető vagy elkerülhető legyen a magánszférát érintő veszély?

ce) Az érintett megfelelő tájékoztatást kapott az adatkezelésről?

cf) Az érintett, ellenőrizheti az adatkezelést vagy tiltakozhat ellene?

cg) Az adatkezelés nyújt valamilyen hozzáadott értéket ahhoz a termékhez vagy szolgáltatáshoz, melyet az érintett igénybe vesz?

ch) Az adatkezelőt kár érné, ha az adatkezelésre nem kerül sor?

ci) Harmadik felet kár érné, ha az adatkezelésre nem kerül sor?

cj) Az érintett jogos érdeke egyensúlyban van az adatkezelő jogos érdekével?

ck) Mi a kapcsolat az érintett és az adatkezelő között? (meglévő, korábbi vagy érdeklődő beteg, dolgozó, partner stb.)

cl) Milyen típusú a kapcsolat az érintett és az adatkezelő között? (folyamatos, visszatérő vagy alkalmi)

cm) Milyen típusú adatokat érint az adatkezelés?

d) az adatkezelő (vagy harmadik fél) és az érintettek érdekeinek összevetése: az adatkezeléssel járó előnyök (az adatkezelő vagy harmadik fél érdekének) és hátrányok (az érintett érdekeinek) összevetése;

e) Biztosítékok leírása: Az adatkezelés során alkalmazott biztosítékok leírása, amelyek alkalmasak arra, hogy a személyes adatok biztonságos kezelését, vagyis a véletlen vagy jogellenes megsemmisítést, elvesztést, megváltoztatást, jogosulatlan nyilvánosságra hozatalt vagy az adatokhoz való jogosulatlan hozzáférést kizárják. Ilyen biztosíték (technikai és szervezési intézkedés) lehet többek között az adatminimalizálás, adatrejtés (pl. titkosítás, álnevesítés), korlátozott hozzáférés (jogosultságkezelés) szabályozása, lehetőség az opt-outra (kilépés az adatkezelésből) és az adatkezelési műveletek nyilvántartása (pl. naplózás), az adat zúzalékképző algoritmussal (hash) és annak elektronikus aláírásával történő sértetlenségi kontrollok biztosítása.

f) Az érdekmérlegelési teszt eredménye: A fenti válaszok alapján annak összefoglalása, hogy a jogos érdek alkalmazható-e az adatkezelés jogalapjaként. Amennyiben nem (pl. az érdekmérlegelési teszt eredményeként az adatkezelés vagy egyes adatfajták kezelése nem szükséges és/vagy nem arányos), az adatkezelés feltételeit felül kell vizsgálni.

5.3.4. 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 kikéri az adatvédelmi felelős véleményét.

A hatásvizsgálat elvégzését a tervezett adatkezelésért felelős szervezeti egység adatkezelési megbízottja koordinálja az adatvédelmi felelős támogatásával. A hatásvizsgálat megállapításait írásban kell rögzíteni

Az elkészült hatásvizsgálati dokumentációt az adatvédelmi felelősnek kell megküldeni, aki 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. Az (5) pont rendelkezéseit jelen esetben is alkalmazni kell. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

A hatásvizsgálat módszertanát minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani. Az Intézményben a Nemzeti Adatvédelmi és Információszabadság Hatóság honlapján (https://naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html) található szoftver által meghatározott módszertant kell alkalmazni.

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

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

a) ha automatizált döntéshozatali módszer (beleértve a profilalkotást is – GDPR 22. cikk) bevezetésére kerül sor, amennyiben természetes személyekre vonatkozó személyes adatok módszeres és kiterjedt értékelését foglalja magában;

b) ha személyes adatok különleges kategóriáinak, így különösen egészségügyi adat vagy a természetes személyek egyedi azonosítását célzó biometrikus adatoknak a kezelésére kerül sor;

c) ha az adatkezelés egészségügyi vagy különleges adatok olyan kategóriáit érinti, melyeket az adatgyűjtés eredeti céljától eltérő egyéb célra használnak, kivéve, ha az adatkezelés az beteg hozzájárulása alapján történik vagy az az adatkezelő jogszabályban előírt kötelezettségének teljesítéséhez szükséges;

d) ha nagyszámú érintettre vonatkozó profilalkotásra (elemzésre) kerül sor;

e) ha a dolgozók munkahelyi teljesítményére, megbízhatóságára, viselkedésére vonatkozó módszeres elemzésre vagy értékelésére kerül sor, különösen automatizált módon;

f) ha térfigyelő rendszer bevezetésére vagy az alkalmazott technológia megváltoztatására kerül sor;

g) ha több adatkezelő közös adatkezelőként olyan alkalmazást vagy adatkezelési környezetet kíván bevezetni valamely, az Intézménynél széles körben végzett tevékenység tekintetében;

h) ha új, innovatív technológiai megoldások bevezetésére kerül sor (pl. felhőszolgáltatás igénybe vétele).

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

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

a) az adatkezelésben érintett szervezeti egységet és a tervezett adatfeldolgozó megjelölését;

b) az adatkezelés jogalapját, célját (az adatkezeléstől várt előnyöket, az adatkezelés szükségességét), terjedelmét;

c) az adatkezeléssel érintettek körét, a kezelendő adatok körét, az adatok megőrzésének tervezett idejét,

d) azon adatkezelők megjelölését, akiknek az adatot továbbítani tervezik, és különösen, ha harmadik országba vagy nemzetközi szervezet felé tervezik az adattovábbítást;

e) az adatkezelésre vonatkozó követelmények (jogszabályi követelmények vagy magatartási kódexből, szabványból eredő követelmények);

f) Az adatkezelés folyamatának a leírása: Milyen célból szükségesek az egyes adatkezelési műveletek? Ha ugyanazon cél elérése többféle adatkezelés, adatkezelési művelet vagy adatkezelési módszer (pl. felhőszolgáltatás igénybe vétele útján vagy on premise módon) lehetséges, annak indoklása, hogy miért az adott adatkezelés mellett döntött az adatkezelő.

A hatásvizsgálat második részében ki kell fejteni és meg kell indokolni

a) az adatkezelés szükségességének és arányosságának garanciáit, különösen

aa) a tervezett adatkezelés célját/céljait: mennyiben felelnek meg annak a követelménynek, hogy a cél legyen meghatározott, egyértelmű és jogszerű;

ab) tervezett adatkezelés jogalapját/jogalapjait: melyik jogalap jöhet számításba és miért. Különösen a „jogos érdek" jogalapot kell megindokolni;

ac) azt, hogy a tervezett adatkezelés mennyiben felel meg az adatminimalizálás elvének;

ad) azt, hogy a tervezett adatkezelés hogyan biztosítja a pontosság követelményét;

ae) az adattárolás tervezett időtartamát, illetve azt, hogy az adattörlést hogyan hajtják végre az adatkezelési időtartam lejártakor;

af) amennyiben az értékelés hiányosságokat tár fel, milyen intézkedések szükségesek a GDPR-nak való megfelelés érdekében;

b) az érintett jogait biztosító garanciák érvényesülését, azt, hogy hogyan biztosítja az adatkezelő

ba) az érintett hozzájárulásának megszerzését,

bb) az érintett tájékoztatáshoz való jogát, hozzáféréshez és/vagy adathordozhatóság való jogát, helyesbítéshez, illetve törléshez való jogát, tiltakozáshoz és az adatkezelés zárolásához való jogát,

bc) az adatfeldolgozóval kapcsolatos kötelezettségek érvényesülését,

bd) harmadik országba vagy nemzetközi szervezethez történő adattovábbítás garanciáinak érvényesülését,

be) amennyiben az értékelés hiányosságokat tár fel, milyen intézkedések szükségesek a GDPR-nak való megfelelés érdekében;

A hatásvizsgálat harmadik részében azonosítani és értékelni kell az adatkezelés lehetséges kockázatait, különösen

a) a fenyegető események vagy veszélyek, kockázatoknak

aa) a típusát [ügyfeleket érintő vagy compliance vagy szervezeti/egész Intézményt érintő kockázat(ok)],

ab) a lehetséges forrását (ember által/emberi behatás nélkül, szándékos/gondatlan, belső/külső), előfordulásának valószínűségét és súlyosságát (jelentéktelen, közepes, jelentős);

ac) az érintettek magánszférájára gyakorolt lehetséges hatását;

b) A kockázatok enyhítésére tervezett, elfogadott intézkedések, megoldások bemutatása (vagy annak megindokolása, hogy azok alkalmazására miért nem kerül sor) és értékelése abból a szempontból, hogy azok megfelelőek-e a kockázatok kiküszöbölésére, mérséklésére, illetve, hogy milyen kiegészítő intézkedésekre van szükség a GDPR-nak való megfelelés érdekében:

ba) a kockázatok mérséklésére szolgáló jogi intézkedések ismertetése, így különösen: adatkezelés célja, kezelendő adatkör minimalizálása, adatok minősége, megőrzési idő, az érintettek tájékoztatása, az érintettek jogainak gyakorlása.

bb) a kockázatok mérséklésére szolgáló szervezési intézkedések, így különösen: az adatkezelésről rendelkező szervezeti egység feladatainak kialakítása; kockázatelemzés elvégzése, a kockázatok kezelése;

bc) az adatfeldolgozók tevékenységének ellenőrzése; az adatbiztonsági intézkedések felügyeletének rendje; az adatkezelésre vonatkozó kiegészítő szabályozás, eljárásrend kialakítása; adatvédelmi tudatosságot növelő intézkedések, speciális képzés.

bd) a kockázatok mérséklésére szolgáló logikai biztonsági intézkedések, így különösen: álnevesítés, maszkolás, anonimizálás, titkosítás, az adatintegritás biztosítékai, naplógyűjtés és -figyelés, hozzáférési jogosultságok kezelése, elemzések elvégzése, tesztelés, konfiguráció-kezelés, azonosítás és hitelesítés szabályozása;

be) a kockázatok mérséklésére szolgáló általános biztonsági intézkedések, így különösen: az alkalmazott szoftverek frissítései, a rosszindulatú szoftverek elleni védelem; a hardverek (munkaállomások, hálózati elemek, stb.), hálózati kapcsolatos megfelelősége, azok folyamatos ellenőrzése; a helyiségekhez és hardverekhez való fizikai hozzáférés kontrollja (pl. belépések ellenőrzése; hozzáférés ellenőrzése, behatolás elleni riasztás); természeti csapások elleni védelem (pl. tűzvédelem); folyamatos áramellátás biztosítása;

bf) a fenti a megoldási javaslatokkal megszűnt vagy mérséklődött a várható kockázat?

c) az esetleges adatvédelmi incidensek elemzése és értékelése: a nem várt események (illetéktelen hozzáférés, az adatok nem kívánt módosítása vagy az adatok törlése) lehetséges forrása, a bekövetkezés valószínűsége, súlyossága, lehetséges hatása), és a hatások mérséklésére alkalmazható eszközök.

A hatásvizsgálat negyedik része tartalmazza a tervezett adatkezelés értékelését:

a) a hatásvizsgálat első-harmadik részében meghatározott szempontok értékelését a tekintetben, hogy azok egyenként megfelelőek, további intézkedésekkel megfelelőek lehetnek, illetve nem megfelelőek;

b) a tervezett kiegészítő intézkedések végrehajtásának ütemtervét;

c) annak egyértelmű rögzítését, hogy a tervezet 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.

5.4. AZ ÉRINTETTI JOGOK GYAKORLÁSÁNAK ELŐSEGÍTÉSE

5.4.1. 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) az Intézmény Adatvédelmi és Adatkezelési Tájékoztatóját az Intézmény egyes adatkezelési tevékenységeihez kapcsolódó (különös) adatkezelési tájékoztatók, ide nem értve a dolgozók, egyéb jogviszonyban foglalkoztatottak adatainak kezelésére vonatkozó tájékoztatókat;

b) 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) Adatvédelmi és Adatkezelési Tájékoztatóra mutató hivatkozást;
b) egyéb releváns dokumentumokat (pl. betegtájékoztatókat, formanyomtatványokat).

Az Intézmény az OKFŐ Adatkezelési megbízásából kidolgozott mintadokumentumok Intézményre adaptált változatát alkalmazza a tevékenysége során.

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

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

5.4.2. 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.

5.4.3. 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.

5.4.4. 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.

5.4.5. Hozzátartozók tájékoztatása

Az Intézmény szervezeti egységeinek vezetői az adatkezelési megbízottak közreműködésével gondoskodnak arról, hogy az Intézményben kezelt vagy az Intézménnyel más módon kapcsolatba kerülő személyek hozzátartozóit az Általános Betegtájékoztatóban szabályozott módon az adatvédelmi szabályoknak megfelelően tájékoztassák, amelyben – az érintett személy képességeit is figyelembe véve – magát az érintettet is bevonhatja. A betegeket megillető jogokra, valamint őket terhelő kötelezettségekre vonatkozó rendelkezések a mindenkor érvényes Általános Betegtájékoztatóban találhatók. A tájékoztatásra jogosult személyek adatait a kezelt személy adataihoz kapcsoltan kell a HIS rendszerbe rögzíteni.

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

5.5. AZ ÉRINTETTŐL SZÁRMAZÓ KÉRELMEK, PANASZOK MEGVÁLASZOLÁSÁNAK RENDJE

5.5.1. Az adatvédelmi bejelentések típusai

A GDPR 12-22. cikkeiben foglalt rendelkezéseknek megfelelően az érintettől a következő, személyes adatai Intézmény általi kezelését érintő beadványok érkezhetnek:

a) bejelentheti az Intézmény által nyilvántartott adatok megváltozását;
b) tájékoztatást kérhet személyes adatai [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 [az Info tv. a személyes adatokkal összefüggő jogoknak az érintett halálát követő érvényesítésére, valamint az Eüak. elhalálozással kapcsolatos egészségügyi és egyéb személyes adatokra vonatkozó rendelkezései]

5.5.2. Az adatvédelmi beadványok kezelésének eljárásrendje

Az Intézményhez érkező, az 5.5.1. pontban meghatározott beadványokat (a továbbiakban: panasz) az Intézmény **Panaszkivizsgálási szabályzat**ában (**SZ-13**), valamint a Szabályzat az érintetti valamint hatósági bejelentés nyilvántartása a Dél-pesti Centrumkórház-Hematológiai és Infektológiai Intézetben a GDPR megfeleléshez elnevezésű dokumentumban foglaltaknak megfelelően kell – a GDPR 12. cikkében írt határidők figyelembevételével – elintézni, az alábbi kiegészítésekkel és eltérésekkel:

a) a beadvány érkezése dátumát és időpontját pontosan rögzíteni kell az OKFŐ által biztosított Datinf rendszerben;
b) az 5.5.1. pont j) alpontban meghatározott panasz kivizsgálását az adatvédelmi felelős végzi. A panasz kivizsgálása során az érintett szervezeti egységek kötelesek az adatvédelmi felelőssel együttműködni. A személyes adatok kezelését, illetve a GDPR szerinti jogok gyakorlását érintő panasz megalapozottsága esetén az adatvédelmi felelős 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 Orvosigazgató bármely beadvány esetén kérheti az adatvédelmi felelős véleményét a tekintetben, hogy a beadvány az 5.5.1. pontban meghatározott tárgyú-e, illetve, hogy

az érintett kérte-e az adatkezelés korlátozását [zárolás, GDPR 18. cikk – lsd. 0. pont e) alpont], és kérés esetén az adatvédelmi felelős az adatvédelmi tisztviselővel egyeztetve – az információbiztonsági szakterület útján – intézkedik annak az informatikai rendszerekben történő megvalósításáról. Az adatkezelés korlátozásának feloldásáról az adatvédelmi felelős külön tájékoztatja az érintett informatikai rendszer (eke) t üzemeltető szervezet egység (ek) et,

d) az adatvédelmi felelős dönt abban a kérdésben, hogy az 5.5.1. pontban meghatározott tárgyú beadvány egyértelműen megalapozatlan vagy túlzó-e,

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

f) amennyiben a beadvány a GDPR hatálya alá tartozó beadványnak minősül, a beadványozót a beadvány érkezését követő 8 napon belül értesíteni kell a beadvány érkezéséről, a megválaszolására nyitva álló határidőről, illetve arról, hol kaphat további felvilágosítást a beadványáról. Nem kell ilyen értesítést küldeni a beadványozónak, ha a beadványban kért intézkedést ezen időn belül teljesítik;

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

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

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

j) az Intézmény szervezeti egységei az 5.5.1. pontban meghatározott tárgyú ügyekben készített válaszlevél-tervezetét jóváhagyás végett bemutatják az adatvédelmi felelősnek;

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 ügyirat-nyilvántartást kell vezetni, amely segítségével bármikor egyértelműen azonosíthatók az 5.5.1. pont szerinti beadványok, nyomon követhetők a beadványok elintézése során tett intézkedések, és a rendelkezésre álló adatokból bármikor statisztika készíthető a következő szempontok szerint:

a) adott időszakban érkezett beadványok száma, típus szerinti bontásban is;
b) a beadványok beérkezésének módja;
c) a beadványok megválaszolásának átlagos időtartama;
d) az elutasított beadványok száma, és azok okai;
e) a válaszadás módja.

Az adatvédelmi tisztviselő illetőleg felelős bármely esetben – az érintettnek az 5.5.1. pont b), d), j) alpontjai alá eső beadványa kivizsgálása, illetve saját ellenőrzése eredményeként, továbbá az adatvédelmi felügyeleti hatóság vagy bíróság döntése végrehajtásaként – a vonatkozó belső rendelkezésekben meghatározott hatásköri és eljárási rendtől függetlenül kezdeményezheti személyes adat helyesbítését, törlését vagy az adatkezelés korlátozását.

A személyes adatok kezelését érintő, szóbeli adatvédelmi bejelentéseket az Intézmény belső rendelkezéseinek megfelelően rögzíteni kell (**SZ-39 M04 Adatvédelmi incidens bejelentő lap**). A szóbeli bejelentésről készített jegyzőkönyvet, valamint a személyes adatok kezelését érintő, írásbeli adatvédelmi bejelentéseket az Intézményhez való beérkezésüket követően haladéktalanul az Információbiztonsági és Adatvédelmi Osztályra, az adatvedelem@dpckorhaz.hu címre kell megküldeni. A beérkezett adatvédelmi bejelentéseket az Információbiztonsági és Adatvédelmi Osztály saját iktatórendszerében iktatja. Az adatvédelmi bejelentés 5.5.2. pontja szerinti minősítését az adatvédelmi felelős szükség esetén az adatvédelmi tisztviselővel folytatott konzultáció után végzi.

Az adatvédelmi tisztviselő a közvetlenül hozzá érkezett, de az 5.5.1. pont hatálya alá tartozó bejelentéseket haladéktalanul továbbítja az adatvédelmi felelősnek, és amennyiben a bejelentés adatkezelési kifogásnak minősül, a panaszkezelési szakterületnek. A bejelentésekben szereplő adatvédelmi kérdéseket az adatvédelmi felelős soron kívül kivizsgálja, és amennyiben a bejelentés adatkezelési kifogásnak minősül, a választervezetet 5 napon belül megküldi a panaszkezelési szakterületnek.

Az adatvédelmi felelős a beérkezett adatvédelmi bejelentéseket haladéktalanul megvizsgálja abból a szempontból, hogy az érintett kérte-e az adatkezelés korlátozását [GDPR 18. cikk – lásd 5.5.1. pont e) alpont], és kérés esetén az adatvédelmi felelős – az Információbiztonsági és Adatvédelmi Osztály útján – és az adatvédelmi tisztviselő– intézkedik az informatikai rendszerekben történő megvalósításáról. Az adatkezelés korlátozásának feloldásáról az adatvédelmi felelős külön tájékoztatja az érintett informatikai rendszert (eket) üzemeltető szervezet egységet/egységeket.

Az adatvédelmi felelős a beérkezett bejelentéseket, kérelmeket megvizsgálja abból a szempontból, hogy egyértelműen megalapozatlan vagy túlzó-e, és javaslatot tesz díj felszámítására vagy a kérelem elutasítására.

Az adatvédelmi bejelentéseket az adatvédelmi felelős – önállóan vagy az Intézmény egyéb szervezeti egységeinek közreműködésével – kivizsgálja, illetve előkészíti a választ vagy intézkedést.

Az Információbiztonsági és Adatvédelmi Osztály szakterülete közreműködik az adatkezelés korlátozásának végrehajtásában, a válaszadáshoz szükséges személyes adatok különböző informatikai rendszerekből történő összegyűjtésében.

Az adatvédelmi felelős által felkért szervezeti egység adatkezelési megbízottja az adatvédelmi felelős által megjelölt - de minimum 3 munkanapos - határidőn belül az adatvédelmi felelős rendelkezésére bocsátja az adatvédelmi bejelentés elbírálásához szükséges adatokat, információkat, felvilágosítást, magyarázatot, illetve az adatvédelmi tisztviselő által kért egyéb módon közreműködik az adatvédelmi felelős döntéseinek előkészítésében. A megkeresett adatkezelési megbízott az érintett ügylet ügyintézőjével, illetve közvetlen felettesével felveszi a kapcsolatot az adatvédelmi felelős által kért adatok megadása érdekében. A panaszkezelési terület által az adatvédelmi terület részére e-mailen az adatvedelem@dpckorhaz.hu.hu címre megküldött adatkezelési kifogásokra az adatvédelmi terület 5 napon belül megküldi a válaszát.

Az informatikai rendszereket üzemeltető szervezeti egység az adatvédelmi felelős kezdeményezésére az adatvédelmi tisztviselő rendelkezésének megfelelően elvégzi az adatkezelés korlátozását, az adatok helyesbítését/módosítását, törlését.

A közvetlenül az adatvédelmi tisztviselőhöz érkezett adatváltozási bejelentéseket – (5.5.1. pont a) alpont – beleértve azokat a helyesbítési kérelmeket 5.5.1. pont c) alpont], amelyeknél a helyes adatok rendelkezésre állnak, az adatvédelmi tisztviselő 5 napon belül átadja az adatvédelmi felelős részére. aki az Információbiztonsági és Adatvédelmi Osztály bevonásával gondoskodik az adatmódosításnak, illetve helyesbítésnek az érintett informatikai rendszerben/rendszerekben történő végrehajtatásáról, a módosítás/helyesbítés alapjául szolgáló dokumentum rendszerben történő rögzítéséről, és a bejelentő tájékoztatásáról, továbbá ezzel összefüggésben a GDPR 19. cikke szerinti kötelezettségek teljesítéséről. A szigetszerűen működő IT rendszerekben a kért változtatások elvégzéséről, továbbá ezzel összefüggésben a GDPR 19. cikke szerinti kötelezettségek teljesítéséről az informatikai szakterület adatkezelési megbízottja gondoskodik.

A személyes adatok kezeléséről való tájékoztatás-kérés [hozzáférési jog gyakorlása – 5.5.1. pont b) alpont] esetén a kérelem teljesítését az adatvédelmi tisztviselő – a kérelem beérkezését követő 5 napon belül – átadja az adatvédelmi felelősnek. Az adatvédelmi felelős az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért az adatkezelő az adminisztratív költségeken alapuló, ésszerű t (Intézmény térítési díjainak megfelelő mértékű díjat számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.

Az adathordozhatósághoz való jog gyakorlására irányuló kérelmet – 5.5.1. pont f) alpont – az adatvédelmi tisztviselő– a kérelem beérkezését követő 5 napon belül – átadja az adatvédelmi

felelősnek. Az Információbiztonsági és Adatvédelmi Osztály közreműködik a szükséges adatok összegyűjtésében és az abban, hogy a kérelem teljesíthető-e, illetve mely adatokra nézve teljesíthető.

Amennyiben az adathordozhatósághoz való jog gyakorlására irányuló kérelem nem teljesíthető, az adatvédelmi tisztviselő a kérelmet elutasítja és erről a kérelmezőt tájékoztatja. Az adathordozhatóság részbeni teljesíthetősége esetén az adatvédelmi tisztviselő a döntését a kiadható adatok rendelkezésre bocsátásával egyidejűleg közli a kérelmezővel.

Amennyiben az adathordozhatósághoz való jog gyakorlására irányuló kérelem teljesíthető, a válaszlevél tervezetét az adatvédelmi felelős előkészíti, majd az adatvédelmi tisztviselő tájékoztatásával a kért adatokat elküldi a kérelmezőnek.

(6) A közvetlenül az adatvédelmi felelőshöz, vagy az adatvedelem@dpckorhaz.hu email címre érkezett olyan adatvédelmi bejelentéseket, amelyekben az érintett tiltakozik személyes adatai kezelése ellen, az adatvédelmi felelős haladéktalanul megküldi az illetékes igazgatóság adatkezelési megbízottjának. A tiltakozási joggal kapcsolatos adatvédelmi bejelentéseket – 5.5.1. pont g) alpont – az adatvédelmi felelős, az érintett szakterület adatvédelemi megbízottja, valamint a panaszkezelési szakterület kijelölt munkatársa közreműködésével megvizsgálja, és dönt a tiltakozási jog elfogadásáról vagy elutasításáról. A döntésről a panaszkezelési terület tájékoztatja az érintettet.

Amennyiben az érintettnek az adatai törlésére – 5.5.1. pont d) alpont – illetve helyesbítésére 5.5.1. pont c) alpont – irányuló egyedi kérelme magalapozott, az adatvédelmi tisztviselő, és/vagy az adatvédelmi felelős a – gondoskodik a törlendő, illetve helyesbítendő személyes adatoknak a törlendő, illetve helyesbítendő adatot tartalmazó informatikai rendszerben/rendszerekben történő azonnali zárolásáról. Továbbá a törlésnek, illetve helyesbítésnek az irányadó protokollok szerinti elvégeztetéséről, majd az érintettnek a törlés, illetve helyesbítés elvégeztetéséről való tájékoztatásáról. Amennyiben a bejelentés adatkezelési kifogásnak minősül, akkor a panaszkezelés közreműködésével gondoskodik a bejelentő tájékoztatásáról, továbbá ezzel összefüggésben a GDPR 19. cikke szerinti kötelezettségek teljesítéséről.

A szigetszerűen működő IT rendszerekben az 5.5.1. pont c) és d) alpontok szerinti helyesbítés és törlés elvégzéséről, továbbá ezzel összefüggésben a GDPR 19. cikke szerinti kötelezettségek teljesítéséről az informatikai szakterület adatkezelési megbízottja gondoskodik

Automatizált döntéshozatal alkalmazásával összefüggő adatvédelmi bejelentéseket – 5.5.1. pont h)-i) alpontok – az adatvédelmi felelős az érintett szakterület adatvédelemi megbízottja közreműködésével megvizsgálja. Az adatvédelmi bejelentés megalapozottsága esetén az automatizált döntést hozó szervezeti egység figyelembe veszi az érintett álláspontját, illetve biztosítja az emberi beavatkozás lehetőségét. Az automatizált döntéshozatal alkalmazásával meghozott döntéssel szembeni kifogást az adatvédelmi tisztviselő véleményének figyelembevételével az adatkezeléssel érintett folyamatot szabályozó belső szabályzat szerint felül-bírálatra jogosult személy bírálja el.

A személyes adatok kezelését, illetve az Infotv. és a GDPR szerinti jogok gyakorlását érintő kifogás megalapozottsága esetén az adatvédelmi felelős az adatvédelmi tisztviselő tájékoztatásával az adatkezelésről rendelkező szervezeti egységnél/egységeknél intézkedést kezdeményez a kifogás kiváltó okainak orvoslására, az érintett folyamatok felülvizsgálatára, valamint – szükség esetén – a személyi felelősség megállapítására.

Az adatvédelmi bejelentéseket indokolatlan késedelem nélkül, de legfeljebb az adatvédelmi bejelentésnek az Intézményhez történő beérkezésétől számított egy hónapon belül kell megválaszolni. Az olyan összetett és/vagy több típusú kérelmet is tartalmazó adatvédelmi bejelentés esetén, amelynek egyes elemei egymástól függetlenül nem válaszolhatóak meg, az érintett előzetes tájékoztatása mellett az adatvédelmi tisztviselő a válaszadási határidőt legfeljebb további két hónappal meghosszabbíthatja. Az adatvédelmi bejelentések kivizsgálásában közreműködő szervezeti egységek –jelen fejezet (6) pont – a határidő meghosszabbítása iránti igényüket legkésőbb az egy hónapos határidő lejárta előtt 8 nappal, indokaikkal együtt, jelzik az adatvédelmi felelősnek

A személyes adatok nyilvánosságra hozatala - kivéve, ha arra az érintett felhatalmazást ad, illetve ha azt törvény rendeli el - tilos.

Az Intézmény dolgozóival, partnereivel, illetve betegeivel kapcsolatos - személyes adatokon is alapuló - összesített statisztikai adatok közölhetőek, amennyiben azokból nem ismerhető fel az, akire az adat vonatkozik. Az adat közlése előtt az adat közlője köteles meggyőződni arról, hogy a közölt adatok alapján nem lehetséges természetes személyek azonosítása. Kétség esetén köteles írásos véleményt kérni az adatvédelmi felelőstől

Amennyiben a büntető vagy más hatósági ügyekben eljáró szervektől - rendőrség, bíróság, ügyészség, NAV -, valamint a nemzetbiztonsági szolgálatoktól érkező megkeresésekre adandó válaszokkal kapcsolatban kétség merül fel, az adatvédelmi tisztviselő véleményét kell kérni az adattovábbítás előtt.

A telefonon történő bejelentések rögzítését jogszabály kötelező jelleggel előírja. Az Intézmény által rögzített felvételeket öt évig kell megőrizni az erre szolgáló informatikai rendszerben. Amennyiben az érintett kéri, biztosítani kell számára a felvétel visszahallgatását vagy a felvételről készített írásos, hitelesített jegyzőkönyv rendelkezésére bocsátását. Az érintett kérheti a hangfelvétel kiadását is. A hangfelvétel CD-re írásáról az Információbiztonsági és Adatvédelmi Osztály gondoskodik az adatvédelmi szakértő (adatvédelmi felelős) felügyelete mellett. A hangfelvétel kiírását a felvétel megküldésével az a szervezeti egység kezdeményezi, amelynél az érintett a kérelmét benyújtotta. Az érintett részére a hangfelvétel rendelkezésre bocsátását az a szervezeti egység teljesíti, ahol az érintett a kérelmét benyújtotta.

Amennyiben a beteg a hangrögzítés ellen tiltakozik, úgy a beszélgetés azonnal megszakítandó azzal a tájékoztatással, hogy a betegnek személyesen kell az betegszolgálatnál eljárnia, vagy írásban teheti meg panaszát.

5.6. 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) SZ-66 Informatikai biztonsági szabályzat
b) SZ-41 Informatikai felhasználói szabályzat
c) SZ-83 Incidenskezelési szabályzat

Az adatbiztonsági szabályok tervezetének kialakításába – a véleményezésre vonatkozó egyéb szabályokat nem érintve – az adatvédelmi felelőst 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 dolgozó 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 információbiztonsági 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.

5.7. A KÖZÖS ADATKEZELÉSI ÉS AZ ADATFELDOLGOZÁSI MEGÁLLAPODÁSOK MEGKÖTÉSÉNEK ÉS VÉGREHAJTÁSA ELLENŐRZÉSÉNEK SZABÁLYAI

5.7.1. Közös adatkezelési megállapodások

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

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

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

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

bd) az esetleges jogellenes adatkezelés következményeit milyen arányban viselik;

c) az adatvédelmi incidens észlelése esetén követendő eljárást, különösen azt, hogy

ca) az adatvédelmi incidens tudomásra jutása esetén a másik adatkezelő adatvédelmi tisztviselőjét (adatvédelmi tisztviselő hiányában a kijelölt kapcsolattartót) haladéktalanul kötelesek értesíteni az adatvédelmi rendellenességről vagy incidensről;

cb) egymással kötelesek együttműködni az adatvédelmi rendellenesség vagy incidens okának kiderítésében és következményeinek felszámolásában;

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

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

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

A közös adatkezelés szükségességét az adatkezelési megbízott az adatvédelmi felelős útmutatása alapján 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 – az 5.11. fejezet megfelelő

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

Amennyiben döntés születik a közös adatkezelés bevezetéséről, az illetékes adatkezelési megbízott(ak), az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi felelős és egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a Jogi és Igazgatási Osztály közreműködésével, továbbá az információbiztonsági 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.

Az 5.7.1. pont alkalmazásában a szerződés megkötésére jogosult személy az, aki – az Intézmény Szervezeti és Működési Szabályzata szerint – az érintett adatkezelés alapjául szolgáló tevékenységgel kapcsolatban döntésre jogosult, illetve – amennyiben a döntés testületi hatáskörbe tartozik – a testületi döntés előkészítéséért felelős. E szabály nem érinti az együttes aláírásra vonatkozó szabályokat.

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

5.7.2. Adatfeldolgozási megállapodások

Amennyiben harmadik országbeli adatfeldolgozó igénybevétele merül fel, először abban a kérdésben kell dönteni – az 5.11. 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 és vagy továbbítására, az adatfeldolgozóval csak a GDPR 49 cikk-ben leírt feltételek legalább egyikének a teljesülése esetén kerülhet sor.

Adatfeldolgozó igénybevétele esetén az adatfeldolgozóval kötendő szerződésnek tartalmaznia kell a GDPR 28. cikk (1)-(4) bekezdésében foglalt tartalmi elemeket a az 5.7.2. pont a)-d)-ig terjedően foglalt kiegészítései és pontosításai szerint.

Az adatfeldolgozóval kötendő szerződésben

a) kötelező tartalmi elemként fel kell tüntetni, az adatkezelés tárgyát, időtartamát jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, továbbá a kellő részletességgel (pl. jogszabályra vagy szabványokra utalással) meg kell határozni az adatfeldolgozó, vagy az adatfeldolgozó által igénybe veendő további adatfeldolgozó

által betartandó adatbiztonsági szabályokat, amelyek nem lehetnek kevésbé szigorúak, mint az Intézmény által alkalmazott adatbiztonsági intézkedések –5.6. fejezet – , és az adatfeldolgozónak az adatbiztonsági intézkedések végrehajtásával kapcsolatos feladatait;

b) 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;

c) rögzíteni kell az adatfeldolgozónak az érintettől származó kérelmek, panaszok megválaszolásában való közreműködésének eljárásrendjét;

d) rögzíteni kell az adatfeldolgozó kötelezettségeit adatvédelmi incidens észlelése esetén, így különösen

da) az adatvédelmi incidens tudomásra jutása esetén az Intézmény adatvédelmi tisztviselőjét haladéktalanul köteles értesíteni az adatvédelmi incidensről,

db) köteles együttműködni az Intézmény adatvédelmi tisztviselőjével és más közreműködő szervezeti egységgel az adatvédelmi incidens okának feltárásban és következményeinek felszámolásában,

dc) köteles együttműködni az adatvédelmi incidens bejelentésének teljesítésében,

de) 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 információbiztonsági 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 felelős és egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a Jogi és Igazgatási Osztály közreműködésével, továbbá információbiztonsági szakterület véleményének kikérésével előkészíti az adatfeldolgozóval kötendő szerződés tervezetét és azt felterjeszti a szerződés megkötésére az Általános Szabályozás 5.3.1. fejezet (1) pont szerint jogosult személynek.

Az adatkezelési megbízott az adatfeldolgozási megállapodás megkötését követően az adatfeldolgozó adatait (név és cím, kapcsolattartó neve és elérhetősége) megküldi az adatvédelmi felelősnek, aki az információkat rögzíti az Adatkezelői Nyilvántartásban.

A jelen fejezet rendelkezéseit al-adatfeldolgozó igénybevétele esetén is megfelelően alkalmazni kell azzal, hogy az al-adatfeldolgozó igénybevételére vonatkozó hozzájáruló nyilatkozatnak az adatfeldolgozási megállapodás megkötésre jogosult személy általi kiadása előtt az adatkezelési megbízott kikéri az adatvédelmi felelős és rajta keresztül a Jogi és Igazgatási Osztály, továbbá az információbiztonsági szakterület véleményét is.

5.8. Az Adatkezelői Nyilvántartás

Az adatvédelmi felelős vezeti az Adatkezelői Nyilvántartást. Az adatkezelői nyilvántartás valamennyi, az Intézmény általi adatkezelés esetén tartalmazza:

a) az adatkezelés elnevezését, célját, a folyamatot, amibe az adatkezelés illeszkedik, az adatkezeléssel kapcsolatos űrlapot, amennyiben értelmezett

b) adatkezelés elnevezését

c) az adatkezelő nevét, szervezeti egységét

d) az adat forrását, amennyiben nem az érintettől származik

e) adatfeldolgozói megállapodást amennyiben értelmezett

f) azt a tényt, hogy különleges adat-e,

g) az adat megőrzési idejének jogalapját

h) az adat megőrzési/törlési idejét;

i) az adatkezelés jogalapját,

j) az adatkezelésről készített hatásvizsgálatra vonatkozó adatokat

k) az adatkezelésről készített érdekmérlegelésre vonatkozó adatokat

l) az adatkezeléssel kapcsolatos automatizált döntéshozatalra vonatkozó adatokat

m) az adatkezeléssel kapcsolatos csatolt dokumentumokat

n) az érintettek körét,

o) az érintettekre vonatkozó adatok leírását,

p) az adatok kezelésének kezdetét és végét

q) rendszerelem nyilvántartást, amennyiben értelmezett

r) az adat rendelkezésre bocsátásának elmaradása esetén felmerülő következmények

s) a tájékoztatás módját

t) dokumentumokat, amelyek meghatározzák az érintettek jogait

u) a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló, valamint nemzetközi szervezethez történő adattovábbításokat is,

adattovábbítás jogalapja, típusa, csatornája, gyakorisága – eseti/rendszeres, célja, csatolt dokumentumok, adattovábbítás kezdete és vége

v) az adatkezelés módszere (manuális, számítógépes, vegyes),

w) technikai és szervezési intézkedések az adatkezeléssel kapcsolatban

Az adatkezelési nyilvántartásban tárolt adatok a jogi szabályzók változása alapján módosulhatnak. A pontos adattartalmat a Datinf szoftverben az intézmény fenntartója határozza meg.

Az Adatkezelői Nyilvántartás adattartalma, amennyiben az Intézmény az adatfeldolgozó:

a) az adatfeldolgozó adatai:

aa) adatfeldolgozó neve és elérhetőségei,

ab) adatvédelmi tisztviselő neve és elérhetőségei

b) az adatkezelő (k) adatai (akinek nevében az adatfeldolgozó eljár):

ba) adatkezelő neve,

aa) adatkezelő elérhetősége,

bc) adatkezelő képviselőjének neve és elérhetősége;

c) az adatkezelési tevékenységek kategóriáinak leírása;

d) harmadik országba történő adattovábbítás esetében a megfelelő garanciák leírása;

e) az adatbiztonsági intézkedések leírása (technikai és szervezési intézkedések).

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

Az adatkezelési megbízott az adatvédelmi felelős utasításai alapján az Adatkezelői Nyilvántartásba való betekintést – a Hatóság képviselőin kívül – az Intézmény érintett szakterületei részére biztosítja.

Az adatkezelési megbízott az új adatkezelés bevezetését az adatkezelés megkezdése előtt 5 munkanappal bejelenti az adatvédelmi felelősnek [vö. Általános Szabályozás 5.3.1.(1) pont e) alpont], majd azt az adatvédelmi felelős utasításai alapján az Adatkezelői Nyilvántartásba bejegyzi.

Amennyiben az Intézmény adatfeldolgozónak minősül, az adatfeldolgozási megállapodás megkötését követő 5 napon belül az adatfeldolgozás adatait [jelen fejezet] rögzíti az Adatkezelői Nyilvántartásban;

Az Adatkezelői Nyilvántartásba bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelési megbízott 5 munkanapon belül köteles bejelenteni az adatvédelmi felelősnek [vö. Általános Szabályozás 5.3.2. fejezet], aki ennek megfelelően módosítja az Adatkezelői Nyilvántartás adatait.

Az Adatkezelői Nyilvántartással összefüggésben az adatvédelmi felelős:

a) biztosítja, hogy az adatkezelések bevezetését megelőző döntés-előkészítés során az érintett szakterületek az adatkezelési tevékenységek nyilvántartása adatait megismerhessék a felesleges, párhuzamos adatkezelések elkerülése, illetve az új adatkezelésnek a meglévő adatkezelésekhez való illeszkedése érdekében;

b) ellenőrzi az adatkezelések, illetve adatfeldolgozás adatainak az Adatkezelői Nyilvántartásba történő rögzítését és jelzi az adatkezelésért felelős szervezeti egység vezetőjének a hiányos, hibás vagy valószínűleg megváltozott adatokat, információkat;

c) a Jogi és Igazgatási Osztállyal együttműködve figyelemmel kíséri az adatkezelést érintő jogszabályok változását és a szükséges módosításokra felhívja az adatkezelési megbízottak figyelmét;

d) az adatvédelmi felügyeleti hatóság megkeresésére adatot szolgáltat az Adatkezelői Nyilvántartásból.

e) az adatkezelés megszüntetése esetén az adatkezelési megbízott jelzése alapján az adatkezelés állapotát megszüntetettre állítja;

5.9. AZ ADATVÉDELMI INCIDENSEK KEZELÉSE

5.9.1. Általános szabályok

Az adatvédelmi incidens minősítése, adatvédelmi incidens bejelentése, általános incidensprotokoll, adatvédelmi incidens kivizsgálása vonatkozásában az érintett tájékoztatása a súlyos adatvédelmi incidensről, az adatvédelmi incidens bejelentése a hatóságnak, az adatvédelmi és egyéb incidensek nyilvántartása vonatkozásában az **Incidenskezelési szabályzat**ban és mellékleteiben (**SZ-83**) foglaltak megfelelően irányadók.

5.9.2. Külső kommunikáció

Amennyiben az adatvédelmi incidenssel kapcsolatosan bármilyen információ a nyilvánosság elé kerül, úgy az adatvédelmi incidenssel kapcsolatos bármilyen és valamennyi sajtóközlemény tételére, a sajtóval való kapcsolattartásra kizárólag az Intézmény főigazgatója vagy az általa megbízott személy jogosult az adatvédelmi tisztviselő közreműködésével.

5.10. AZ ADATVÉDELMI FELÜGYELETI HATÓSÁGOKKAL VALÓ KAPCSOLATTARTÁS

Az adatvédelmi tisztviselő

a) az adatkezelési megbízott javaslatára az adatvédelmi felelős támogatásával előzetes konzultációt kezdeményez a felügyeleti hatósággal, amennyiben az adatvédelmi hatásvizsgálat elvégzését követően megállapítható, hogy az adatkezelés a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár [GDPR 36. cikk (1) bek. és 58. cikk (3) bek. a) pont];

b) a magatartási kódexben előírt tanúsítási eljárást kezdeményez és a tanúsítást végző szervezettel kapcsolatot tart, illetve az együttműködést koordinálja a tanúsítási eljárás lefolytatása érdekében [GDPR 42. cikk (6) bek.];

c) az adatvédelmi felügyeleti hatóságtól érkező, a GDPR, illetve az Infotv. hatálya alá tartozó ügyre vonatkozó megkeresésekre (vagyis az adatvédelmi felügyeleti hatóság vizsgálati, illetve korrekciós hatáskörében hozott intézkedésekre – a továbbiakban együtt: adatvédelmi hatósági megkeresés) adandó választ koordináltan előkészíti [GDPR 58. cikk (1)-(2) bek.], továbbá a felügyeleti hatóság által folytatott helyszíni vizsgálat esetén a felügyeleti hatósággal való együttműködést koordinálja;

d) az adatvédelmi felügyeleti hatóság eljárását kezdeményezi a magatartási kódex jóváhagyása céljából [GDPR 57. cikk (1) bek. m) pont];

e) az adatvédelmi felügyeleti hatóság eljárását kezdeményezi adattovábbítási szerződéses feltételek jóváhagyása céljából [GDPR 57. cikk (1) bek. r) pont];

f) az adatvédelmi felügyeleti hatóság eljárását kezdeményezi kötelező erejű vállalati szabályok jóváhagyása céljából [GDPR 57. cikk (1) bek. s) pont];

g) dönt az adatvédelmi felügyeleti hatóság döntéseivel szembeni jogorvoslati eljárás megindításáról [GDPR 78. cikk] szükség esetén a Jogi és Igazgatási Osztály, illetőleg az adatvédelmi felelős bevonásával;

h) a felügyeleti hatóságot értesíti az adatvédelmi incidensről az Általános Szabályozás 5.9. fejezetben foglaltak alkalmazásával;

f) az adatvédelmi hatósági megkeresést megvizsgálja. Ennek keretében az adatvédelmi tisztviselő az adatvédelmi felelős bevonásával;

fa) az adatvédelmi hatósági megkereséssel érintett szakterülettől/szakterületektől – az adatkezelési megbízott útján – adatok rendelkezésre bocsátását és álláspontja (álláspontjuk) kifejtését kéri, illetve felvilágosítást, magyarázatot, szakmai állásfoglalást, illetve az adatvédelmi tisztviselő döntésének előkészítésében való egyéb közreműködést kér;

fb) kérheti az informatikai rendszerekben tárolt adatokhoz és az adatkezelési műveletekhez való hozzáférés biztosítását;

fc) szükség esetén a Jogi és Igazgatási Osztálytól jogszabály-értelmezési kérdésben támogatást kér;

fd) az általa az adatvédelmi hatósági megkeresés megválaszolásához szükségesnek ítélt egyéb intézkedést kérhet.

Az adatvédelmi felügyeleti hatóságtól érkező bármilyen küldeményt – amennyiben azt nem az adatvédelmi tisztviselőnek címezték és/vagy nem közvetlenül hozzá juttatta el az adatvédelmi felügyeleti hatóság – a küldeményt átvevő szervezeti egység haladéktalanul, de legkésőbb az átvételt követő munkanapon átadja az adatvédelmi tisztviselőnek, illetve továbbítja az adatvedelem@dpckorhaz.hu email címre.

Az adatvédelmi tisztviselő az adatvédelmi hatósági megkeresést megvizsgálja. Ennek keretében az adatvédelmi tisztviselő az adatvédelmi felelős bevonásával

a) az adatvédelmi hatósági megkereséssel érintett szakterülettől/szakterületektől – az adatkezelési megbízott útján – adatok rendelkezésre bocsátását és álláspontja (álláspontjuk) kifejtését kéri, illetve felvilágosítást, magyarázatot, szakmai állásfoglalást, illetve az adatvédelmi tisztviselő döntésének előkészítésében való egyéb közreműködést kér;

b) kérheti az informatikai rendszerekben tárolt adatokhoz és az adatkezelési műveletekhez való hozzáférés biztosítását;

c) szükség esetén a Jogi és Igazgatási Osztálytól jogszabály-értelmezési kérdésben támogatást kér;

d) az általa az adatvédelmi hatósági megkeresés megválaszolásához szükségesnek ítélt egyéb intézkedést kérhet.

Az adatvédelmi tisztviselő illetőleg az adatvédelmi felelős által kért adatot, információt, felvilágosítást, magyarázatot, hozzáférést, illetve jogi és szakmai állásfoglalást megjelölt határidőben kell a rendelkezésére bocsátani, az érintett szakterület munkatársainak.

Az adatvédelmi hatósági megkeresésekre adandó választ az adatvédelmi felelős készíti elő, a főigazgató az adatvédelmi tisztviselővel egyeztetve kiadmányozza és küldi meg az adatvédelmi felügyeleti hatóságnak.

Az adatvédelmi tisztviselő illetőleg adatvédelmi felelős a tanúsítási eljárás kezdeményezésére irányuló eljárást, a magatartási kódex jóváhagyására, adattovábbítási szerződéses feltételek jóváhagyására, kötelező erejű intézményi szabályok jóváhagyására irányuló adatvédelmi felügyeleti hatósági eljárást az említett dokumentumok tervezetének főigazgató általi jóváhagyást követően indítja meg.

Az adatvédelmi felügyeleti hatósági eljárásban az Intézményt a főigazgató általi megbízása esetén az adatvédelmi tisztviselő képviseli. Az adatvédelmi felügyeleti hatósági eljárásban az adatvédelmi felelős és a Jogi és Igazgatási Osztály szükség szerint közreműködik.

Az adatvédelmi felügyeleti hatóság határozata elleni jogorvoslati eljárás megindításáról az adatvédelmi tisztviselő az érintett szakterület vezetőjének, az adatvédelmi felelős és a Jogi és Igazgatási Osztály véleményének kikérése után dönt. A jogorvoslati eljárásban az Intézmény képviseletét a Jogi és Igazgatási Osztály biztosítja. A jogorvoslati kérelem előkészítésében, megszövegezésében, a perstratégia kialakításában, továbbá a jogorvoslati eljárás során az Intézmény képviselőjét az adatvédelmi tisztviselő támogatja.

Az adatvédelmi felügyeleti hatóság helyszíni vizsgálata során követendő eljárás meghatározására az érintett területek bevonásával kerül sor.

5.11. HARMADIK ORSZÁGBA IRÁNYULÓ ADATTOVÁBBÍTÁS KÜLÖNÖS SZABÁLYAI

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

Az érintett szervezeti egység az adatvédelmi felelős, – szükség esetén az adatvédelmi tisztviselő, a Jogi és Igazgatási Osztály, az infomációbiztonsági szakterület, véleményének kikérése után – javaslatot tesz az adattovábbítás módjára, az adatátadás során alkalmazandó biztosítékok körére.

Abban az esetben, ha nem harmadik országba történik az adattovábbítás, akkor annak úgy kell megvalósulnia, mintha az Magyarországon belül történne, azaz, ha van az adatkezelésnek célja és jogalapja mind az adatkezelő, mind a címzett3 oldalán – figyelemmel az adattakarékosság elvére is –, akkor a cél eléréshez szükséges személyes (beleértve a különleges) adatok továbbítása végrehajtható a szükséges és elégséges adatvédelem, csatorna védelem és titkosítás mellett. Természetesen ezek a szabályok irányadók akkor is, ha az nem harmadik országbéli, külföldi egészségügyi szolgáltató adattovábbításra irányuló megkereséssel fordul a hazai egészségügyi szolgáltatóhoz. A lehetséges jogi alapok tehát a GPDR 6. cikk (1) bek. a)-e) pont valamelyike és a 9. cikk (2) bek. a) vagy h) vagy i) alpontja.

Abban az esetben pedig, ha harmadik országba történik az adattovábbítás, akkor a személyes adatok harmadik országba történő továbbítása előtt vizsgálni kell, hogy

a) a harmadik országba történő adattovábbítás GDPR 45-46. cikk szerinti feltételei valamelyike teljesül-e, és

b) az adattovábbítás elengedhetetlenül szükséges-e.

c) Az adattovábbítás lehetséges jogi alapjai pedig a következőképpen alakulnak: a GPDR 6. cikk (1) bek. a)-e) pont valamelyike, továbbá a 9. cikk (2) bek. a) vagy h) vagy i) alpontja, továbbá a GDPR 45. cikke alapján a Bizottság által közzétett megfelelőségi határozat; vagy

d) a GPDR 6. cikk (1) bek. a)-e) pont valamelyike, továbbá a 9. cikk (2) bek. a) vagy h) vagy i) alpontja, továbbá – megfelelőségi határozat hiányában – a GDPR 46. cikkében írott mechanizmusok valamelyike. A lehetséges mechanizmusok

da) közhatalmi vagy közfeladatot ellátó szervek közötti, jogilag kötelező erejű, kikényszeríthető jogi eszköz;

db) kötelező erejű vállalati szabályok (BCR);

dc) a Bizottság által elfogadott általános adatvédelmi kikötések;

[3] A GDPR 4. cikk 9. pontja szerint "címzett" az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e.

dd) az adatvédelmi felügyeleti felügyelő hatóság által elfogadott és a Bizottság által jóváhagyott általános adatvédelmi kikötések;

de) jóváhagyott magatartási kódex, amely kötelező erővel és kikényszeríthető módon tartalmazza az adatvédelmi – beleértve az érintett jogai gyakorlásának biztosítására vonatkozó – garanciákat;

df) jóváhagyott tanúsítási mechanizmus, amely kötelező erővel és kikényszeríthető módon érinti az adatvédelmi – beleértve az érintett jogai gyakorlásának biztosítására vonatkozó – garanciákat;

dg) az adatot továbbító adatkezelő és a címzett, harmadik országbeli adatkezelő/adatfeldolgozó között létrejött, az illetékes adatvédelmi felügyelő hatóság által engedélyezett szerződéses rendelkezések. (Itt kívánjuk megjegyezni, hogy az adatkezelőknek (adatátadóknak) az Általános Szerződési Feltételek megkötésével egyidejűleg széleskörű vizsgálatot és értértékelést kell lefolytatniuk annak megállapítása érdekében, hogy az adattovábbítás célországában ténylegesen érvényesülni tudnak-e a személyes adatok védelmére vonatkozó garanciák. Amennyiben nem, úgy az Általános Szerződés Feltételek megkötése ellenére sem lesz jogszerű az adattovábbítás.)

dh) közhatalmi vagy közfeladatot ellátó szervek között létrejött, az illetékes adatvédelmi felügyelő hatóság által engedélyezett közigazgatási megállapodásba illesztendő rendelkezések, amelyben szerepelnek az érintett jogai biztosítására, illetve a jogorvoslatra vonatkozó rendelkezések is;

e) vagy az előző két pontban írtak (tehát megfelelőségi határozat, illetve a megfelelőséget biztosító mechanizmusok) hiányában

ea) a GDPR 49. cikk (1) bek. a) pont alapján (az érintett a személyes adatok védelmi szintjének nem megfelelőségéből adódó kockázatok ismeretében adott, kifejezett hozzájárulása),

eb) GDPR 49. cikk (1) bek. b) vagy c) pontjai (szerződéses jogalapok) alapján vagy

ec) a GDPR 49. cikk (1) bek. f) alapján (ha az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására, az érintett vagy más személy létfontosságú érdekének védelme érdekében) történő adattovábbítás4

5.12. Belső adatvédelmi ellenőrzési eljárás

A belső adatvédelmi ellenőrzési eljárás célja, hogy az adatvédelmi felelős illetőleg tisztviselő meggyőződjön arról, hogy az Intézmény egyes szervezeti egységei az adatvédelemmel kapcsolatos jogszabályoknak és belső szabályzatoknak megfelelően kezelik-e az adatokat.

[4] Az EU-USA Adatvédelmi Pajzs érvénytelenítése körében az EUB megállapította, hogy a 2016/1250 számú határozat a nemzetbiztonság, a közérdek és a bűnüldözés követelményeinek elsőbbségét fejezi ki, amely így lehetővé teszi a beavatkozást az EU-s állampolgárok alapvető jogaiba, amennyiben személyes adataikat az Egyesült Államokba továbbítják, tekintettel arra, hogy az érintetteknek nem biztosított bíróság előtt érvényesíthető jogokat, ezáltal e személyek számára nem elérhető jogorvoslati lehetőség olyan szerv előtt, amely az uniós jogban megkövetelt garanciákkal lényegében azonos garanciákat nyújtana. A fentiek értelmében az Egyesült Államokba történő adattovábbítás lehetséges jogalapjait tehát csak a GDPR 49. cikkében lehet keresni, ami egyedi esetekben, a GDPR nyújtotta védelem hiányából fakadó kockázatokra is kitérő részletes tájékoztatás birtokában ad lehetőséget adattovábbításra.

Az adatvédelmi felelős illetőleg tisztviselő éves ellenőrzési tervet készít. Az éves ellenőrzési tervnek az ellenőrzés alá vont szervezeti egység nevét és az ellenőrzés várható időpontját, továbbá az ellenőrzés tárgykörét kell tartalmaznia. Az éves ellenőrzési terveket úgy kell elkészíteni, hogy hároméves időtartam alatt lehetőség szerint minden szervezeti egység ellenőrzésére sor kerüljön. Az éves ellenőrzési tervet legkésőbb adott év február 28. napjáig kell elkészíteni és az Intézmény főigazgatója részére bemutatni.

Az éves ellenőrzési tervet az Intézmény főigazgatója hagyja jóvá.

Az adatvédelmi felelős illetőleg tisztviselő az ellenőrzés lefolytatásáról az érintett szervezeti egység vezetőjét az ellenőrzés kezdete előtt 10 nappal tájékoztatja, melyben az eljárás kezdő időpontjára is javaslatot tesz. A szervezeti egység vezetője köteles gondoskodni arról, hogy az adatvédelmi felelős/adatvédelmi tisztviselő a javasolt időpontban megkezdhesse ellenőrzését, illetve szükség esetén – legfeljebb tíz munkanapon belüli – új időpontra tesz javaslatot.

Az ellenőrzés során adatvédelmi felelős illetőleg tisztviselő a szervezeti egység irodahelységeibe beléphet, a szervezeti egység – ellenőrzés tárgyával összefüggésben kezelt – irataiba betekinthet, a szervezeti egység munkatársaitól tájékoztatást kérhet adott üggyel kapcsolatos adatkezelésről.

Az adatvédelmi felelős illetőleg tisztviselő az ellenőrzés megtörténtéről jegyzőkönyvet készít, melyet az ellenőrzött szervezeti egység vezetőjével mindketten aláírnak. A jegyzőkönyv az ellenőrzött szervezeti egység, valamint annak vezetője nevét, az ellenőrzés lefolytatásának tényét, annak időpontját és időtartamát tartalmazza.

Az adatvédelmi felelős illetőleg tisztviselő a lefolytatott ellenőrzésről vizsgálati jelentést készít, melynek mellékletét képezi az ellenőrzésről készült jegyzőkönyv. A vizsgálati jelentés tartalmazza az adott szervezeti egységnél vizsgált körülményeket, adatokat, megállapításokat. A vizsgálati jelentés tervezetére a szervezeti egység vezetője 10 napon belül észrevételt tehet. Az észrevételezés elmaradása a szervezeti egység vezetőjének egyetértését jelenti. Az adatvédelmi ellenőrzések főigazgató által jóváhagyott jelentéseit az iratkezelési szabályok szerint kell kezelni, s mind a papír alapú, mind az elektronikus változatát 5 évig meg kell őrizni.

Ha az adatvédelmi felelős illetőleg tisztviselő megállapítja, hogy az adatkezelés az ellenőrzés alá vont szervezeti egységnél nem a belső szabályzatoknak vagy jogszabályoknak megfelelően történik, javaslatot tesz a szabályszerű adatkezelés – meghatározott határidőn belüli – helyreállítására. Az ezek alapján megtett intézkedésekről a szervezeti egység vezetője tájékoztatást nyújt. Az adatvédelmi tisztviselő a megtett intézkedéseket, illetve azok betartását bármikor jogosult ellenőrizni.

Az adatvédelmi felelős illetőleg tisztviselő rendkívüli ellenőrzést is lefolytathat szúrópróbaszerűen vagy az adatvédelmi incidens kivizsgálása során tett megállapítás következményeként, valamint, ha adatvédelmi szempontból az indokolt, különösen, ha a személyes adatkezeléssel érintettek száma jelentős. Rendkívüli ellenőrzésnek minősül az éves

ellenőrzési tervben nem szereplő ellenőrzés. A rendkívüli ellenőrzést az Intézmény főigazgatója előzetesen engedélyezi.

Az adott ellenőrzéssel kapcsolatban az Intézmény főigazgatója külön tájékoztatást kérhet az adatvédelmi felelőstől illetőleg tisztviselőtől, egyébként az adatvédelmi tisztviselő illetőleg az adatvédelmi felelős évente egy alkalommal, legkésőbb a tárgyévet követő év február 28. napjáig összefoglaló jelentést készít az általa a tárgyévben lefolytatott ellenőrzésekről, amelyet az Intézmény főigazgatója részére küld meg.

Amennyiben az adatbiztonsági szabályok és intézkedések megtartásának ellenőrzése információbiztonsági szakértelmet is megkíván, az adatvédelmi ellenőrzésbe az információbiztonsági felelőst is be kell vonni.

Az adatvédelmi ellenőrzést legfeljebb 60 nap alatt el kell végezni, ami szükség esetén egyszer 30 nappal meghosszabbítható. Az ennél hosszabb időt igénylő ellenőrzéseket szakaszokra kell bontani, hogy az ellenőrzés ne tartson az indokoltnál hosszabb ideig.

5.13. EGÉSZSÉGÜGYI ADATVÉDELMI SZABÁLYOZÁS

5.13.1. Az egészségügyi szabályozás célja

Az Egészségügyi Adatvédelmi Szabályozás (a továbbiakban: Egészségügyi Szabályozás) az egészségi állapotra vonatkozó különleges személyes adatok és az azokhoz kapcsolódó személyes adatok kezelésének feltételeit határozza meg.
Az Egészségügyi Szabályozás célja, hogy biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza az adatokhoz történő jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

5.13.2. Az általános szabályozás és az egészségügyi szabályozás kapcsolata

A GDPR 9. cikk (4) bekezdése alapján a tagállamok további feltételeket – köztük korlátozásokat – tarthatnak hatályban, illetve vezethetnek be a genetikai adatok, a biometrikus adatok és az egészségügyi adatok kezelésére vonatkozóan. Az Egészségügyi Szabályozás az egészségi állapotra vonatkozó különleges személyes adatok és az azokhoz kapcsolódó személyes adatok kezelésének feltételeit határozza meg. Az Egészségügyi Szabályozás az Általános Szabályozáshoz, mint speciális rendelkezés viszonyul az általános szabályokhoz. Minden olyan kérdésben, amelyre vonatkozóan az Egészségügyi Szabályozás nem tartalmaz eltérő, illetőleg kiegészítő rendelkezéseket, az Általános Szabályozás előírásai megfelelően alkalmazandók.

5.13.3. Az egészségi állapotra vonatkozó alapfogalmak

genetikai minta: minden, a Hgatv. szerinti humángenetikai vizsgálat, illetve humángenetikai kutatás céljából levett vagy a törvény keretei között e célra egyébként felhasználni kívánt, emberből származó biológiai anyagminta;

kódolt genetikai minta vagy adat: olyan genetikai minta vagy adat, amely mellett a mintát szolgáltató személyre vonatkozó összes személyazonosító adatot kóddal helyettesítették;

biobank: genetikai mintát és az ehhez kapcsolódó genetikai és személyazonosító adatokat Hgatv. szerinti humángenetikai vizsgálat, illetve humángenetikai kutatás céljából tartalmazó - jogszabályban meghatározott működési, illetve kutatási engedéllyel rendelkező -

mintagyűjtemény, ide nem értve az egészségügyi ellátás vagy orvostudományi kutatás céljából levett, vagy valamilyen egészségügyi ellátás, beavatkozás során másodlagosan keletkezett biológiai sejt- és szövetmintákat, valamint e mintákhoz kapcsolódó személyazonosító és egyéb egészségügyi adatokat tartalmazó mintagyűjteményt;

pszeudonimizált genetikai minta vagy adat: olyan kódolt genetikai minta vagy adat, amelynél a személyazonosító adatot helyettesítő kódot az érintett személy kizárólagos rendelkezésére bocsátottak;

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

orvosi titok: a gyógykezelés során az adatkezelő tudomására jutott egészségügyi és személyazonosító adat, továbbá a szükséges vagy folyamatban lévő, illetve befejezett gyógykezelésre vonatkozó, valamint a gyógykezeléssel kapcsolatban megismert egyéb adat;

EESZT: Elektronikus Egészségügyi Szolgáltatási Tér;

egészségügyi dokumentáció: a gyógykezelés során a betegellátó tudomására jutott egészségügyi és személyazonosító adatokat tartalmazó feljegyzés, nyilvántartás vagy bármilyen más módon rögzített adat, függetlenül annak hordozójától vagy formájától;

kezelést végző orvos: 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;

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;

egészségügyi szolgáltatás: működési engedély birtokában végezhető egészségügyi tevékenységek összessége, amely az egyén egészségének megőrzése, továbbá a megbetegedések megelőzése, korai felismerése, megállapítása, gyógykezelése, életveszély elhárítása, a megbetegedés következtében kialakult állapot javítása vagy a további állapotromlás megelőzése céljából a beteg vizsgálatára és kezelésére, gondozására, ápolására, egészségügyi rehabilitációjára, a fájdalom és a szenvedés csökkentésére, továbbá a fentiek érdekében a beteg vizsgálati anyagainak feldolgozására irányul, ideértve a gyógyszerekkel, a gyógyászati segédeszközökkel, a gyógyászati ellátásokkal kapcsolatos külön jogszabály szerinti tevékenységet, valamint a szülészeti ellátást, az emberi reprodukcióra irányuló különleges eljárásokat, a művi meddővételt, az emberen végzett orvostudományi kutatásokat, stb.;

betegellátó: a kezelést végző orvos, az egészségügyi szakdolgozó, az érintett gyógykezelésével kapcsolatos tevékenységet végző egyéb személy, a gyógyszerész;

kapcsolati kód: olyan, az érintett azonosítására szolgáló egyedi azonosító kód, mely nem személyazonosító adatból származik, valamint tartalmaz véletlenszerűen megállapított, egyedi elemet, továbbá kizárja az érintett személyazonosító adatainak a kódból való visszafejtését, vagy összekapcsolását, de biztosítja az érintettre vonatkozó egészségügyi és genetikai adatok

személyazonosításra alkalmatlan összekapcsolását, azaz álnevesítéses technikával történő kezelését;

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;

sürgős szükség: az egészségi állapotban hirtelen bekövetkezett olyan változás, amelynek következtében azonnali egészségügyi ellátás hiányában az érintett közvetlen életveszélybe kerülne, illetve súlyos vagy maradandó egészségkárosodást szenvedne.

5.14. EGÉSZSÉGÜGYI ADATVÉDELEM

5.14.1. Az egészségügyi adatkezelés célja

5.14.1.1. Az egészségügyi és személyazonosító adat kezelésének célja

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

5.14.1.2. Az 5.14.1.1. pontban meghatározottakon túl - törvényben meghatározott esetekben - az alábbi célból lehet adatot kezelni

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 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 az Rtv-ben meghatározott feladatok ellátására kapott felhatalmazás körében bűnmegelőzés.

i) Az Nsztv-ben meghatározott feladatok ellátása, az abban kapott felhatalmazás körében.
j) Közigazgatási hatósági 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, közszolgálati, vagy állami szolgálati jogviszony, hivatásos szolgálati viszony vagy egyéb jogviszony keretében történik.
p) Köznevelés, szakképzés, illetve felsőoktatás és szakképzés céljából az oktatásra, illetve képzésre való alkalmasság megállapítása.
q) A katonai szolgálatra, illetve a személyes honvédelmi kötelezettség teljesítésére való alkalmasság megállapítása.
r) Munkanélküli ellátás, foglalkoztatás elősegítése, valamint az ezzel összefüggő ellenőrzés.
s) Az egészségügyi ellátásokra jogosultak részére vényen rendelt gyógyszer, gyógyászati segédeszköz és gyógyászati ellátás folyamatos és biztonságos kiszolgáltatása, illetve nyújtása érdekében
t) A munkabalesetek, foglalkozási megbetegedések - ideértve a fokozott expozíciós eseteket is - kivizsgálása, nyilvántartása és a szükséges munkavédelmi intézkedések megtétele.
u) Az egészségügyi dolgozóval 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-tervezés.
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.
aa) Az Európai Unión belüli határon átnyúló egészségügyi ellátáshoz kapcsolódó jogok érvényesítése.

A fenti, 5.14.1.1. és 5.14.1.2. pontokban meghatározott 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.

Az 5.14.1.1. és 5.14.1.2. pontokban meghatározott adatkezelési célokra csak annyi és olyan egészségügyi, illetve személyazonosító adat kezelhető, amely az adatkezelési cél megvalósításához elengedhetetlenül szükséges.
Fentieket meghaladóan egészségügyi adatot csak oly módon lehet kezelni, hogy az érintett személyazonossága ne legyen megállapítható.

5.14.2. Egészségügyi adatkezelésre jogosultak köre

Az Intézményben az egészségügyi és a hozzájuk kapcsolódó személyazonosító adat kezelésére az alábbiak jogosultak:

a) a kezelést végző orvos,
b) az érintett kezelésében, ellátásában résztvevő egészségügyi szakdolgozó,
c) az érintett gyógykezelésével kapcsolatos tevékenységet végző egyéb személy,
d) a gyógyszerész,
e) a főigazgató,
f) az orvosigazgató,
g) adatvédelmi felelős
h) az adatvédelmi tisztviselő.

5.14.3. Titoktartási kötelezettség

Az egészségügyi dolgozót, valamint az egészségügyi szolgáltatóval munkavégzésre irányuló vagy egyéb jogviszonyban álló más személyt minden, a beteg állapotával kapcsolatos, valamint az egészségügyi szolgáltatás nyújtása során tudomására jutott adat és egyéb tény vonatkozásában, időbeli korlátozás nélkül, titoktartási kötelezettség terheli, függetlenül attól, hogy az adatokat közvetlenül a betegtől, vizsgálata vagy gyógykezelése során, illetve közvetetten az egészségügyi dokumentációból vagy bármely más módon ismer meg.
A titoktartási kötelezettség nem vonatkozik arra az esetre, ha ez alól a beteg felmentést adott vagy a jogszabály az adat szolgáltatásának kötelezettségét írja elő.

A betegnek joga van rendelkezni arról, mely személyek jogosultak adatainak (teljes vagy részleges) megismerésére, illetve kiket zár ki annak (teljes vagy részleges) megismeréséből.
Az adatkezelés során mindvégig biztosítani kell az adatok védelmét és meg kell akadályozni, hogy azok megsemmisüljenek, nyilvánosságra kerüljenek, azokat megváltoztathassák, vagy arra jogosulatlan személy az adatokhoz hozzáférjen. Az adatkezelő titoktartási kötelezettsége magába foglalja, hogy működése során tudomására jutott információkat csak a hivatkozott törvényben szabályozottak szerint közölheti.

5.14.4. A tájékoztatáshoz, valamint az önrendelkezéshez való jog, illetve kötelezettség

Az érintett, az (EU) 2016/679 európai parlamenti és tanácsi rendelet 15. cikk (3) bekezdésében, valamint az Eüak. rendelkezéseiben meghatározottak alapján megilleti a tájékoztatáshoz való jog. Az érintett tájékoztatására vonatkozó eljárásrend tekintetében az 5.5.2. pontjában foglalt rendelkezések mellett a Szabályzat az érintetti valamint hatósági bejelentés nyilvántartása a Dél-pesti Centrumkórház-Hematológiai és Infektológiai Intézetben a GDPR megfeleléshez elnevezésű dokumentum előírásai is megfelelően alkalmazandók.

A fenti jog

a) az érintett ellátásának időtartama alatt az általa írásban felhatalmazott személyt,

b) az érintett ellátásának befejezését követően az általa teljes bizonyító erejű magánokiratban felhatalmazott személyt illeti meg.

c) az érintett házastársa, egyeneságbeli rokona, testvére, valamint élettársa - írásbeli kérelme alapján a beteg életében, illetőleg halálát követően - akkor is jogosult a fenti jog gyakorlására, ha

ca) az egészségügyi adatra a házastárs, az egyeneságbeli rokon, a testvér, illetve az élettárs, valamint leszármazóik életét, egészségét befolyásoló ok feltárása, illetve e személyek egészségügyi ellátása céljából van szükség, és

cb) az egészségügyi adat más módon való megismerése, illetve az arra való következtetés nem lehetséges. Ebben az esetben csak azoknak az egészségügyi adatoknak a megismerése lehetséges, amelyek a ca) pont szerinti okkal közvetlenül összefüggésbe hozhatóak.

Az érintett halála esetén az érintett közeli hozzátartozója, törvényes képviselője, örököse – írásos kérelme alapján - jogosult a halálozással összefüggő, vagy összefüggésbe hozható, a megelőző kezeléssel kapcsolatos egészségügyi adatokat megismerni, az egészségügyi dokumentációba betekinteni, valamint azokról saját költségére másolatot kapni[5].

A genetikai mintavétel előtt - függetlenül a genetikai adat kezelésének céljától - a rendelkezésre jogosult részletes tájékoztatáson alapuló, írásban rögzített beleegyezése szükséges. Ha a genetikai minta kutatási célra felhasználásra kerül, a beleegyező nyilatkozat aláírása előtt az érintettet (a kutatás alanyát) a kutatásba való beleegyezését megelőzően szóban és írásban tájékoztatni kell

a) a kutatásban való részvételének önkéntességéről, valamint arról, hogy a beleegyezés bármikor, indoklás és hátrányos következmények nélkül visszavonható;

b) a tervezett vizsgálat, vagy beavatkozás kísérleti jellegéről, céljáról, várható időtartamáról;

c) a kutatás során elvégzendő vizsgálatok, illetve egyéb beavatkozások jellegéről, tartalmáról és esetleges kockázatairól, következményeiről, valamint a kutatással járó kellemetlenségekről;

d) a kutatás alanya vagy mások számára várható előnyökről;

e) a kutatásban való részvétel helyett alkalmazható esetleges egyéb vizsgálatokról, beavatkozásokról;

f) a kutatásban való részvétel kockázatának körébe tartozó egészségkárosodás jellegéről és gyógykezeléséről, valamint a kártalanításról, illetve kártérítésről;

g) a kutatásért felelős személy (ek) nevéről.

h) a genetikai minta és adat tárolásának módjairól,

j) a különböző formában tárolt genetikai minták, illetve adatok azonosíthatóságának lehetőségeiről, valamint

k) az érintett egyéb nyilatkozata hiányában a genetikai minta archivált gyűjteménybe való bekerüléséről,

l) a tárolt genetikai minták esetleges továbbításáról.

(1) Genetikai adat az érintettel, valamint az érintett által közokiratban, teljes bizonyító erejű magánokiratban vagy írásképtelensége esetén két tanú együttes jelenlétében megtett szóbeli nyilatkozatával megnevezett személlyel, illetve azzal közölhető, aki a vonatkozó törvény alapján a genetikai adat megismerésére jogosult. Amennyiben a közeli hozzátartozó betegsége megelőzése, betegsége természetének megismerése, gyógykezelése, valamint utódaira

[5] **Eüak 7. § (7)**

vonatkozó betegségkockázat megítélése érdekében ez szükséges, akkor a genetikai adatot a közeli hozzátartozó is megismerheti genetikai tanácsadás keretében.

Elhunyt személyből genetikai minta levételére, a levett, személyazonosító adatokkal együttesen tárolt vagy kódolt genetikai minta vizsgálatára, humángenetikai kutatás céljából történő igénybevételére vagy a belőle származó genetikai adat felhasználására akkor kerülhet sor, ha az elhunyt ez ellen életében nem tett tiltakozó nyilatkozatot.

Az egészségügyi adat felvétele a gyógykezelés része. A kezelőorvos dönti el, a szakma szabályainak megfelelően – a kötelezően felveendő adatokon kívül - mely egészségügyi adat felvétele szükséges az **5.14.1.1.** alpont szerinti célból.

Az érintett gyógykezelésével kapcsolatos tevékenységet végző egyéb személy a kezelést végző orvos utasításának megfelelően, illetve a feladatai ellátásához szükséges mértékben vehet fel egészségügyi adatot.

5.14.5. A gyógykezelés során jelenlévő személyek

A gyógykezelés során a kezelést végző orvoson és egyéb betegellátó személyen kívül csak az lehet jelen, akinek a jelenlétéhez az érintett hozzájárul. Az érintett hozzájárulása nélkül jelen lehet az érintett emberi jogainak és méltóságának tiszteletben tartásával:

a) más személy, ha a gyógykezelés rendje több beteg egyidejű ellátását igényli,
b) a rendőrség hivatalos állományú tagja, amennyiben a gyógykezelésre fogvatartott személy esetében kerül sor,
c) a büntetés-végrehajtási szervezet szolgálati jogviszonyban álló tagja, amennyiben a gyógykezelésre olyan személy esetében kerül sor, aki a büntetés-végrehajtási intézetben szabadságelvonással járó büntetését tölti, és a gyógykezelést végző betegellátó biztonsága, illetve szökés megakadályozása céljából erre szükség van,
d) a b)-c) pontok szerinti személyek, ha bűnüldözési érdekből a beteg személyi biztonsága ezt indokolttá teszi, és a beteg nyilatkozattételre képtelen állapotban van,
e) szakember-képzésre kijelölt intézményben orvostanhallgató, egészségügyi szakképzésben résztvevő szakdolgozó (de erről a beteget ellátása előtt tájékoztatni kell),
f) az a személy, aki az érintettet az adott betegség miatt korábban gyógykezelte, kivéve, ha ez ellen az érintett kifejezetten tiltakozott,
g) akinek a főigazgató vagy az orvosigazgató, illetve az adatvédelmi tisztviselő szakmai-tudományos célból engedélyt adott, kivéve, ha ez ellen az érintett kifejezetten tiltakozott,
h) a fentieken kívül csak a beteg hozzájárulásával lehet jelen más személy.

5.14.6. Adatszolgáltatás az érintett részéről

Az egészségügyi és a személyazonosító adatoknak az érintett részéről történő szolgáltatása - az egészségügyi ellátás igénybevételéhez kötelezően előírt személyazonosító adatok és az 5.14.6. pont a)-g) pontjaiban meghatározott esetek kivételével - önkéntes.

Az Intézmény egészségügyi szolgáltatásainak önként történő igénybevétele esetén a gyógykezeléssel összefüggő egészségügyi és személyazonosító adatok kezelésére szolgáló hozzájárulást az érintett részéről - ellenkező nyilatkozat hiányában - megadottnak kell tekinteni és erről az érintettet (törvényes képviselőjét) tájékoztatni kell.

Sürgős szükség, valamint az érintett belátási képességének hiánya esetén az önkéntességet vélelmezni kell.

Az érintett (törvényes képviselője) köteles a betegellátó felhívására egészségügyi és személyazonosító adatait átadni:

a) ha valószínűsíthető, vagy beigazolódott, hogy a törvény mellékletében felsorolt valamely betegség kórokozója által fertőződött, vagy fertőzéses eredetű mérgezésben, illetve fertőző betegségben szenved, kivéve a HIV vírusra vonatkozó szűrővizsgálat esetét,
b) ha arra a törvényben felsorolt szűrő- és alkalmassági vizsgálatok elvégzéséhez van szükség,
c) heveny mérgezés esetén,
d) ha valószínűsíthető, hogy az érintett a törvény melléklete szerinti foglalkozási eredetű megbetegedésben szenved,
e) ha az adatszolgáltatásra magzat, vagy kiskorú gyermek gyógykezelése, egészségi állapotának megőrzése vagy védelme érdekében van szükség,
f) ha bűnüldözés, bűnmegelőzés céljából, továbbá ügyészségi, bírósági eljárás, illetve szabálysértési vagy közigazgatási hatósági eljárás során az illetékes szerv a vizsgálatot elrendelte
g) ha az adatszolgáltatásra a nemzetbiztonsági szolgálatokról szóló törvény szerinti ellenőrzés céljából van szükség.

5.14.7. A gyógykezelés céljából történő adatkezelés

Az érintett kezelését végző orvos az 5.14.1.1. alpont szerinti cél érdekében - ha az érintett ezt írásban nem tiltotta meg - jogosult az érintett által a kötelező egészségbiztosítás terhére igénybe vett egészségügyi ellátás adatairól tudomást szerezni úgy, hogy az adatokat az egészségbiztosítási szerv elektronikus lekérdezés formájában biztosítja számára.
A kezelést végző orvos jogosult áttekinteni a Nemzeti Egészségbiztosítási Alapkezelő (továbbiakban: NEAK) adatbázisában, hogy az általa ellátott biztosítottak mikor, hol és milyen típusú egészségügyi ellátásokat vettek igénybe a kötelező egészségbiztosítás terhére. Ettől az alapértelmezett szabálytól csak abban az esetben lehet eltérni, ha az érintett jelzi a NEAK felé, hogy tiltakozik az ellen, hogy orvosai a fenti adatokhoz hozzáférjenek.

Az érintettet a kezelést végző orvos tájékoztatja a tiltakozás lehetőségéről.

Az érintett a tiltakozását a NEAK honlapján (www.neak.gov.hu) is elérhető dokumentumot (**SZ-39 A02 Kezelőorvos betegéletút lekérdezési lehetősége tiltakozás**) kitöltve eljuttatja az egészségbiztosítási szerv részére. Ezt megteheti személyesen, postai úton vagy elektronikus úton.

Az érintett a korábbi tiltakozását feloldhatja oly módon, hogy a NEAK honlapján (www.neak.gov.hu) is elérhető dokumentumot (**SZ-39 A03 Kezelőorvos betegéletút lekérdezési lehetősége tiltakozás feloldása**) kitöltve eljuttatja az egészségbiztosítási szerv részére. Ezt megteheti személyesen, postai úton vagy elektronikus úton.
A fenti egyedi adatbetekintésre, illetve adatkezelésre történő felhatalmazás nem jogosítja fel a kezelőorvost sem az adatok esetleges továbbadására, sem más célú felhasználására.

5.14.8. Adattovábbítás az egészségügyi intézmény részéről jogszabály alapján

Az adatvédelmi jogszabályokban foglalt rendelkezések alapján az érintettek adatai (ideértve a korábbi betegségre vonatkozó egészségügyi adatokat is) az érintett hozzájárulása nélkül is jogszerűen továbbíthatók az alábbi esetekben:

a) ha mások életének, testi épségének és egészségének védelme szükségessé teszi,
b) az érintett további ápolását, gondozását végző személyekkel közölni lehet azokat az egészségügyi adatokat, amelyek ismeretének hiánya az érintett egészségügyi állapotának károsodásához vezethet,
c) sürgős szükség esetén a kezelést végző orvos által ismert, a gyógykezeléssel összefüggésbe hozható minden egészségügyi és személyazonosító adat,
d) az érintett választott háziorvosa részére a beteg ellenkező tartalmú rendelkezésének hiányában,
e) az igazságügyi orvos szakértő részére,
f) olyan betegellátó részére, aki az orvosi vizsgálatban, a kórisme megállapításában, ill. a gyógykezelésben vagy műtétnél közreműködött,
g) olyan betegellátó részére, amely ugyan nem közreműködött a fentiekben, de amellyel az adatok közlése a kórisme megállapítása vagy az érintett további gyógykezelése érdekében szükséges,

A kezelést végző orvos az érintett egészségügyi- és személyazonosító adatait - a megkeresésnek megfelelő tartalommal és mélységben - köteles az alábbiakban felsorolt megkereső szerveknek továbbítani:

a) büntetőügyben: a nyomozóhatóságnak, ügyészségnek, bíróságnak, az előkészítő eljárást folytató szervnek, az igazságügyi szakértőnek,
b) polgári peres és nemperes, valamint közigazgatási hatósági ügyben: a közigazgatási hatóságnak, az ügyészségnek, a bíróságnak, az igazságügyi szakértőnek,
c) szabálysértési eljárásban: az eljárást lefolytató szervnek,
d) potenciális hadköteles és hadköteles személy esetén a fővárosi és megyei kormányhivatal járási (fővárosi kerületi) hivatalának, a Magyar Honvédség katonai igazgatási és központi adatfeldolgozó szervének, valamint a katonai egészségügyi alkalmasságot megállapító bizottságnak,
e) az Nsztv-ben meghatározott feladatok ellátása érdekében, az abban kapott felhatalmazás körében,
f) a Magyar Honvédség katonai igazgatási és központi adatfeldolgozó szervének, a kiképzett tartalékosok békeidőszakban történő hadi beosztásra történő kiírása és a kiképzett tartalékosok gyors és differenciált behívása érdekében, a honvédelemről és a Hvtv-ben meghatározott körben,
g) egészségügyi dolgozóval szemben folyamatban lévő etikai eljárás során az eljárás lefolytatására hatáskörrel és illetékességgel rendelkező kamarai szerv részére
h) a rendőrségről szóló törvényben meghatározott belső bűnmegelőzési és bűnfelderítési feladatokat ellátó, valamint a terrorizmust elhárító szerveknek a törvényben meghatározott feladatok ellátása érdekében, az abban kapott felhatalmazás körében,
i) halottvizsgálat során a halottvizsgálatot végző orvosnak,
j) a légi-, a vasúti és a víziközlekedési balesetek és egyéb közlekedési események szakmai vizsgálatáról szóló törvényben, valamint a polgári légiközlekedési balesetek és repülőesemények vizsgálatáról és megelőzéséről és a 94/56/EK irányelv hatályon kívül helyezéséről szóló, 2010. október 20-i 996/2010/EU európai parlamenti és

tanácsi rendeletben meghatározott szakmai vizsgálat során a közlekedésbiztonsági szerv részére.

Az adattovábbításra vonatkozó eljárásrend vonatkozásában a Szabályzat az érintetti valamint hatósági bejelentés nyilvántartása a Dél-pesti Centrumkórház-Hematológiai és Infektológiai Intézetben a GDPR megfeleléshez elnevezésű dokumentum előírásai megfelelően alkalmazandók.

Amennyiben a megkeresésben vagy adatkérésben az adatkezelés pontos célja és a kért adatok köre nincs meghatározva, úgy az orvosigazgató

- megfelelő indokolással elutasítja a kérelmet, vagy
- ha a kérelem formailag nem megfelelő, kiegészítésre hívja fel az adatkérőt.

Az érintett első ízben történő orvosi ellátásakor, ha az érintett 8 napon túl gyógyuló sérülést szenvedett és a sérülés feltehetően bűncselekmény következménye, a kezelőorvos a rendőrségnek haladéktalanul bejelenti az érintett személyazonosító adatait.

A kiskorú érintett első ízben történő egészségügyi ellátásakor - az érintett beleegyezése nélkül - az Intézmény megbízott orvosa köteles az Intézmény telephelye szerint illetékes gyermekjóléti szolgálatot haladéktalanul értesíteni, ha:

- feltételezhető, hogy a gyermek sérülése vagy betegsége bántalmazás, illetve elhanyagolás következménye,
- a gyermek egészségügyi ellátása során bántalmazásra, elhanyagolásra utaló körülményekről szerez tudomást.

Annak érdekében, hogy a fent ismertetett eseteken kívül továbbíthatóak legyenek az érintett egészségügyi és személyazonosító adatai, az adattovábbításhoz szükség van az érintett előzetes írásbeli hozzájárulására.

Minden olyan adat, melyből nem lehet visszakövetkeztetni az érintett személyére, az érintett hozzájárulása nélkül nyilvánosságra hozható és továbbítható, időbeli és területi korlátozás nélkül.

Az olyan adatot, melyből vissza lehet következtetni az érintett személyére, továbbítani lehet az érintett hozzájárulása nélkül olyan közérdekű feladatot ellátó szerv számára, amely az ilyen típusú adatot az érintett írásbeli hozzájárulása nélkül is jogosult nyilvánosságra hozni,

Egészségügyi és személyazonosító adatok csak jogszabályban meghatározott esetekben és módon, azaz vagy az érintett hozzájárulásával vagy jogszabály felhatalmazásával továbbíthatók, illetve kapcsolhatók össze. A különböző forrásból származó adatokat csak addig az időpontig és olyan mértékig lehet összekapcsolni, ameddig az a megelőzés, a gyógykezelés, a népegészségügyi, a közegészségügyi és járványügyi intézkedések megtétele érdekében feltétlenül szükséges. Amennyiben erre vonatkozóan az adatkezelőnek bármilyen aggálya merül fel, úgy a szükséges mértéket az adatvédelmi tisztviselő dönti el.
Ugyanezen feltételek szükségesek az egészségügyi és személyazonosító adatok helyesbítése és törlése esetén is, amennyiben azt nem maga az érintett kéri.

5.14.9. Közegészségügyi, járványügyi célból történő adatkezelés

Az Intézmény haladéktalanul köteles továbbítani az - az érintett lakóhelye, tartózkodási helye, illetve munkahelye szerint illetékes - kormányhivatal felé az adatfelvétel során tudomására jutott egészségügyi és személyazonosító adatot, ha:

a) jogszabályban meghatározott fertőző betegséget észlel, vagy annak gyanúja merül föl

b) A kormányhivatal közegészségügyi vagy járványügyi közérdekre hivatkozva - az anonim szűrővizsgálat HIV fertőzött és AIDS beteg kivételével - kérheti az érintett személyazonosító adatait.
c) Amennyiben az érintett annak megállapítása érdekében, hogy HIV vírusával fertőződött-e - személyazonosságának előzetes felfedése nélkül - szűrővizsgálaton kíván részt venni, személyazonosító adatait a betegellátó részére nem köteles átadni.

A közegészségügyi, járványügyi célból történő adatkezelésre vonatkozóan a részletes listát az Eüak. 1-3. számú melléklete tartalmazza.

5.14.10. Népegészségügyi célból történő adatkezelés

Amennyiben az érintett újszülött vagy csecsemő a Betegségek Nemzetközi Osztályozása (BNO) szerinti valamely veleszületett rendellenességben szenved, a kezelést végző orvos az érintett személyazonosító adatait és egészségügyi adatait, valamint törvényes képviselője nevét, illetve lakcímét továbbítja a külön jogszabály szerint vezetett Veleszületett Rendellenességek Országos Nyilvántartása (VRONY) részére.

> Amennyiben a magzatnál veleszületett rendellenességre utaló elváltozást észlelnek, az előző pont szerint kell eljárni, és az érintett személyazonosító adatain a várandós anya adatait kell érteni.

Spontán vagy indukált magzati halálozás, illetve halvaszületés esetén a VRONY által küldött kérdőívet a kezelőorvos tölti ki.

Ha az Intézmény, mint betegellátó az érintett betegnél népegészségügyi szempontból kiemelt jelentőségű vagy egyébként jelentős költségteherrel járó, a miniszteri rendeletben felsorolt megbetegedések valamelyikét észleli, vagy annak időszakos felülvizsgálatát végzi, az 5.14.1.1. a), c) és d) pontja, valamint az 5.14.1.2. b) pontja szerinti célból továbbítja az érintett személynek a miniszter rendeletében meghatározott személyazonosító és az észlelt megbetegedéssel összefüggő egészségügyi adatait az észlelt megbetegedést nyilvántartó betegségregisztert vezető szerv részére.

5.14.11. Az intézmény, mint betegségregisztert vezető szerv adatkezelése

Az Intézmény, mint a miniszteri rendeletben meghatározott betegségregisztert vezető szerv az általa felügyelt hematológiai szakterületen népegészségügyi szempontból kiemelt jelentőségű, társadalmi vagy egyéni szinten jelentős betegségteherrel járó betegségcsoportok tekintetében betegségregisztert hoz létre és működtet ezen megbetegedések nyilvántartása érdekében az Általános Szabályozás 5.14.1.1. a), c) és d) pontja, és az 5.14.1.2. b) pontja szerinti célból. A betegségregiszter kezeli az érintett személyek megbetegedéssel összefüggő egészségügyi és halálozással összefüggő adatait, TAJ számát, nemét, születési helyét és idejét, valamint a lakóhelyét és tartózkodási helyét.
Az Intézmény a regiszterben nyilvántartott elhunytak elhalálozásának tényét átvezeti, a regiszterben nem szereplő, de az adott megbetegedésben elhunytak adatait a regiszterbe

felveszi, majd az adatok egyeztetését követően a regiszterben nem nyilvántartott elhunytak adatait törli.

Az Intézmény adategyeztetést folytat a jogszabály szerinti adatszolgáltatókkal a megküldött adatok tekintetében.

Az Intézmény az azonos érintettre vonatkozó személyazonosító adatokhoz kapcsolódóan átadott egészségügyi és halálozási adatok tekintetében az átadást követően haladéktalanul kapcsolati kódot képez, amelyet minden átadott adat tekintetében azonos kódképzési módszer alapján hoz létre. A kapcsolati kód biztosítja az érintettre és az egyes ellátási eseményekre, betegutakra vonatkozó adatok személyazonosításra alkalmatlan összekapcsolását.

Az Intézmény a kapcsolati kód képzését követően az összekapcsolás céljából kapott személyazonosító adatokat haladéktalanul törli.

Ha a diagnózis változása kerül megállapításra a regiszterbe felvett érintett személynél, akkor az adatszolgáltató kezdeményezi a betegségregisztert vezető szervnél az érintett adatainak módosítását vagy törlését.

Az Intézmény a nyilvántartott adatokat a regiszterbe történő felvételtől számított, az 5.14.15. pontban foglalt ideig kezelheti.

5.14.12. Statisztikai célú adatkezelés

Az érintett egészségügyi adatai statisztikai célra - az alábbi bekezdésekben foglaltak kivételével - személyazonosításra alkalmatlan módon kezelhetők:

Az egészségügyi és személyazonosító adat statisztikai célú felhasználására - személyazonosításra alkalmas módon akkor, ha - az érintett írásban hozzájárult.

Élve születés és halálozás esetén a születés, illetve halálozás helye szerint illetékes anyakönyvvezető útján a Központi Statisztikai Hivatal részére az egészségügyi és személyazonosító adatokat át kell adni. A születéssel, illetve halálozással kapcsolatos események anyakönyvezése céljából teljesítendő bejelentési kötelezettsége során a betegellátó megismerheti és továbbíthatja élve születés esetén a gyermek szülei, halálozás esetén az életben lévő házastárs személyi azonosító adatait.

5.14.13. Tudományos kutatás céljából történő adatkezelés

Tudományos kutatás céljából a főigazgató - akadályoztatása esetén - az orvosigazgató, az adatvédelmi tisztviselővel/felelőssel való konzultáció eredményeként megadott 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 fenti bekezdés alapján a tárolt adatokba betekintett személyekről, a betekintés céljáról és időpontjáról a szervezeti egység vezetője/adatgazda az adatkezelési megbízotton keresztül nyilvántartást vezet. A nyilvántartás kötelező megőrzési ideje 10 év.

A kutatási kérelem megtagadását a főigazgató - akadályoztatása esetén - az orvosigazgató, az adatvédelmi tisztviselő véleménye alapján köteles írásban megindokolni. A kérelem megtagadása esetén a kérelmező bírósághoz fordulhat.

Archivált gyűjteményben tárolt, nem anonimizált genetikai minta, illetve adat új kutatáshoz történő felhasználásához az érintett 5.14.4. (1) pont szerinti beleegyező nyilatkozata szükséges. Amennyiben az érintett az adott kutatáshoz történő felhasználáshoz nem járul hozzá, a minta és adat az adott célra nem használható fel. Amennyiben a beleegyezés más ok miatt nem szerezhető be, a személyazonosító adattal együtt tárolt genetikai mintát, illetve adatot a további felhasználást megelőzően kóddal kell ellátni azzal, hogy a kódolt genetikai minta, illetve adat kizárólag az érintett hozzájárulása esetén tárolható ismét személyazonosító adatokkal együttesen. A genetikai minta, illetve adat kódolás nélkül, külön beleegyezés hiányában humángenetikai kutatási célra akkor is felhasználható, ha az érintett 5.14.4. (1) pont szerinti nyilatkozata ezt lehetővé tette.

A genetikai minta, illetve adat tárolása során biztosítani kell a genetikai minta, illetve adat védelmét megsemmisítéssel, megsemmisüléssel, megváltoztatással, károsodással, nyilvánosságra kerüléssel, továbbá illetéktelen személy hozzáférésével szemben. Genetikai mintát és adatot - amennyiben a Hgatv. másként nem rendelkezik - kódolt formában kell tárolni. A kódolt genetikai mintát, adatot, illetve a kódkulcsokat mind fizikailag, mind elektronikusan elkülönítve kell tárolni. A kódkulcshoz való hozzáférés joga - a Hgatv. keretei között - az Intézmény főigazgatóját, illetve az általa a biobank működésének felügyeletére kijelölt személyt illeti meg. A kódkulcs elkülönített tárolása során biztosítani kell, hogy az arra jogosult személyen kívül ahhoz más ne férhessen hozzá. A pszeudonimizált minta, illetve adat kódját a mintát szolgáltató személy kizárólagos rendelkezésére kell átadni.

Genetikai minta, illetve adat személyazonosító adatokkal együttesen csak az érintett hozzájárulása alapján tárolható. Személyazonosító adatokkal együttesen tárolt, valamint kódolt genetikai mintát, illetve adatot tartalmazó nyilvántartás személyazonosító adatokat tartalmazó nyilvántartással nem kapcsolható össze.

A biobankon belül a genetikai minták és genetikai adatok védelméért, a genetikai minták és adatok nyilvántartásáért, a nyilvántartás megőrzéséért az Intézmény főigazgatója, valamint az általa a biobank működésének felügyeletére kijelölt személy (a továbbiakban: felelős személy) a felelős. A felelős személy feladatkörében

a) érvényesíti a genetikai minták és adatok gyűjtésére, tárolására és feldolgozására, valamint az adatvédelmi követelményekre vonatkozó jogszabályi előírásokat és intézményi szabályokat;
b) rendszeresen értékeli az Intézményben működő biobank tevékenységének jogszerűségét és szakszerűségét, és az értékelés eredményéről tájékoztatja a főigazgatót;
c) a jogszabályoknak, illetve szakmai szabályoknak nem megfelelő működés esetén kezdeményezi a főigazgatónál a jogszerű, illetve szakszerű működés helyreállítása érdekében szükséges intézkedés megtételét, szükség szerint a tárolt genetikai mintákkal vagy anyagokkal végzett tevékenység felfüggesztését;

d) a biobank működésének ellenőrzését végző hatóságokat tájékoztatja a működéssel összefüggő, az ellenőrzéshez szükséges adatokról és éves beszámolót készít a biobank működéséről, melyet a tárgyévet követő február 15-ig – az Egészségügyi Tudományos Tanács Humán Reprodukciós Bizottság (ETT HRB) részére készülő jelentés elkészítéséhez - megküld az egészségügyi államigazgatási szervnek.

A biobankban tárolt minden genetikai mintát és adatot, valamint az ezekkel kapcsolatos minden eljárást, tevékenységet, a genetikai minta és adat továbbítását nyilván kell tartani az adatfelvételtől számított legalább 30 évig, kivéve, ha az érintett a genetikai adat kezeléséhez adott beleegyezését visszavonja. Ebben az esetben - az érintett tájékoztatását követően - valamennyi, a genetikai adatokra vonatkozó nyilvántartást meg kell semmisíteni. A kötelező nyilvántartási időt követően az adatok az Eüak. szerint kezelhetőek. A nyilvántartás elektronikus formában is történhet. A nyilvántartás tartalmazza a gyűjtött, vizsgált, tárolt, feldolgozott és elosztott, illetve egyéb módon felhasználásra került genetikai minták típusát, mennyiségét, eredetét és rendeltetési célját, valamint az ezekből kialakított genetikai adatokat.

A biobank további genetikai vizsgálat, illetve humángenetikai kutatás céljából nem anonimizált módon csak az érintett az 5.14.4. (1) pont szerinti nyilatkozata keretei között továbbíthat genetikai adatot. Minden további, az 5.14.4. (1) pont alpont szerinti beleegyező nyilatkozat kereteit meghaladó adattovábbításhoz az érintett beleegyezésének ismételt beszerzése szükséges.

5.14.14. Az egészségügyi és személyazonosító adatok nyilvántartása

Az érintettről felvett, az egészségügyi ellátás érdekében szükséges egészségügyi és személyazonosító adatot, valamint azok továbbítását nyilván kell tartani. Az adattovábbításról szóló feljegyzésnek tartalmaznia kell az adattovábbítás címzettjét, módját, időpontját, valamint a továbbított adatok körét. A nyilvántartás eszköze lehet minden olyan adattároló eszköz vagy módszer, amely biztosítja az adatok 5.14.20. alpont szerinti védelmét. A kezelést végző orvos az általa vagy az egyéb betegellátó által felvett – a gyógykezelés vagy a közegészségügy-járványügy szempontjából jelentős – egészségügyi adatokról, valamint a saját tevékenységéről és intézkedéseiről feljegyzést készít. A feljegyzés a nyilvántartás részét képezi.

Az Intézmény nyilvántartja azokat az érintetteket, akikről bebizonyosodott vagy valószínűsíthető, hogy fertőző betegségben szenvednek.

Ezzel összefüggésben nyilván kell tartani a megelőző gyógyszeres kezelésre, a szűrővizsgálatra, a járványügyi megfigyelésre, a járványügyi ellenőrzésre, a járványügyi zárlatra kötelezett személyeket, a védőoltásra kötelezett személyeket, továbbá azon személyeket, akik kábítószer-élvezők, gyógyszert kóros mértékben fogyasztók, illetve egyéb, hasonló jellegű függőséget okozó anyagot használnak.

Az Intézményre vonatkozóan kötelezően, az Intézményből továbbított adatokról (a beteg, a hozzátartozó, a beteg által erre felhatalmazott személy, továbbá kötelező adatközlés esetei) folyamatos sorszámozással és évszámmal ellátott nyilvántartási könyvben naprakész adattovábbítási nyilvántartást kell vezetni.

5.14.15. Az egészségügyi dokumentáció megőrzése

Az egészségügyi dokumentáció részét képező iratok megőrzéséért annak az osztálynak a vezetője felelős, ahol az adott vizsgálati eredmény keletkezett.

Az egészségügyi dokumentációt valamennyi részével együtt 30 évig, a zárójelentést 50 évig kell megőrizni. A képalkotó eljárással készült felvételt a keletkezéstől számított 10 évig, a felvételről készült leletet a készítéstől számított 30 évig kell megőrizni. Amennyiben az orvosi dokumentációnak tudományos jelentősége van, a kötelező nyilvántartási időt követően át kell adni az illetékes levéltár részére.

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 őrzi meg, azzal, hogy ha a működési nyilvántartásban nem szereplő, de valamely államban gyógyszer rendelésére jogosult személy által rendelt vényköteles gyógyszer kiadásának alapjául szolgáló külföldi vény visszaadásra kerül, a vény másolatát kell megőrizni és az expediálás tényét a vény eredeti példányán fel kell tüntetni. 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. A kötelező őrzési időt követően a papíralapú vényeket és a kiadási igazolásokat meg kell semmisíteni.

A gyógyszer, a gyógyszertárban forgalmazható gyógyászati segédeszköz - az EESZT-hez informatikai rendszere útján csatlakozott - kiszolgálója, az EESZT-ben rögzíti a papíralapon kiállított és felhasznált vény adatait. Az EESZT működtetője az egyes vényekre vonatkozó adatokat a vény visszavonásától, felhasználásától vagy felhasználási idejének lejártától számított 30 év elteltével törli.

A gyógyszer, gyógyászati segédeszköz kiszolgálója a megőrzési időn belül jogosult adatot igényelni az EESZT útján kiállított és általa kiszolgált vényekről. Az adatmegőrzés érdekében folyamatosan biztosítani kell, hogy az adathordozó az adott technikai feltételek mellett olvasható maradjon, vagy olvasható állapotba kerüljön.

5.14.16. Egészségügyi adatok, betegdokumentáció kérés, kiadás

Az egészségügyi dokumentáció másolatának kiadására vonatkozó megkeresést a főigazgató az orvosigazgató részére szignálja ki, aki indokolt esetben bevonja a Jogi és Igazgatási Osztályt. A magánszemélytől érkező megkeresés az **SZ-39 A01 Egészségügyi dokumentáció kikérő lap** kitöltésével történhet, mely az Intézmény honlapján elérhető. A kikérő lap, a 3. pontjában megnevezett jogosultak kivételével a kérelem érvényességéhez a beteg ellátásának ideje alatt a beteg által adott írásbeli felhatalmazás, az ellátás befejezését követően a beteg által adott teljes bizonyító erejű magánokiratba foglalt meghatalmazás szükséges, amelyet a KÉRELEMHEZ CSATOLNI SZÜKSÉGES!

Az **SZ-39 A01 Egészségügyi dokumentáció kikérő lap** kitöltésével nyilatkozik a kérelmező arról is, hogy a dokumentáció kiadásával járó költségek megfizetését vállalja. A megkeresés érkezhet postai úton, telefaxon, szkennelt formában elektronikus levélben, vagy személyes átadással.

Egészségügyi dokumentáció másolata az arra jogosult hatóság, bíróság, igazságügyi szakértő által, a felhasználás céljának pontos megjelölése esetén, annak keretében adható ki.

Amennyiben a dokumentáció kiadhatóságának feltételei fennállnak, az Orvosigazgatóság 5 napon belül továbbítja a megkeresést az illetékes betegellátó egység (ek) hez, vagy az Egészségügyi Dokumentációs Irodának, amely 10 napon belül köteles a kért dokumentáció másolatát az Orvosigazgatóság részére megküldeni, egyben köteles csatolni a megküldött dokumentáció teljeskörűségéről és az eredetivel mindenben megegyezőségéről szóló nyilatkozatot. Eredeti dokumentáció csak a rendőrség, bíróság vagy más hatóság írásos kérelme alapján, a konkrét ok megjelölésével, tételes irat átadás/átvételi jegyzőkönyv felvétele és az átadás/átvétel tényének egyidejű igazolása mellett adható ki. A jegyzőkönyvben rögzíteni szükséges, hogy az eredeti iratok Intézményhez történő visszajuttatásáról az átvevő köteles gondoskodni. Eredeti dokumentáció kiadása esetén a kiadásra illetékes betegellátó egység, vagy az Egészségügyi Dokumentációs Iroda köteles az eredeti dokumentációról másolatot készíteni és azt az eredeti dokumentáció visszaérkezéséig megőrizni.

Amennyiben a kiadhatóság feltételei nem állnak fenn, erről az orvosigazgató tájékoztatja az Igénylőt és hiánypótlásra szólítja fel.

Az illetékes szervezeti egység (ek) a szükséges dokumentáció másolatát az osztályvezető által aláírt teljességi nyilatkozattal együtt küldik meg az Orvosigazgatóságra. Az orvosigazgató az orvosi dokumentáció másolatát megküldi az Igénylő részére vagy szükség esetén továbbítja a Jogi és Igazgatási Osztály részére, további ügyintézés céljából.

Az orvosigazgató/Jogi és Igazgatási Osztály értesíti az Igénylőt a dokumentáció költségeire vonatkozó számla befizetéséről és a dokumentáció kiadásának feltételeiről. A befizetés személyesen az Intézmény pénztárában, vagy csekken történhet. Az orvosi dokumentációt abban az esetben adja ki az orvosigazgató/Jogi és Igazgatási Osztály az Igénylő részére, ha a megjelölt költséget megfizette. Az orvosi dokumentáció másolásának és kiadásának költségeit az **SZ-49 Térítési díj szabályzat** tartalmazza. A dokumentáció kiadása történhet személyes átvétel útján, vagy postai úton történő továbbítással, az Igénylő kérésének megfelelően. Amennyiben személyesen nem az Igénylő veszi át az iratokat, úgy szükséges csatolni az átvételre feljogosító meghatalmazást. Ennek hiányában a dokumentáció nem adható ki.

5.14.17. Dokumentáció és adattárolás

A betegellátó osztályon, ahol az érintett megbetegedésével, testi, lelki, értelmi állapotával, az ellátás körülményeire utaló, személyi illetve betegadatokat tárolnak, gondoskodni kell a szakszerű tárolásról. A dokumentumok tárolási és selejtezési rendjéről az **SZ-48 Iratkezelési szabályzat** rendelkezik.

5.14.18. Egészségügyi és személyazonosító adatok megsemmisítése

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

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

A megsemmisítés alóli kivételre a betegellátó osztály vagy részleg vezetője tesz javaslatot az orvosigazgatónak.

A megsemmisítendő dokumentációt a **Selejtezési Bizottság** jegyzőkönyvbe veszi, majd az elszállításra szolgáló zárható konténerbe helyezi. Olyan eljárással történhet a megsemmisítés, amely lehetetlenné teszi a dokumentumok rekonstruálását.

A selejtezéshez és megsemmisítésre való előkészítéshez selejtezési tervet kell készíteni. A selejtezés és előkészítés terv szerinti végrehajtását az Intézmény adatvédelmi tisztviselője/felelőse ellenőrzi. Az Intézmény (meghatározott tárgyú) dokumentumainak megsemmisítésre történő előkészítésének ellenőrzéséről jelentés készül. A jelentés része a megsemmisítési dokumentációnak.
Az Intézmény főigazgatója - az orvosigazgató javaslata alapján - dönt a kötelező nyilvántartási időt követően a nyilvántartott adatok további tárolásáról vagy megsemmisítéséről, az általános tudomány- és kultúrtörténeti okokra figyelemmel.

A megsemmisítésre vonatkozó engedélyt a jelentés alapján az Intézmény főigazgatója adja meg, mint az Intézményen belül az egészségügyi és személyazonosító adatok védelméért, a nyilvántartás megőrzéséért felelős személy.

A megsemmisítést dokumentálni kell, melynek a következőket kell tartalmaznia:

a) a megsemmisítés jogszabályi alapja;
b) a megsemmisítés helye;
c) a megsemmisítés ideje;
d) a megsemmisítés alá vont iratok terjedelme
e) papír alapú dokumentáció esetén;
f) digitális adathordozón tárolt dokumentáció esetén;
g) a megsemmisítés alá vont iratok évköre;
h) a megsemmisítési eljárás leírása
i) papír alapú dokumentáció esetén;
j) digitális adathordozón tárolt dokumentáció esetén;
k) a megsemmisítésben részt vevő adatfeldolgozó adatai;
l) a megsemmisítésnél jelen lévő személyek adatai;
m) a megsemmisítés végrehajtásáért felelős személy adatai;
n) a megsemmisítendő dokumentumok felsorolása külön jegyzékben
o) papír alapú dokumentáció esetén;
p) digitális adathordozón tárolt dokumentáció esetén;
q) a dokumentum készítésének helye, ideje, készítőjének és jóváhagyójának adatai.

A dokumentáció előkészítésénél, értékelésénél a területileg illetékes közlevéltárat – szükség esetén – szaktanácsadásra fel lehet kérni. A megsemmisítésről szóló dokumentációt min. 20 évig kell megőrizni.

5.14.19. Adatfelvétel és módosítása

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.

Az adatfelvétel során az egészségügyi dokumentációban rögzíteni kell az adatfelvétel időpontját és az adatfelvevő személyét.

Az egészségügyi dokumentációban szereplő hibás egészségügyi adatot - az adatfelvételt követően - úgy kell **kijavítani** vagy **törölni**, hogy az eredetileg felvett adat megállapítható legyen. A módosítást kézjeggyel el kell látni.

A nyilvántartott adatokról, az egészségügyi dokumentációról a szervezeti egység vezető/adatgazdahiteles másolatot készít, ha ezt az adatbiztonság vagy a tárolt adatok fizikai védelme, illetve azt törvényben előírt adatközlési kötelezettség szükségessé teszi.

Az egészségügyi és személyes adatokat ért sérülés vagy megsemmisülés esetén a rendelkezésre álló adatforrásból meg kell kísérelni - a lehetséges mértékig - a károsodott adatok pótlását. Sérült adat pótlására annak a szervezeti egységnek a vezetője felelős, ahol a sérülés bekövetkezett. A pótolt adatokon a pótlás tényét fel kell tüntetni. A pótlásról jegyzőkönyvet kell felvenni.

5.14.20. Adatvédelem az elektronikus adatkezelés során

Az informatikai rendszerben történő adatkezelést/tárolás, adatmentés, adathozzáférés, adatmódosítás, adattörlés, adatbiztonság szabályait az **SZ-66 Informatikai biztonsági szabályzat,** valamint az **Informatikai felhasználói szabályzat** (**SZ-41**) tartalmazza.

5.15. AZ ÉRINTETT JOGAI

5.15.1. A hozzáféréshez való jog

Az érintett jogosult arra, hogy az Adatkezelőtől tájékoztatást kérjen arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy megismerje azt, hogy

a) milyen személyes adatait;
b) milyen jogalapon;
c) milyen adatkezelési cél miatt;
d) mennyi ideig kezelik; továbbá, hogy
e) az Adatkezelő kinek, mikor, milyen jogszabály alapján, mely személyes adataihoz biztosított hozzáférést vagy kinek továbbította a személyes adatait;
f) az Adatkezelő alkalmaz-e automatizált döntéshozatalt, valamint annak logikáját, ideértve a profilalkotást is.

Az Adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett erre irányuló kérésére első alkalommal díjmentesen bocsátja a rendelkezésére, ezt követően adminisztratív költségeken alapuló, ésszerű mértékű díjat számíthat fel.

Az adatbiztonsági követelmények teljesülése és az érintett jogainak védelme érdekében az Adatkezelő köteles meggyőződni a hozzáférési jogával élni kívánó személy személyazonosságának egyezéséről, ennek érdekében a tájékoztatás, az adatokba történő betekintés, illetve azokról másolat kiadása is az érintett személyének azonosításához kötött.

5.15.2. A helyesbítéshez való jog

Az érintett jogosult arra, hogy – az erre vonatkozó hitelt érdemlő bizonyítékok bemutatása esetén – kérje, hogy az Adatkezelő módosítsa valamely személyes adatát. Az Adatkezelő a kérelmet legfeljebb egy hónapon belül teljesíti, és erről az érintettet az általa megadott elérhetőségre küldött levélben értesíti.

5.15.3. A törléshez való jog

Az érintett jogosult arra, hogy írásban kérje az Adatkezelőtől a hozzájárulása alapján kezelt személyazonosító adatainak a törlését. Ebben az esetben a személyazonosító adatoktól megfosztott, de kapcsolati kóddal kiegészített egészségügyi és genetikai adatokat – a 4. pontban (ld: deperszonalizálás (anonimizálás)) írtak szerint, személyazonosításra immár alkalmatlanul – az Adatkezelő jogosult a továbbiakban is kezelni.
A személyazonosító adatainak törlésére vonatkozó kérelmet az Adatkezelő legfeljebb egy hónapon belül teljesíti, és erről az érintettet az általa megadott elérhetőségre küldött levélben értesíti.

5.15.4. A zároláshoz (adatkezelés korlátozásához) való jog

Az érintett jogosult arra, hogy írásban, indoklás megadásával kérje az Adatkezelőtől, hogy személyazonosító adatait zárolja (az adatkezelés korlátozott jellegének egyértelmű jelölésével és az egyéb adatoktól elkülönített kezelés biztosításával). A zárolás addig tart, amíg az érintett által megjelölt indok szükségessé teszi az adatok tárolását.

5.15.5. A tiltakozáshoz való jog

Az érintett jogosult arra, hogy írásban saját helyzetével kapcsolatos okokból bármikor tiltakozzon az adatkezelés ellen, ha álláspontja szerint az Adatkezelő a személyes adatát a jelen adatkezelési tájékoztatóban megjelölt céllal összefüggésben nem megfelelően kezelné.

5.15.6. Az adathordozhatósághoz való jog

Az érintett jogosult arra, hogy írásban az Adatkezelő által tárolt adatait tagolt, széles körben használt, géppel olvasható formátumban megkapja vagy azokat más adatkezelőhöz továbbítsa, amennyiben ez technikailag megvalósítható.

5.15.7. Hatósági és bírósági jogérvényesítéshez való jog

Az érintett jogosult arra, hogy jogainak megsértése esetén a Nemzeti Adatvédelmi és Információbiztonság Hatósághoz (1364 Budapest, Falk Miksa utca 9-11, Pf. 125., telefon: +36 (1) 391-1400, e-mail: ugyfelszolgalat@naih.hu), illetve a lakó- vagy tartózkodási helye szerint illetékes törvényszékhez forduljon, utóbbi esetben követelje az adatai jogellenes kezelésével vagy az adatbiztonság megszegésével neki okozott kár megtérítését, személyiségi jogsérelem esetén sérelemdíj megfizetését.

5.16. A SZABÁLYZATOKHOZ KAPCSOLÓDÓ JOGSZABÁLYOK, BELSŐ SZABÁLYZATOK

GDPR	Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről
Info tv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [az Infotv-nek a GDPR hatálya alá eső adatkezelésekre alkalmazandó szabályai – lsd. Infotv. 2. § (2) és (4) bekezdése]
Ibtv.	az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény és végrehajtására kiadott jogszabályok
Eüak.	az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről, és a végrehajtására kiadott jogszabályok 1997. évi XLVII. törvény
Eütv.	az egészségügyről szóló 1997. évi CLIV. törvény, és a végrehajtására kiadott jogszabályok
Ebtv.	kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény, és a végrehajtására kiadott jogszabályok
Eszjtv.	az egészségügyi szolgálati jogviszonyról szóló 2020. évi C. törvény
Mt.	a Munka Törvénykönyvéről szóló 2012. évi I. törvény
Rtv.	a rendőrségről szóló 1994. évi XXXIV. törvény
Nsztv.	a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény
Hgatv.	a humángenetikai adatok védelméről, a humángenetikai vizsgálatok és kutatások, valamint a biobankok működésének szabályairól szóló 2008. évi XXI. törvény
Hvt.	a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény
SZ-01	a Dél-pesti Centrumkórház – Országos Hematológiai és Infektológiai Intézet Szervezeti és működési szabályzata
SZ-13	a Dél-pesti Centrumkórház – Országos Hematológiai és Infektológiai Intézet Panaszkivizsgálási szabályzata
SZ-14	a Dél-pesti Centrumkórház – Országos Hematológiai és Infektológiai Intézet Munkavédelmi szabályzata
SZ-30	a Dél-pesti Centrumkórház – Országos Hematológiai és Infektológiai Intézet Rendészeti és vagyonvédelmi szabályzata
SZ-41	Informatikai felhasználói szabályzat
SZ-48	Dél-pesti Centrumkórház – Országos Hematológiai és Infektológiai Intézet Iratkezelési szabályzata
SZ-53	a Dél-pesti Centrumkórház – Országos Hematológiai és Infektológiai Intézet A közérdekű adatok megismerésére irányuló kérelmek intézésének, továbbá a kötelezően közzéteendő adatok nyilvánosságra hozatalának rendjéről szóló szabályzata
SZ-66	a Dél-pesti Centrumkórház – Országos Hematológiai és Infektológiai Intézet Informatikai biztonsági szabályzata
Sz-83	a Dél-pesti Centrumkórház – Országos Hematológiai és Infektológiai Intézet Incidenskezelési Szabályzata

5.17. ZÁRÓ RENDELKEZÉSEK

Jelen Adatvédelmi és adatkezelési szabályzat az aláírás napján lép hatályba.

A hatályba lépés előtt az Intézmény az Adatvédelmi és adatkezelési szabályzat végrehajtása iránt az alábbiak szerint intézkedik:

a) Az Informatikai igazgató megküldi az oktatási anyagot az adatkezelésért felelős szervezeti egységek vezetőinek;

b) az adatkezelésért felelős szervezeti egység vezetői felelnek azért, hogy az oktatási anyagot az irányításuk alá tartozó szervezeti egység munkavállalói megismerjék és az ahhoz tartozó tesztet kitöltsék;

c) Az Információbiztonsági és Adatvédelmi Osztály figyelemmel követi az oktatási anyag kitöltésének eredményét;

d) Az adatkezelésért felelős szervezeti egységek vezetői intézkednek az **SZ-39 M01**-es nyilatkozat irányításuk alá tartozó szervezeti egységnél foglalkoztatott dolgozók által történő tudomásul vétele és aláírása, valamint a Bérszámfejtési, Munkaügyi és Humánpolitikai Osztálynak való megküldése iránt;

e) Az új belépő dolgozók vonatkozásában a Bérszámfejtési, Munkaügyi és Humánpolitikai Osztály intézkedik **SZ-39 M01**-es nyilatkozat tudomásul vétele és aláírása iránt.

6. HIVATKOZÁSOK

- 1994. évi XXXIV. törvény a rendőrségről
- 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról
- 1996. évi XX. törvény a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról
- 1997 évi XLVII törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről
- 1997. évi LXXXIII. törvény a kötelező egészségbiztosítás ellátásairól
- 1997. évi CLIV. törvény az egészségügyről
- 2008. évi XXI. törvény a humángenetikai adatok védelméről, a humángenetikai vizsgálatok és kutatások, valamint a biobankok működésének szabályairól
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről
- 2012. évi I. törvény Munka Törvénykönyvéről
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 2020. évi C. törvény az egészségügyi szolgálati jogviszonyról
- Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete 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 (általános adatvédelmi rendelet)
- SZ-01 Szervezeti és működési szabályzat
- SZ-13 Panaszkivizsgálási szabályzat

- SZ-14 Munkavédelmi szabályzat
- SZ-30 Rendészeti és vagyonvédelmi szabályzat
- SZ-41 Informatikai felhasználói szabályzat
- SZ-48 Iratkezelési szabályzat
- SZ-49 Térítési díj szabályzat
- SZ-53 Belső ellenőrzési szabályzat
- SZ-66 Informatikai biztonsági szabályzat
- SZ-79 Kockázatkezelés eljárásrendje
- SZ-83 Incidenskezelési szabályzat

7. MELLÉKLETEK, ADATLAPOK JEGYZÉKE

- SZ-39 M01 Adatvédelmi, információbiztonsági, titokvédelmi követelmények tudomásul vételéről szóló nyilatkozatok
- SZ-39 M02 Tájékoztató a munkavégzésre irányuló jogviszonnyal kapcsolatos személyes adatok kezeléséről
- SZ-39 M03 Adatkezelés bevezetésével kapcsolatos döntés előkészítését támogató minta
- SZ-39 M04 Adatvédelmi incidens bejelentő lap
- SZ-39 A01 Egészségügyi dokumentáció kikérő lap
- SZ-39 A02 Kezelőorvos betegéletút lekérdezési lehetősége tiltakozás
- SZ-39 A03 Kezelőorvos betegéletút lekérdezési lehetősége tiltakozás feloldása