



Észak-budai
Szent János
Centrumkórház

Kód: 40.
Változatszám: 6
Mellékletek száma: 2

Iktatószám: SZJC-SZAB/20-1/2024

40. számú ADATVÉDELMI SZABÁLYZAT

Jóváhagyta:


Dr. Balovich Zsolt
intézményvezető-főigazgató

Budapest, 2024 SZEP 10

A szabályzatot készítette:


Dr. Török Árpád
igazgatási, jogi és humánpolitikai
főigazgató-helyettes

Érvénybelépés időpontja: 2024 SZEP 11

A szabályzat az Észak-budai Szent János Centrumkórház, szellemi tulajdona, szerzői jogi védelmet élvez.
Továbbadása, sokszorosítása írásos engedélyhez kötött.





Tartalomjegyzék

I. A szabályzat célja és hatálya	4
II. A Szabályzat alkalmazásában használt fogalmak.....	5
III. Az adatvédelem alapelvei.....	8
IV. Az adatvédelmi tevékenység szervezete és irányítása az Intézménynél	9
1. A főigazgató feladatai	9
2. Az adatvédelmi tisztviselő feladatai.....	9
3. A szervezeti egységek vezetőinek feladatai	13
4. Az adatvédelemért felelős főigazgató-helyettes feladatai	13
5. A jogi iroda feladatai.....	14
6. A kommunikációért felelős személyfeladatai	15
7. Az adatvédelmi felelősök feladatai	15
V. Adatkezelők, adatfeldolgozás és közös adatkezelés.....	16
VI. Az adatkezelés bevezetésével, módosításával és megszüntetésével kapcsolatos feladatok.....	17
1. Adatkezelés bevezetésével kapcsolatos feladatok.....	17
2. Az érdekmérlegelési teszt elvégzésének módszertana	20
3. Az adatvédelmi felelős feladatai az adatkezelés során.....	22
4. Adatkezelés megszüntetésével kapcsolatos feladatok.....	23
5. Az adatfeldolgozó igénybevételének feltételei, az adatfeldolgozói megállapodás	24
6. A közös adatkezelés feltételei, a közös adatkezelői megállapodás.....	26
VII. Az adatkezelési nyilvántartás.....	28
VIII. Az érintettektől származó kérelmek, panaszok megválaszolásának rendje.....	29
1. Az adatvédelmi bejelentések típusai	29
2. Az adatvédelmi beadványok elintézése.....	30
IX. Az érintettek jogai, azok érvényesítése	31
1. Tájékoztatási kötelezettség.....	31
2. Az érintett tájékoztatáshoz való joga – hozzáféréshez való jog	32
3. A helyesbítéshez való jog.....	33
4. Az adatkezelés korlátozásához való jog	33
5. Adathordozhatósághoz való jog.....	33
6. A törléshez való jog	34
7. A tiltakozáshoz való jog	35
8. Jogorvoslathoz való jog	35
X. Az adatkezelés biztonsága	36



1. Adatkezelési nyilvántartás, kockázatelemzés, adatbiztonság	36
2. Adatvédelmi hatásvizsgálat és előzetes konzultáció.....	37
3. Adatvédelmi incidens, és kezelése	40
4. Belső adatvédelmi ellenőrzési eljárás	44
XI. Adattovábbítás szabályai.....	45
XII. Az adatvédelmi kockázatelemzés szabályai.....	46
XIII. Betegek adatainak kezelése, nyilvántartása	49
1. Az egészségügyi adatok kezelésének és védelmének alapvető intézményi szabályai...	50
2. Adatkezelés célja.....	50
3. Titoktartási kötelezettség.....	50
4. Adatkezelés a betegfelvétel során.....	53
5. Adatkezelés a betegellátás során.....	53
6. Egészségügyi dokumentáció vezetése	56
7. Betegadatok statisztikai célú kezelése	58
8. Adatkezelés közegészségügyi, járványügyi célból	58
9. Tudományos kutatás céljából történő adatkezelés	59
10. A társadalombiztosítási igazgatási szervek adatkezelése.....	60
11. Adattovábbítás az egészségügyi ellátó hálózaton kívülre.....	60
XIV. A gyermekek adatainak kezelésére vonatkozó különös szabályok.....	62
XV. A cselekvőképességében korlátozott nagykorú személyek adatainak kezelésére vonatkozó különös szabályok	62
XVI. A cselekvőképtelen állapotban lévő személyek személyes adatainak kezelésére vonatkozó különös szabályok	63
XVII. A látássérültek személyes adatainak kezelésére vonatkozó különös szabályok.....	63
XVIII. Dolgozói adatok kezelése, nyilvántartása.....	64
1. Pályázók adatainak kezelése	64
2. Dolgozók adatainak kezelése.....	64
XIX. Szerződő partnerek adatainak kezelése, nyilvántartása	65
XX. A papír alapon kezelt személyes adatok	65
XXI. Elektronikusan kezelt személyes adatok	66
XXII. Elektronikus térfelügyeleti rendszerre vonatkozó alapvető szabályok.....	66
XXIII. Záró rendelkezések	67
1.számú melléklet: Incidens nyilvántartás sablonja	68
2. számú melléklet: Adatvédelmi incidens bejelentőlap	69

m



ÁLTALÁNOS RÉSZ

I. A szabályzat célja és hatálya

Az Észak-budai Szent János Centrumkórház (a továbbiakban: SZJC), valamint az irányítása alá tartozó Budapesti Szent Margit Kórház (a továbbiakban: SZMK) és Visegrádi Szent Kozma és Damján Rehabilitációs Szakkórház és Gyógyfürdő (a továbbiakban: SZKD) (SZJC, SZMK és SZKD a továbbiakban külön-külön mint Intézmény vagy együttesen Intézmények) 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, az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) (a továbbiakban: GDPR), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.), valamint az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (Eüak.) alapján az Intézmények adatvédelmének, adatbiztonságának és adatkezelésének egységes elvek mentén történő szabályozása érdekében az alábbi szabályzatot alkotja.

A szabályzat célja, hogy meghatározza az Intézmény és a szabályzat hatálya alá tartozó egyéb szervezetek tevékenysége és működése során általa kezelt személyes adatok védelmére irányuló intézkedések és eljárások jogszerű rendjét, valamint biztosítsa az adatvédelem alapjogi elveinek, a kapcsolódó irányelvek, az információs önrendelkezési jognak, a személyes adatok védelméhez való jognak és az adatbiztonság követelményeinek érvényesülését, továbbá az adatvédelmi tevékenység ellátásában résztvevő szervezeti egységek feladatait és együttműködésük kereteit, illetve az Intézmény által kezelt adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes és különleges adatok kezelése során irányadó adatvédelmi és adatbiztonsági szabályokat. Az Intézmény a fentiek szerint meghatározott jogszabályok, valamint az Intézményre irányadó egyéb jogszabályok rendelkezései szerint köteles kezelni az érintettek személyes adatait.

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

A Szabályzat további célja, hogy meghatározza az Intézmény szervezeti egységeinél vezetett, személyes adatokat tartalmazó nyilvántartások vezetésének és működtetésének jogszerű rendjét, valamint biztosítsa a személyes adatok védelmi elveinek és az adatbiztonság követelményeinek érvényesülését az adatvédelemmel összefüggő feladatok, felelősségek és hatáskörök meghatározásával.

Az Intézmény a személyes adatok kezelésével járó tevékenysége során érvényre juttatja a GDPR 5. cikkében meghatározott alapelveket.

A szabályzat személyi hatálya kiterjed az Intézmény valamennyi szervezeti egységére, és az Intézmény nevében bármely jogviszony alapján tevékenységet végző természetes személyre, aki tevékenysége során személyes adatok kezelését végzi.



A szabályzat személyi hatálya kiterjed továbbá minden, az Intézmény szolgáltatásait vagy szervezeti egységeit, infrastruktúráját igénybe vevő, vagy az Intézménnyel akár jogviszony létesítése céljából, akár egyéb célból ténylegesen kapcsolatba került, vagy kerülő természetes személyre.

A szabályzat személyi hatálya kiterjed továbbá azon személyekre is, akik az Intézménnyel nem állnak a fentiekben meghatározott jogviszonyban, illetve kapcsolatban, azonban személyes adataikat jogszabályi előírás folytán az Intézmény kezeli.

A szabályzat tárgyi hatálya kiterjed az Intézmény által bármely célból kezelt személyes adatra és a személyes adatoknak az Intézménynél megtalálható valamennyi nyilvántartására, függetlenül azok megjelenési formájától.

A szabályzat területi hatálya kiterjed az Intézmény székhelyén és telephelyein található valamennyi betegellátó osztályra, részlegre és irodára, továbbá mindazon helyiségekre, amelyekben a szabályzat tárgyi hatálya alá tartozó elektronikus adatokat vagy dokumentumokat, információkat hoznak létre, tárolnak, használnak, továbbítanak vagy bármely más módon kezelnek.

A szabályzat hatálya nem terjed ki az informatikai eszközökkel összefüggő technikai adatvédelemre, amelyről az Informatikai biztonsági szabályzat rendelkezik.

II. A Szabályzat alkalmazásában használt fogalmak

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 ez által a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a minimálisra csökkentik.

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

Adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet, vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása, vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése, vagy az adatokba való betekintés.

Adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, illetve jogi személyiséggel nem rendelkező bármely szervezet, aki, vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.

Adatvédelmi felelős: olyan az Intézménnyel munkaviszonyban, vagy munkavégzésre irányuló egyéb jogviszonyban álló, felsőfokú képesítéssel rendelkező személy, aki az



érintett szervezeti egység tekintetében a jelen szabályzatban foglaltaknak való megfelelést hivatott biztosítani.

Adatvédelmi felügyeleti hatóság: a Nemzeti Adatvédelmi és Információszabadság Hatóság.

Adatvédelmi hatásvizsgálat: amennyiben valamely tervezett adatkezelés – figyelemmel annak jellegére, hatókörére, körülményeire és céljaira, ideértve különösen az új technológiák alkalmazásának esetét – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Intézmény hatásvizsgálatot végez, amelynek célja annak megállapítása, hogy a tervezett adatkezelés a személyes adatok védelmét hogyan érinti. Az adatvédelmi hatásvizsgálat egy olyan eljárás, amelynek során az adatkezelő a tervezett adatkezelési műveletet vagy műveleteket áttekinti, megvizsgálja az adatkezelés érintettekre gyakorolt esetleges hatását, felméri annak kockázatait, a kockázatok kezelésének módját, és mindezt megfelelően dokumentálja.

Adatvédelmi incidens: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan közlés vagy azokhoz való hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, elvesztés, valamint a véletlen megsemmisülés és sérülés.

Adatvédelmi tisztviselő: a személyes adatok védelméért, az adatkezelés jogszerűségéért felelős személy, aki ellátja a GDPR-ban, más jogszabályokban és a jelen szabályzatban meghatározott feladatokat.

Álnevesítés: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.

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

Címzett: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel, vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnak; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak.

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.

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.



EGT-állam: az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez.

Érdelmérlegelési teszt: jogos érdeken alapuló adatkezelés folytatása vagy 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.

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 kiszolgáltatását, a mentést és betegszállítást, valamint a szülészeti ellátást is.

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

Harmadik ország: minden olyan állam, amely nem EGT-állam.

Kezelést végző orvos, kezelőorvos: a beteg adott betegségével, illetve egészségi állapotával kapcsolatos vizsgálati és terápiás tervet meghatározó, továbbá ezek keretében beavatkozásokat végző orvos, illetve orvosok, akik a beteg gyógykezeléséért felelősséggel tartozna.

Közei hozzátartozó: a házastárs, az egyeneságbeli rokon, az örökbefogadott, a mostoha- és a nevelt gyermek, az örökbefogadó-, a mostoha- és a nevelőszülő és a testvér. Az Eüak. hatálya alá tartozó adatkezelések esetében közei hozzátartozó továbbá az élettárs.

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.

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.

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.



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

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

III. Az adatvédelem alapelvei

A jogszerűség, tisztességes eljárás és átláthatóság elve szerint a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.

A célhoz kötöttség elve alapján az adatgyűjtés során ügyelni kell arra, hogy azok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat nem lehet ezekkel a célokkal össze nem egyeztethető módon kezelni. Nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.

Az adattakarékosság elve értelmében a kezelt adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek és a szükséges mértékre kell korlátozódniuk.

A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük és az adatkezelőnek minden észszerű intézkedést meg kell tennie annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatok haladéktalanul törlésre vagy helyesbítésre kerüljenek.

A korlátozott tárolhatóság elvére figyelemmel a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. A személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a jogszabályi előírásoknak megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.

Az integritás és bizalmas jelleg elvét biztosítandó, a személyes adatok kezelését olyan 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.

Az Intézmény, mint adatkezelő felelős az alapelveknek való megfelelésért (GDPR 5. cikk (1) bekezdés), továbbá az elszámoltathatóság elvének megfelelően képesnek kell lennie e megfelelés igazolására is (GDPR 5. cikk (2) bekezdés). A megfelelés igazolása különösen az adatkezeléshez kapcsolódó döntéseket megalapozó körülmények



és a döntések (pl. az adatkezelés feltételeit meghatározó döntéselőkészítő iratok), az érintetteknek szóló adatkezelési tájékoztatók, az érintettektől 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.

IV. Az adatvédelmi tevékenység szervezete és irányítása az Intézménynél

Az adatvédelmi tevékenység irányításában és ellátásában az Intézmény szervezeti egységei – az Intézmény Szervezeti és Működési Szabályzatában (a továbbiakban: SzMSz) meghatározott feladatkörükön belül – az alábbiak szerint vesznek részt.

1. A főigazgató feladatai

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

- a) gondoskodik az adatvédelmi tevékenység irányításában és ellátásában résztvevő személyek és szervezeti egységek kijelöléséről, feladataik, az adatvédelmi tárgyú ügyekkel kapcsolatos döntési jogkörök meghatározásáról, az egyes adatkezelési döntési szintek kialakításáról,
- b) **biztosítja az adatvédelmi tevékenység irányításához és ellátásához, valamint az érintett jogai gyakorlásához szükséges személyi és tárgyi feltételeket,**
- c) felelős az adat- és titokvédelmi, valamint biztonsági és információbiztonsági szabályzatok kiadásáért és betartatásáért,
- d) gondoskodik arról, hogy az adatvédelmi tevékenység során esetleg előforduló, feltárt hiányosságok megszüntetéséről, szükség szerint a felelősségre vonásról,
- e) kinevezi az Intézmény adatvédelmi tisztviselőjét, és az adatvédelmi tisztviselő nevét és elérhetőségét bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak.

A főigazgató az adatvédelemmel kapcsolatos egyes feladat- és hatásköröket – jogszabály eltérő rendelkezése hiányában – delegálhatja.

2. Az adatvédelmi tisztviselő feladatai

Az adatvédelmi tisztviselőt az Intézmény főigazgatója bízza meg. Az adatvédelmi tisztviselő közvetlenül és kizárólag az Intézmény főigazgatójának tartozik felelősséggel. Az adatvédelmi tisztviselő független, függetlensége biztosítása érdekében a szakmai feladatai ellátásával kapcsolatban utasításokat senkitől sem fogadhat el. Az Intézmény az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja.

Az adatvédelmi tisztviselő az Intézmény alkalmazottja lehet, vagy megbízási szerződés keretében láthatja el a feladatait. A kinevezés során a szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a GDPR 39.



cikkében említett feladatok ellátására való alkalmasságra szükséges figyelemmel lenni. Az adatvédelmi tisztviselőnek ismernie kell az Intézmény működését, feladatait, illetve munkafolyamatait.

Adatvédelmi tisztviselőként jogi, informatikai főiskolai (BSc) vagy egyetemi (MSc) felsőfokú végzettséggel vagy az Intézmény tevékenysége körében adatvédelmi területen legalább 10 éves szakmai gyakorlattal rendelkező személy bízható meg. Adatvédelmi tisztviselőként az jelölhető ki, aki a személyes adatok védelmére vonatkozó jogi előírások és jogalkalmazási gyakorlat megfelelő szintű ismeretével rendelkezik és alkalmas a jogszabályokban meghatározott feladatok ellátására. Az adatvédelmi tisztviselőnek rendelkeznie kell továbbá az alapvető adatvédelmi és IT folyamatok, valamint az európai uniós, illetve a hazai adatvédelemmel kapcsolatos főbb szabályozók, hatósági és bírósági határozatok, iránymutatások ismeretével. Az Intézmények közös adatvédelmi tisztviselőt jelölhetnek ki, az Intézmények szervezeti felépítésének és méretének figyelembevételével.

Az Intézményben nem lehet adatvédelmi tisztviselő az a természetes személy, aki az Intézményben az adatkezelési tevékenység céljainak, kereteinek, eszközeinek meghatározásáról dönt, különösen a főigazgató, az adatkezelésért felelős főigazgató-helyettes vagy szervezeti egység vezető, a belső ellenőr, illetve az informatikai biztonsági felelős.

Az adatvédelmi tisztviselő az adatvédelmi tisztviselői feladatokon kívül a főigazgató döntése alapján más munkakörhöz kötődő feladatokat is elláthat, amennyiben azok nem eredményeznek összeférhetetlenséget. Az Intézmény az adatvédelmi tisztviselő kinevezése mellett adatvédelmi tanácsadási feladattal egyéb jogi, információbiztonsági vagy más különleges szakértelemmel bíró szakértőt is megbízhat.

Az Intézmény honlapján közzéteszi az adatvédelmi tisztviselő nevét és elérhetőségét, és azokat a felügyeleti hatóság részére bejelenti.

Az adatvédelmi tisztviselő ellátja a GDPR által nevesített feladatait, így különösen:

- a) tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végzők részére a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban,
- b) ellenőrzi az GDPR-nak, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek való megfelelést, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is,
- c) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését és közreműködik abban a személyes adatot is kezelő új informatikai rendszer belső fejlesztéssel történő bevezetése, valamint új folyamatok vezetése során,
- d) az adatvédelmi incidenskezeléssel kapcsolatban ellátja a jelen szabályzat szerinti feladatokat,
- e) kapcsolatot tart – és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – együttműködik az adatvédelmi felügyeleti



hatósággal, valamint biztosítja az ágazati adatkezeléshez szükséges információkat a fenntartó ezzel foglalkozó részlegének,

- f) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele,
- g) részt vesz az adatvédelmi tárgyú szabályzatok felülvizsgálatában,
- h) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában,
- i) kivizsgálja a hozzá érkezett bejelentéseket, panaszokat, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az illetékes adatkezelőt vagy az adatfeldolgozót,
- j) gondoskodik az adatvédelmi ismeretek Intézmény keretében történő oktatásáról,
- k) ellátott feladatairól összefoglaló jelentést készít a főigazgatónak.

Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

Az Intézmény az adatvédelmi tisztviselő közreműködésével, az adatvédelmi felelősök által szolgáltatott adatok alapján nyilvántartást vezet:

- a) Az Intézménynél végzett adatkezelési tevékenységekről. A nyilvántartás tartalmazza
 - az adatkezelő és az érintett szervezeti egység nevét és elérhetőségét, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a nevét és elérhetőségét,
 - az adatkezelés céljait, jogalapját,
 - az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetését,
 - olyan címzettek kategóriáit, akikkel a személyes adatokat közlik vagy közölni fogják,
 - adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információkat (beleértve a megfelelő garanciák leírását),
 - ha lehetséges, a különböző adatkategóriák törlésére előírányzott határidőket,
 - ha lehetséges, az adatvédelmi biztonsági technikai és szervezési intézkedések általános leírását, valamint az alkalmazott adatfeldolgozási technológia megnevezését.

A nyilvántartást írásban vagy elektronikus formában kell megőrizni, és folyamatosan naprakészen kell tartani.



A nyilvántartást

- az SZJC esetén az Igazgatói Titkárság,
- az SZMK esetén a Főigazgató, a főigazgató SZMSZ szerinti helyettese vagy a főigazgató által írásban kijelölt dolgozó,
- az SZKD esetén a Főigazgató, a főigazgató SZMSZ szerinti helyettese vagy a főigazgató által írásban kijelölt dolgozó

köteles megőrizni.

Az adatkezelési nyilvántartásba bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelésért felelős szervezeti egység adatvédelmi felelőse haladéktalanul, de legfeljebb nyolc napon belül köteles bejelenteni az adatvédelmi tisztviselőnek, aki ennek megfelelően jóváhagyja az adatkezelési nyilvántartás módosítását.

b) Az Intézménynél észlelt adatvédelmi incidensekről.

A nyilvántartás az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat a jelen szabályzat 1. számú mellékletében meghatározottak szerint.

Az adatkezelési nyilvántartással összefüggésben az adatvédelmi tisztviselő:

- jelzi az adatkezelésért felelős szervezeti egység vezetőjének a rendelkezésre álló adatok alapján megállapíthatóan hiányos, hibás vagy valószínűleg megváltozott adatokat, információkat és ellenőrzi azok adatkezelési nyilvántartásban történő bejegyzését, átvezetését;
- a jogi irodával együttműködve figyelemmel kíséri az adatkezelést érintő jogszabályok változását és a szükséges módosításokra felhívja az Intézményt, illetve az adatvédelmi felelősök figyelmét;
- az adatvédelmi felügyeleti hatóság megkeresésére adatot szolgáltat az adatkezelési nyilvántartásból.

Az érintettek a személyes adataik kezeléséhez és a GDPR szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak.

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

Az adatvédelmi tisztviselő feladatai ellátása során – és tisztsége megszűnését követően is – a tudomására jutott, közérdekű vagy közérdekből nyilvános adatnak nem minősülő információk vonatkozásában az uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.

Az Intézmény elősegíti az adatvédelmi tisztviselő megfelelő szakmai feladatellátását, ennek érdekében biztosítja az adatvédelmi tisztviselő feladatai végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáférést, valamint a szakértői szintű ismereteinek fenntartásaihoz szükséges forrást, feladatai ellátásához

elegendő időt biztosít, valamint az informatikai és a biztonsági szakterület együttműködése révén gondoskodik az adatvédelmi tisztviselő bevonásáról 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.

Az adatvédelmi felügyeleti hatósággal történő együttműködés során az adatvédelmi tisztviselő –az ügy természetéből adódóan szükség szerint bevonandó más szakterület munkatársainak közreműködésével – tartja a kapcsolatot.

Az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódhat, feladatai ellátása során a személyes adatokhoz és az adatkezelési műveletekhez hozzáférhet. Az adatvédelmi tisztviselő biztosítja továbbá az adatvédelmi nyilvántartásba való betekintést az Intézmény érintett szakterületei részére.

Az adatvédelmi tisztviselő jogosult ellenőrizni az Intézmény valamennyi adatkezelési, adatfeldolgozási tevékenységét és a főigazgató, az illetékes szakági igazgató és az érintett szervezeti egység adatvédelmi felelősének tájékoztatása mellett felhívni a mulasztó szervezeti egység vezetőjét az ellenőrzés során észlelt esetleges hiányosságok megszüntetésére.

3. A szervezeti egységek vezetőinek feladatai

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

- a) betartják és betartatják az adat- és titokvédelmi, valamint a külön szabályzat szerinti biztonsági és információbiztonsági előírásokat,
- b) kijelölik az irányításuk alá tartozó szervezeti egység adatvédelmi felelősét, azzal, hogy kijelölés hiányában a szervezeti egységek vezetői maguk kötelesek ellátni az ezzel kapcsolatos feladatokat,
- c) gondoskodnak arról, hogy az irányításuk alá tartozó szervezeti egységek felelősségi körébe tartozó nyilvántartási rendszerek naprakészek, megbízhatóak legyenek,
- d) gondoskodnak arról, hogy az irányításuk alatt álló személyek az adatkezelés meghatározott feltételeinek megfelelően járjanak el [GDPR 32. cikk (4) bek.],
- e) az Intézmény döntés előkészítésre vonatkozó szabályainak megfelelően döntenek a jelen szabályzatban, illetve az adatkezeléssel járó folyamatot szabályozó egyéb belső szabályzatokban a feladat- és hatáskörükbe utalt kérdésekben.

4. Az adatvédelemért felelős főigazgató-helyettes feladatai

Az adatvédelmi feladatok koordinálásáért felelős főigazgató-helyettes

- az SZJC esetén az igazgatási, jogi és humánpolitikai főigazgató-helyettes, az informatikát és dokumentációt érintő kérdések tekintetében a stratégiai főigazgató-helyettes,



- az SZMK esetén a Főigazgató, a főigazgató SZMSZ szerinti helyettese vagy a főigazgató által írásban kijelölt dolgozó,
- az SZKD esetén a Főigazgató, a főigazgató SZMSZ szerinti helyettese vagy a főigazgató által írásban kijelölt dolgozó

felelős.

Az adatvédelemért felelős főigazgató-helyettes a jogi iroda bevonásával:

- a) az adatvédelmi tisztviselő szükség szerinti közreműködésével - a személyes adatok kezelését, illetve a GDPR szerinti jogaik gyakorlását érintő panaszok kivételével - ellátja az érintetti jogok gyakorlásával kapcsolatos beadványok megválaszolását,
- b) biztosítja, hogy az adatvédelmi tisztviselő véleményét kikérjék az Intézmény adatvédelmi tárgyú vagy adatvédelmi vonatkozású belső szabályzatainak előkészítése során,
- c) szakmai támogatást nyújt az adatkezeléssel összefüggő, valamint a nem adatvédelmi jogszabályok értelmezésében.

Az adatvédelemért felelős főigazgató-helyettes az informatikai és dokumentációs főosztály és az informatikai biztonságvédelmi felelős bevonásával:

- a) ellátja az informatikai biztonsággal kapcsolatos adatvédelmi feladatokat az Informatikai biztonsági szabályzatban meghatározottak szerint;
- b) az informatikai fejlesztéseknél és beszerzéseknél ellátja a beépített és alapértelmezett adatvédelem elvének érvényesüléséhez szükséges informatikai feladatokat,
- c) az informatikai üzemeltetés területén ellátja a személyes adatok kezelésével kapcsolatos technikai védelem megvalósítását, ellátja – az Informatikai biztonsági szabályzatban meghatározott – hatáskörébe tartozó információbiztonsági feladatokat, valamint a rendelkezésre állási kontrollok biztosítását, a tárolt és továbbított személyes adatok bizalmasságának védelmét, az incidens felderítési és - kezelési tevékenység támogatását,
- d) gondoskodik az Intézmény honlapján és intranetes hálózatán, vagy más, a kezelésében álló közösségi felületén közzétett adatkezelési tájékoztatók aktualizálásáról, archiválásáról és megőrzéséről.

5. A jogi iroda feladatai

A jogi iroda:

- a) szakmai támogatást nyújt az adatkezeléssel összefüggő és nem adatvédelmi jogszabályok értelmezésében,
- b) szükség szerint az eseti meghatalmazás keretei között biztosítja az Intézmény képviselőjét az érintett által az Intézmény ellen az érintett adatvédelmi jogainak megsértése miatt indított, illetve az Intézmény által a Nemzeti Adatvédelmi és



Információszabadság Hatóság határozatainak felülvizsgálata iránt indított perekben, illetve egyéb eljárásokban.

6. A kommunikációért felelős személyfeladatai

Az adatvédelemmel összefüggő kommunikációs feladatok ellátásáért

- az SZJC esetén a kommunikációs vezető,
- az SZMK esetén a Főigazgató, a főigazgató SZMSZ szerinti helyettese vagy a főigazgató által írásban kijelölt dolgozó,
- az SZKD esetén a Főigazgató, a főigazgató SZMSZ szerinti helyettese vagy a főigazgató által írásban kijelölt dolgozó

felel.

A kommunikációért felelős személy szükség esetén az informatikai főosztály bevonásával:

- a) gondoskodik az érintettek részére nyújtott tájékoztatás közzétételéről,
- b) adatvédelmi incidens esetén közreműködik az érintettek tájékoztatásának módjáról és a tájékoztatás tartalmáról való döntés előkészítésében, megvalósításában,
- c) adatvédelmi incidens esetén – az adatvédelmi tisztviselő közreműködésével – szükség esetén előkészíti a sajtóközleményt, segíti a főigazgató munkáját a sajtóval való kapcsolattartás során.

7. Az adatvédelmi felelősök feladatai

Adatvédelmi felelőst valamennyi szervezeti egységnél ki kell jelölni. Adatvédelmi felelősnek olyan felsőfokú végzettséggel rendelkező személyt kell kijelölni, aki az adott szakterület működését és munkafolyamatait, illetve a szakterület tevékenységét támogató informatikai rendszereket illetően kellő ismeretekkel bír.

Kijelölés hiányában az adatvédelmi felelős a szervezeti egység vezetője.

Az adatvédelmi felelős az öt foglalkoztatott szervezeti egység tevékenységi körén belül:

- a) előkészíti az adatkezeléssel kapcsolatos, az adatkezelőt terhelő döntéseket, illetve abban közreműködik,
- b) gondoskodik az adatkezeléshez kapcsolódó adminisztratív teendők ellátásáról (az adatkezeléssel összefüggő döntések dokumentálása, érdekmérlegelési teszt elvégzése, hatásvizsgálat lefolytatása, az adatkezeléssel összefüggő szerződések előkészítése, az adatkezelések nyilvántartásának naprakészen tartása stb.), illetve abban való közreműködés,
- c) együttműködik az ugyanazon adatkezelésben érintett más adatvédelmi felelősökkel, valamint az adatvédelmi tisztviselővel,
- d) közreműködik az érintettek jogai gyakorlásának biztosításában,
- e) közreműködik az adatvédelmi incidensek következményeinek elhárításában,

- f) közreműködik az adatvédelmi tisztviselő vizsgálataiban,
- g) közreműködik az adatkezelési nyilvántartás elkészítésében,
- h) közreműködik az Intézmény kezelésében lévő adatok biztonsági osztályba sorolásában,
- i) ellátja a jelen szabályzat szerint hatáskörébe utalt, valamint adatvédelmi jellegű eseti feladatokat.

Az adatvédelmi felelős az adatbiztonsági intézkedéseket érintően:

- a) információk szolgáltatásával közreműködik az adatkezelés biztonságát fenyegető kockázatok felmérésében és meghatározásában,
- b) az informatikai és dokumentációs feladatok ellátásáért felelős vezető vele együttműködve közreműködik azon információbiztonságot érintő feladatok végrehajtásában, amelyek az adatbiztonsági követelmények megvalósulásához szükségesek,
- c) figyelemmel kíséri az adatbiztonsági előírások érvényre juttatását a szervezeti egységen belül, felhívja a szakterületen dolgozók figyelmét a szabályok betartására, jelzi a szabályok megsértését az érintett munkavállaló felettesének, közreműködik a szakterületen dolgozók adatvédelmi tudatosságának növelésében.

V. Adatkezelők, adatfeldolgozás és közös adatkezelés

Az Intézményben mindazon, a jelen szabályzat személyi hatálya alá tartozó személy, aki személyes adat birtokába jut, illet munkaköre vagy tisztsége alapján kezel, köteles védeni és őrizni a személyes adatokat, és minden erőfeszítést megtenni annak érdekében, hogy azok megfelelő védelmét biztosítsa.

Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

Az egyes szervezeti egységek egységszintű működési szabályzata tartalmazza az adott szervezeti egység hatáskörén belül a személyes adatok kezelésére jogosultak körét. A szervezeti egység keretében tevékenységet végzők munkaköri leírása, illetve feladatleírása tartalmazza a dolgozó személyes adatok kezelésével és védelmével kapcsolatos feladatait.

Az Intézménnyel jogviszonyban állók a munkakörükből, velük kötött szerződésből, tisztségükből adódó feladataik teljesítése során kötelesek bizalmasan kezelni minden olyan adatot, információt vagy dokumentumot – függetlenül attól, hogy ahhoz milyen formában és milyen módon jutottak hozzá –, amely előttük a feladataik teljesítése során vagy azzal összefüggésben vált ismertté.

Az Intézménnyel jogviszonyban álló, adatkezelést vagy adatfeldolgozást végző személyek felelősséggel tartoznak minden olyan kárért, amely adatkezelési, adatvédelmi kötelezettségük megszegéséből származik.

Ha az adatkezelést az Intézmény nevében más végzi, az Intézmény kizárólag olyan adatfeldolgozókat vehet igénybe, akik, vagy amelyek megfelelő garanciákat nyújtanak

az adatkezelés követelményeinek való megfelelésért és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

Az adatfeldolgozói megállapodás tartalmi követelményeivel kapcsolatos rendelkezéseket és a szerződéskötés eljárásrendjét a VI. pont 5. alpontja tartalmazza részletesen.

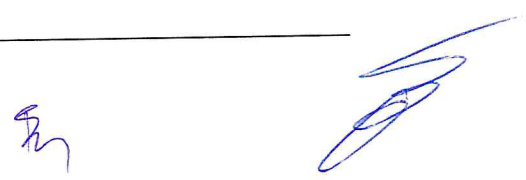
Közös adatkezelésnek minősül, ha az adatkezelés céljait és eszközeit az Intézmény egy vagy több másik adatkezelővel közösen határozza meg. (GDPR 26. cikk)

A közös adatkezelői megállapodás tartalmi követelményeivel kapcsolatos rendelkezéseket és a szerződéskötés eljárásrendjét a VI. pont 6. alpontja tartalmazza részletesen.

VI. Az adatkezelés bevezetésével, módosításával és megszüntetésével kapcsolatos feladatok

1. Adatkezelés bevezetésével kapcsolatos feladatok

- 1.1. Új adatkezeléssel járó tevékenység bevezetése esetén (beleértve a meglévő nyilvántartási rendszer adatainak új célú felhasználásával, új célú adatkezelés bevezetésével, nyilvántartási rendszerbe adatok felvételével, adatok tárolásával, harmadik személynek továbbításával megvalósuló adatkezelést is), az adatkezelés bevezetése során a döntés előkészítés rendjére vonatkozó Intézményi szabályokat e fejezet rendelkezéseit figyelembe véve kell alkalmazni.
- 1.2. Új, személyes adatokra is kiterjedő nyilvántartási kötelezettség bevezetése főigazgatói utasítással történik. A főigazgatói utasítás tartalmazza
 - az adatkezelésért felelős szervezeti egységnek és egyéb szervezeti egységeknek az adatkezeléssel kapcsolatos feladatait, így különösen:
 - az adatok felvételének, módosításának, törlésének rendjét,
 - adatszolgáltatási kötelezettségek meghatározását az adatok naprakészen tartása érdekében,
 - a nyilvántartási rendszerből történő adattovábbítást, az ahhoz való hozzáférés rendjét.
 - mellékletként
 - a GDPR-nak, az Infotv.-nek és egyéb alkalmazandó jogszabályoknak megfelelő adatkezelési tájékoztatót,
 - hozzájáruláson alapuló adatkezelés esetén a hozzájáruló nyilatkozat mintáját.
- 1.3. Az adatkezelésért felelős szervezeti egység adatvédelmi felelősét az új adatkezelés bevezetésére vonatkozó igény megfogalmazásától kezdve be kell vonni az adatkezelés feltételeinek kidolgozása folyamatába.
- 1.4. Amennyiben az új adatkezelés bevezetése több szervezeti egységet érint, az adatkezelésért felelős valamennyi érintett szervezeti egység adatvédelmi felelősét be kell vonni az adatkezelés feltételeinek kidolgozása folyamatába. A fejlesztési igényt megfogalmazó szervezeti egység vezetője az egyéb területek adatvédelmi felelősei bevonásának szükségességéről az érintett adatvédelmi felelősöket és az adatvédelmi tisztviselőt értesíti.





- 1.5. Az adatkezelés feltételeinek kidolgozásában érintett szervezeti egységek adatvédelmi felelősei kötelesek egymással és az adatvédelmi tisztviselővel együttműködni. Az adatkezelés feltételeinek kidolgozásában érintett szakterületek/szervezeti egységek adatvédelmi felelősei tevékenységének koordinálásáról az adatvédelmi tisztviselő gondoskodik.
- 1.6. Az adatkezelés bevezetésével, az adatkezelés feltételeinek meghatározásával kapcsolatban
- a) a leendő adatkezelésért annak tárgya szerint felelős szervezeti egység adatvédelmi felelőse (vagy szükség esetén több érintett adatvédelmi felelős egymással együttműködve):
 - a. meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, és írásbeli összefoglalót készít (GDPR 4. cikk 7. és 16. pont),
 - b. az a) pont a. alpontjában meghatározott feladat részeként előterjesztést tesz a főigazgatónak arról, hogy az eltérő célú adatkezelés összeegyeztethető-e az eredeti adatkezelési céllal, és így szolgálhat-e a tervezett adatkezelés új jogalapjául [GDPR 6. cikk (4) bek.],
 - c. az a) pont a. alpontjában meghatározott feladat részeként, amennyiben az adatkezelés jogalapja a jogos érdek lehet, elkészíti az érdekmérlegelési teszt dokumentumának tervezetét [GDPR 6. cikk (1) bek. f) pont],
 - d. aza) pont a. alpontjában meghatározott feladat részeként az adatvédelmi tisztviselő véleményének kikérése után javaslatot tesz a főigazgatónak adatvédelmi hatásvizsgálat elvégzésére; a főigazgató erre vonatkozó pozitív döntése esetén – az Informatikai Osztály adatvédelmi felelősenek közreműködésével – elvégzi a hatásvizsgálatot, elkészíti ennek dokumentumát, és kikéri róla az adatvédelmi tisztviselő, valamint – ha alkalmazható – az érintettek vagy képviselőik véleményét [GDPR 35. cikk (1)-(2) és (9) bek.],
 - e. az a) pont a. alpontjában meghatározott feladat részeként előterjesztést tesz a főigazgatónak arról, hogy az adatkezelést közös adatkezelésként indokolt-e ellátni, illetve indokolt-e adatfeldolgozót bevonni,
 - f. az a) pont a. alpontjában meghatározott feladat részeként javaslatot tesz automatizált döntéshozatali módszer, illetve profilalkotási módszer alkalmazására [GDPR 22. cikk (1) bek.],
 - g. aza) pont a. alpontjában meghatározott feladat részeként megszövegezi a hozzájáruló nyilatkozat mintáját [GDPR 7. cikk (2) bek.], illetve a megfelelő szerződéses rendelkezéseket,
 - h. megfogalmazza az adatkezelésről szóló tájékoztatást (GDPR 13-14. cikk),
 - i. az informatikai osztály közreműködésével szükség esetén gondoskodik az adatkezelésről szóló tájékoztatás könnyen



- hozzáférhető módon való közzétételéről [GDPR 12. cikk (1) bek.],
- j. az adatkezelés bevezetéséről való döntést követően gondoskodik az új adatkezelés, illetve a nyilvántartott adatokban bekövetkezett valamennyi változás adatkezelési nyilvántartásban történő rögzítéséről [GDPR 30. cikk (1) bek.],
 - k. amennyiben ennek szükségessége felmerül, egyedi esetben előterjesztést tesz a főigazgatónak az érintett vagy harmadik személy létfontosságú érdeke fennállásáról [GDPR 6. cikk (1) bek. d) pont, 9. cikk (2) bek. d) pont] mint az adatkezelés lehetséges jogcíméről,
 - l. amennyiben ennek szükségessége felmerül, egyedi esetben előterjesztést tesz a főigazgatónak arról, hogy személyes adatok harmadik országba továbbíthatók-e egyedi ügyekben [GDPR 49. cikk (1) bek.].
- b) az informatikai és dokumentációs főosztály adatvédelmi felelőse a személyes adatot kezelő rendszer fejlesztése és beszerzése során közreműködik
- 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 visszakereshető módon valósuljanak meg,
 - c. annak biztosításában, hogy az adatvédelmi tájékoztatók és nyilatkozatok könnyen elérhetők legyenek az érintettek számára,
 - d. annak biztosításában, hogy az adatkezeléssel kapcsolatos ügyfélrendelkezéseket visszakereshető formában tárolják,
 - e. az adatok sértetlenségével, bizalmasságuk megőrzésével kapcsolatos kontrollok tervezéskori érvényesítésében, illetve dokumentált meglétében,
 - f. az a) pont a., d., e., f., h., és l. alpontjai szerinti döntések előkészítésében.
- 1.7. A VI. pont 1.6. alpontjának alkalmazása során döntésre jogosultnak minősül az személy, aki az érintett adatkezelés alapjául szolgáló tevékenységgel kapcsolatban döntéshozatalra jogosult, illetve – amennyiben a döntés testületi hatáskörbe tartozik – a testületi döntés előkészítéséért felelős.
- 1.8. A VI. pont 1.6. alpontjában meghatározott döntések, javaslatok véglegesítése előtt ki kell kérni az adatvédelmi tisztviselő véleményét, úgy, hogy az adatvédelmi tisztviselőnek legalább nyolc munkanapja legyen a vélemény adására.
- 1.9. Az adatvédelmi tisztviselő véleményének kikéréséhez olyan dokumentumot, leírást kell benyújtani, amely kellő részletességgel meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, illetve a VI. pont 1.6. alpontjában meghatározott egyéb döntési javaslatokat.



- 1.10. Az adatvédelmi tisztviselő adatvédelmi jogi támogatást nyújt az adatvédelmi felelős által előkészített, megszövegezett, adatkezeléshez kapcsolódó dokumentumok elkészítésében és közreműködik azok véglegesítésében. Az adatvédelmi tisztviselő
- a) beszerzi az alábbi szervezeti egységek véleményét is:
 - a. a főigazgató, a főigazgató SZMSZ szerinti helyettese, vagy a főigazgató által írásban megbízott dolgozó véleményét a VI. pont 1.6. alpontja a) pontjának a., e., f., g., h., és i. alpontjai tekintetében;
 - b. az informatikai főosztály véleményét VI. pont 1.6. alpontja a) pontjának a., d., e., f., h. és i. alpontjai tekintetében;
 - b) megvizsgálja a véleményezésre megküldött dokumentumot, leírást
 - a. adatvédelmi jogi szempontból,
 - b. abból a szempontból, hogy azok milyen módon illeszthetők be az Intézmény informatikai rendszereibe, illetve nincs-e a tervezett adatkezeléssel azonos vagy hasonló adatkezelés.
- 1.11. A végleges dokumentumok szakmai megfelelőségéért a dokumentum létrehozását kezdeményező adatvédelmi felelős, az adatvédelmi megfelelőségéért az adatvédelmi tisztviselő, az informatikai biztonsági megfelelőségéért pedig az informatikai biztonságvédelmi felelős a felelős. Abban az esetben, ha bármely terület eltér a megfogalmazott szakmai, adatvédelmi vagy információbiztonsági állásfoglalásoktól, az eltérést, illetve a végleges dokumentumért az adatvédelmi tisztviselő vagy az információbiztonsági felelős semmilyen felelősséggel nem tartozik.
- 1.12. AVI. pont 1.11. alpontjában említett szervezeti egységek a véleményüket az adatvédelmi tisztviselőnek küldik meg az adatvédelmi tisztviselő által meghatározott határidőben, amely nem lehet kevesebb öt munkanapnál. A véleményeket az adatvédelmi tisztviselő összesíti és véglegesíti, szükség esetén az adatvédelmi felelősökkel és a véleményezőkkel való konzultáció után.
- 1.13. Amennyiben az adatkezelés feltételei kidolgozásában részt vevő adatvédelmi felelősök között véleményeltérés van, illetve az igazgatási, jogi és humánpolitikai főigazgató-helyettes vagy az informatikai osztály kifogást fogalmaz meg, az adatvédelmi tisztviselő – szükség esetén az adatvédelmi felelősökkel és a véleményezőkkel való konzultáció után – javaslatot tesz a lehetséges megoldásra.
- 1.14. Az adatvédelmi tisztviselő véleményét az adatkezelés bevezetéséről való döntést kezdeményező előterjesztésben ismertetni kell. Az adatvédelmi tisztviselő véleményétől való eltérést az előterjesztésben részletesen meg kell indokolni.

2. Az érdekmérlegelési teszt elvégzésének módszertana

- 2.1. 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.

- 2.2. Az érdekmérlegelési tesztet a tervezett adatkezelésért felelős szervezeti egység adatvédelmi felelőse végzi el az adatvédelmi tisztviselő közreműködése mellett. Az érdekmérlegelési tesztet írásban kell elvégezni. Az elkészült dokumentumot – a VI. pont 1.8.-1.10. alpontjai szerint – az adatvédelmi tisztviselőnek kell megküldeni, aki azt szakmai szempontból véleményezi. A jogos érdeken alapuló adatkezelés kizárólag az érdekmérlegelési teszt elvégzését és az adatvédelmi tisztviselő véleményének beszerzését követően kezdhető meg. A VI. pont 1.14. alpontjának rendelkezéseit jelen esetben is alkalmazni kell.
- 2.3. Az érdekmérlegelési teszt módszertanát, a megválaszolandó kérdéseket minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani, a jelen szabályzatban meghatározott kérdések köre csak iránymutató jellegű, az a tervezett adatkezelés szempontjából releváns egyéb kérdésekkel bővítendő. Abból kell kiindulni, hogy bármilyen adatkezelés beavatkozás az érintett magánszférájába és e beavatkozás jogosságát, szükségességét és arányosságát kell bizonyítani.
- 2.4. Az érdekmérlegelési teszt részei:

- a) A tervezett adatkezelés leírása és az annak keretében kezelni tervezett személyes adatok meghatározása.

Itt szükséges a lehető legrészletesebben meghatározni az adatkezelési tevékenységet, így elsősorban: az adatkezelés jellegét, hatókörét, körülményeit és célját.

- b) Az adatkezelő vagy azon harmadik fél jogos érdekének azonosítása, akinek az adatkezelés érdekében áll.

Itt szükséges kifejtetni, hogy az Intézmény az adatkezelés során pontosan mely jogos érdekre alapítja az adatkezelés jogszerűségét. Lényeges arra is kitérni, hogy az adatkezelés valóban szükséges-e az elérni kívánt célhoz, vagy az más, az érintett magánszféráját kevésbé sértő módon is elérhető.

A GDPR (47) preambulum bekezdése alapján ilyen jogos érdekről lehet szó például olyankor, amikor releváns és megfelelő kapcsolat áll fenn az érintett és az Intézmény között, például olyan esetekben, amikor az érintett az adatkezelő ügyfele vagy annak alkalmazásában áll. A jogos érdek fennállásának megállapításához mindenképpen körültekintően meg kell vizsgálni többek között azt, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e észszerűen arra, hogy adatkezelésre az adott célból sor kerülhet.

Az érintett érdekei és alapvető jogai elsőbbséget élvezhetnek az Intézmény érdekével szemben, ha a személyes adatokat olyan körülmények között kezelik, amelyek közepette az érintettek nem számítanak további adatkezelésre. Személyes adatoknak a csalások megelőzése céljából feltétlenül szükséges kezelése szintén az érintett adatkezelő jogos érdekének minősül. Személyes adatok



közvetlen üzletszerzési célú kezelése szintén jogos érdeken alapulónak tekinthető.

c) Az érintett érdekeinek, jogainak azonosítása.

Itt szükséges kifejtteni, hogy az adatkezelés során az érintett mely érdekei, alapvető jogai vagy szabadságai sérülhetnek, azaz mely érintetti érdekek állnak szemben az Intézmény jogos érdekével. Ilyen lehet például a magánélet tiszteletben tartásához való jog, kép- és hangmáshoz való jog stb.

d) Az Intézmény (vagy harmadik fél) és az érintettek érdekeinek összevetése.

Annak mérlegelése, hogy az Intézmény jogos érdeke és az érintettek érdekeinek védelme között hogyan teremthető meg az egyensúly.

Itt kell kifejtteni, hogy az Intézmény vagy a harmadik felek adatkezeléshez fűződő jogos érdeke miért erősebb, mint az adatkezeléssel megsértett vagy megsérthető érintetti érdekek. Valószínűsíteni kell, hogy az adatkezeléssel okozott érdeksérelem bekövetkezésének esélye alacsony, az esetlegesen okozott sérelem csekély súlyú, továbbá azt az adatkezeléssel elérhető előnyök meghaladják.

e) Biztosítékok leírása.

A kockázatot megszüntető vagy mérséklő intézkedési terv meghatározását tartalmazza.

Annak leírása, hogy milyen biztosítékok és garanciák alkalmazhatók az érintettek érdekeinek védelme érdekében, azaz az Intézmény milyen lépéseket tesz az érdeksérelem bekövetkezésének csökkentésére, vagy az elkerülhetetlenül okozott sérelem minimalizálására, így különösen biztonsági és informatikai biztonsági intézkedések.

Itt kell hivatkozni azon intézkedésekre, amelyeket az adatkezelő a megfelelés bizonyítása és az átláthatóság érdekében megtesz, így elsősorban az érintettek megfelelő tájékoztatásának helyét, módját is szükséges meghatározni, pl. hivatalos honlapon történő közzététellel.

f) Az érdekmérlegelési teszt eredménye, az érdekmérlegelés végkövetkeztetéseinek leírása.

3. Az adatvédelmi felelős feladatai az adatkezelés során

3.1. Az adatkezelés során az adatkezelésért felelős szervezeti egység adatvédelmi felelőse az adatkezelésért felelős szervezeti egység feladatkörébe tartozó kérdésekben:

- a) képviseli az adatkezelőt az adatfeldolgozó felé vagy – közös adatkezelés esetén – a többi adatkezelő felé (amennyiben releváns),
- b) figyelemmel kíséri az adatkezelés feltételeinek folyamatos fennállását (beleértve az adatkezelés jogszerűségéhez szükséges



tájékoztatások megadását, nyilatkozatok beszerzését stb.) és szükség esetén megteszi vagy kezdeményezi a szükséges intézkedéseket az adatkezelés feltételeinek módosítása iránt,

- c) amennyiben az adatkezelés hozzájáruláson alapul, megfelelő szabályozás kialakítása útján gondoskodik arról, hogy mindenkor igazolható legyen, hogy az érintett a hozzájárulását megadta [GDPR 7. cikk (1) bek.],
- d) gondoskodik arról, hogy legalább az érintettel való első kapcsolatfelvételkor felhívják a figyelmét a tiltakozási jogra, és hogy az erről szóló tájékoztatást egyértelműen és más információtól elkülönítve jelenítsék meg [GDPR 21. cikk (4) bek.],
- e) rendszeres időközönként, de legalább évente áttekinti a hatásvizsgálatban azonosított kockázatok alakulását, jelzi az adatvédelmi tisztviselőnek az adatkezeléssel járó kockázatok változását, közreműködik az adatvédelmi hatásvizsgálatok utóellenőrzésben [GDPR 35. cikk (11) bek.].

3.2. Az adatkezelés során (személyes adatok kezelési életciklusának üzemeltetési szakaszában) az informatikai osztály adatvédelmi felelőse – 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.

3.3. A VI. pont 3.1. alpont b) pontja alá eső esetekben

- a) megfelelően alkalmazni kell a VI. pont 1.2.-1.14. alpontjainak rendelkezéseit,
- b) az adatkezelés megváltozott adatait – a változást elrendelő döntés után – át kell vezetni az adatkezelési nyilvántartásban.

4. Adatkezelés megszüntetésével kapcsolatos feladatok

- 4.1 Amennyiben a kezelt adatokra a továbbiakban már nincs szükség (az adatkezelési cél megvalósult vagy megszűnt), vagy jogszabályi változások miatt, vagy az adatvédelmi felügyeleti hatóság vagy bíróság döntése értelmében az adatok kezelését meg kell szüntetni, az adatvédelmifelelős – az adatvédelmi tisztviselő és rajta keresztül az igazgatási, jogi és



humánpolitikai főigazgató-helyettes és szükség esetén az informatikai osztály vagy más érintett szervezeti egységálláspontjának 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.

4.2 A VI. pont 4.1.alpontjában meghatározott esetben

- a) megfelelően alkalmazni kell a VI. pont 1.2.-1.14. alpontjaiban foglalt rendelkezéseit,
- b) az adatkezelési nyilvántartásból az adatkezelést vagy az egyes adatfajtákat törölni kell,
- c) az adatokat – a VI. pont 4.1. alpontjának a) és b) pontjában tett megkülönböztetés szerint –
 - a. az informatikai rendszerekben archiválni kell, illetve
 - b. az informatikai rendszerekből törölni kell, a papír alapú nyilvántartásban kezelt adatokat pedig – az Iratkezelési szabályzat rendelkezései szerint – selejtezni kell.

5. Az adatfeldolgozó igénybevételének feltételei, az adatfeldolgozói megállapodás

- 5.1 Az adatfeldolgozó igénybevételének szükségességét az adatvédelmi felelős az adatkezelés bevezetéséről való döntés előkészítése részeként vizsgálja meg. Ezt a szabályt kell alkalmazni akkor is, ha az adatfeldolgozó igénybevételéről a folyamatban lévő adatkezelés során születik döntés. A döntés meghozatalára az adatvédelmi tisztviselő állásfoglalásának ismeretében a főigazgató jogosult.

Amennyiben döntés születik az adatfeldolgozó igénybevételéről, az adatvédelmi felelős az adatvédelmi jogi megfelelés biztosítása tekintetében az adatvédelmi tisztviselő és egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a jogi iroda közreműködésével, továbbá szükség esetén az informatikai osztály vagy az adatkezelésben érintett más szervezeti egység véleményének kikérésével előkészíti az adatfeldolgozóval kötendő szerződés tervezetét.

- 5.2 Az adatfeldolgozó által végzett adatkezelést olyan – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó – szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az Intézménnyel szemben. A szerződés kizárólag írásban köthető meg, és abban a GDPR 28. cikk (3) bekezdésében rögzített tartalmat is rögzíteni szükséges, így különösen előírni, hogy az adatfeldolgozó:

- a) a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli, – beleértve a személyes adatoknak valamely harmadik ország



vagy nemzetközi szervezet számára való továbbítását is –, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja,

- b) biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt álljanak,
- c) meghozza az adatkezelés biztonsága érdekében szükséges, a GDPR 32. cikkében előírt intézkedéseket,
- d) a további adatfeldolgozó igénybevételére vonatkozóan tiszteletben tartja a GDPR 28. cikk (2) és (4) bekezdésben említett feltételeket,
- e) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett GDPR III. fejezetében foglalt jogainak gyakorlásához kapcsolódó kérelmek megválaszolója tekintetében,
- f) segíti az adatkezelőt a GDPR 32–36. cikk szerinti kötelezettségeinek – így elsősorban az adatvédelmi incidens bejelentése, az adatvédelmi hatásvizsgálat lefolytatása és az előzetes konzultáció - teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat,
- g) az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő,
- h) az adatkezelő rendelkezésére bocsát minden olyan információt, amely a fenti kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is. Az adatfeldolgozó köteles haladéktalanul tájékoztatni az adatkezelőt, ha úgy véli, hogy annak valamely utasítása sérti a GDPR vagy a tagállami vagy uniós adatvédelmi rendelkezéseket,
- i) köteles közreműködni az érintettől származó kérelmek, panaszok megválaszolásában, az erről szóló eljárásrendet a szerződésben rögzíteni szükséges,
- j) rögzíteni szükséges az adatfeldolgozó kötelezettségeit az adatvédelmi incidens észlelése esetén, így különösen
 - i. az adatvédelmi incidens tudomására jutása esetén az Intézmény adatvédelmi tisztviselőjét haladéktalanul értesíteni köteles,
 - ii. köteles együttműködni az Intézmény adatvédelmi tisztviselőjével és más közreműködő szervezeti egységével az adatvédelmi



incidens okának feltárásában és következményeinek felszámolásában,

iii. köteles együttműködni az adatvédelmi incidens bejelentésének teljesítésében,

k) rögzíteni szükséges 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 utóellenőrzésében.

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

5.4 Az adatbiztonsági intézkedések megfelelőségének megítélése a főigazgató vagy az SZMSZ szerinti helyettese vagy a főigazgató által írásban megbízott dolgozó 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.

5.5 Az adatfeldolgozói szerződés megkötését követően – az adatkezelések nyilvántartására vonatkozó szabályok szerint – az adatfeldolgozó adatait (név és cím, kapcsolattartó neve és elérhetősége) rögzíteni kell az adatkezelési nyilvántartásban.

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

6. A közös adatkezelés feltételei, a közös adatkezelői megállapodás

6.1 A közös adatkezelés szükségességét az adatvédelmi felelős az adatkezelés bevezetéséről való döntés előkészítése részeként vizsgálja meg. A döntés meghozatalára az adatvédelmi tisztviselő álláspontjának ismeretében a főigazgató jogosult.

Amennyiben döntés születik a közös adatkezelés bevezetéséről, az illetékes adatvédelmi felelős(ök), az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő és egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében az igazgatási, jogi és humánpolitikai főigazgató-helyettes közreműködésével, továbbá szükség esetén az informatikai osztály vagy más érintett szervezeti egység véleményének kikérésével előkészíti a közös adatkezelésről szóló megállapodás tervezetét (benne a közös adatkezelőknek az érintettek számára kijelölendő kapcsolattartójának kijelölésével kapcsolatos döntést, valamint a közös adatkezelésre vonatkozó megállapodásnak az érintettek



rendelkezésére bocsátható lényegi elemeit) és azt felterjeszti a szerződés megkötésére jogosult személynek.

A jelen pont alkalmazásában a szerződés megkötésére jogosult személy az, aki az érintett adatkezelés alapjául szolgáló tevékenységgel kapcsolatban döntésre jogosult, illetve – amennyiben a döntés testületi hatáskörbe tartozik – a testületi döntés előkészítéséért felelős.

6.2 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
 - i. mely adatkezelési műveleteket (pl. hozzájáruló nyilatkozatok felvétele, adatok tárolása, adatok felhasználása stb.) végzik,
 - ii. az érintett tájékoztatását hogyan végzik (pl. melyik adatkezelő készíti el az adatkezelési tájékoztatót és bocsátja az érintettek rendelkezésére stb.),
 - iii. az érintett jogainak gyakorlását hogyan biztosítják (pl. egyesített vagy elkülönített ügyfélszolgálat stb.),
 - iv. az esetleges jogellenes adatkezelés következményeit milyen arányban viselik;
 - v. az adatvédelmi incidens észlelése esetén követendő eljárást, különösen azt, hogy
 - az adatvédelmi incidens tudomásra jutása esetén a másik adatkezelő adatvédelmi tisztviselőjét (adatvédelmi tisztviselő hiányában a kijelölt kapcsolattartót) haladéktalanul kötelesek értesíteni az adatvédelmi rendellenességről vagy incidensről,
 - egymással kötelesek együttműködni az adatvédelmi rendellenesség vagy incidens okának kiderítésében és következményeinek felszámolásában,
 - az egyes adatkezelőket mely adatvédelmi incidensek tekintetében terheli a bejelentési kötelezettség;
- c) azt, hogy kijelölnek-e kapcsolattartót az érintettek számára, és ha igen, a kapcsolattartó személyét és elérhetőségét naprakészen kell tartani,
- d) a megállapodásról az érintett rendelkezésére bocsátandó összefoglalót, amelynek – 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.



VII. Az adatkezelési nyilvántartás

Az adatvédelmi tisztviselő feladatainak segítése keretében az adatvédelmi tisztviselő az adatvédelmi felelősök közreműködésével vezeti az adatkezelési nyilvántartást. Az adatkezelési nyilvántartás valamennyi, az Intézmény általi adatkezelés esetén tartalmazza:

- a) az adatkezelés célját,
- b) az adatkezelés jogalapját,
- c) az érintettek körét,
- d) az érintettekre vonatkozó személyes adatok kategóriáit,
- e) az adatok forrását (opcionális),
- f) az adatok kezelésének időtartamát vagy az adattörlés ideje megállapításának szempontjait;
- g) a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló, valamint nemzetközi szervezethez történő adattovábbításokat és azok garanciáinak leírását is,
- h) az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét,
- i) az alkalmazott adatfeldolgozási technológia jellegét (opcionális);
- j) az alkalmazott automatizált döntéshozatali logikákat (opcionális);
- k) az adatkezelő, valamint közös adatkezelés esetén a közös adatkezelők megnevezését és elérhetőségét,
- l) az adatkezelésért felelős szervezeti egység megnevezését, az adatokhoz hozzáférésre jogosult személyek körét (munkakör), (opcionális),
- m) az adatvédelmi tisztviselő nevét és elérhetőségét,
- n) az adatkezelés módszerét (manuális, számítógépes, vegyes),
- o) ha lehetséges, az adatbiztonsági intézkedések általános leírását,
- p) az archiválás módját, gyakoriságát (opcionális),
- q) az adatbiztonsági kockázati besorolást (opcionális)
- r) az érdekmérlegelési teszt és a hatásvizsgálati dokumentum elérhetőségét (opcionális).

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

Az Intézmény adatvédelmi tisztviselője az adatkezelési nyilvántartásba való betekintést – a hatóság képviselőin kívül – az Intézmény érintett szakterületei, továbbá a közös adatkezelést érintő rész tekintetében a közös adatkezelő részére biztosítja.



A nyilvántartási célú adatállományt kezelő szervezeti egység adatvédelmi felelőse az új adatállomány kialakítását a tevékenység megkezdése előtt 5 munkanappal bejelenti az adatvédelmi tisztviselőnek, aki azt adatkezelési nyilvántartásba bejegyzí.

Az adatkezelési nyilvántartásba bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelésért felelős szervezeti egység adatvédelmi felelőse 5 munkanapon belül köteles bejelenteni az adatvédelmi tisztviselőnek, aki ennek megfelelően módosítja az adatkezelési nyilvántartás adatait.

Az adatkezelési nyilvántartással összefüggésben az adatvédelmi tisztviselő:

- a) biztosítja, hogy az adatkezelések bevezetését megelőző döntéselőkészítés során az érintett szakterületek az adatkezelési tevékenységek nyilvántartása adatait megismerhessék a felesleges, párhuzamos adatkezelések elkerülése, illetve az új adatkezelésnek a meglévő adatkezelésekhez való illeszkedése érdekében,
- b) ellenőrzi az adatkezelések, közös adatkezelők, illetve adatfeldolgozók adatainak az adatkezelési nyilvántartásba történő rögzítését és jelzi az adatkezelésért felelős szervezeti egység vezetőjének a hiányos, hibás vagy valószínűleg megváltozott adatokat, információkat,
- c) a jogi feladatok ellátásáért felelős főigazgató-helyettessel és a jogi irodával együttműködve figyelemmel kíséri az adatkezelést érintő jogszabályok változását és a szükséges módosításokra felhívja az adatkezelési megbízottak figyelmét,
- d) az adatvédelmi felügyeleti hatóság megkeresésére adatot szolgáltat az adatkezelési nyilvántartásból.

VIII. Az érintettektől származó kérelmek, panaszok megválaszolásának rendje

1. Az adatvédelmi bejelentések típusai

Az érintettől különösen a következő, személyes adatai Intézmény általi kezelését érintő beadványok érkehetnek:

- bejelentheti az Intézmény által nyilvántartott adatok megváltozását,
- tájékoztatást kérhet személyes adatai tekintetében (milyen személyes adatokat milyen célból, milyen jogalapon, milyen forrásból szereztve 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),
- kérheti pontatlanul nyilvántartott személyes adatai helyesbítését, illetve vitathatja a nyilvántartott személyes adatok pontosságát – helyesbítéshez való jog (GDPR 16. cikk),
- kérheti nyilvántartott személyes adatai törlését – törléshez való jog (GDPR 17. cikk),
- 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),

- 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),
- 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),
- automatizált döntéshozatal alkalmazása esetén az adatkezelő részéről emberi beavatkozást kérhet, közölheti álláspontját (GDPR 22. cikk (3) bek.),
- kifogást nyújthat be az automatizált döntéshozatal alkalmazásával meghozott döntéssel szemben (GDPR 22. cikk (3) bek.),
- panaszt nyújthat be a személyes adatok kezelését, illetve a GDPR szerinti jogaik gyakorlását érintően (GDPR 77. cikk, 38. cikk (4) bek.),
- az elhunyt érintett életében tett meghatalmazottjaként vagy közeli hozzátartozójaként gyakorolni kívánja az érintett egyes jogait (Infotv. 25. §).

2. Az adatvédelmi beadványok elintézése

Az adatvédelmi tisztviselő bármely esetben – az érintett beadványának kivizsgálása, illetve saját ellenőrzése eredményeként, továbbá az adatvédelmi felügyeleti hatóság vagy bíróság döntése végrehajtásaként – kezdeményezheti személyes adat helyesbítését, törlését vagy az adatkezelés korlátozását (zárolást).

Az Intézményhez érkező, jelen szabályzat VIII. pontjának 1. alpontjában meghatározott beadványokat a GDPR 12. cikkében írt határidők figyelembevételével – elintézni, az alábbi kiegészítésekkel és eltérésekkel:

- A GDPR 77. cikkében, valamint a 38. cikkének (4) bekezdésében meghatározott panasz kivizsgálását az adatvédelmi tisztviselő végzi. A panasz kivizsgálása során az érintett szervezeti egységek kötelesek az adatvédelmi tisztviselővel együttműködni. A személyes adatok kezelését, illetve a GDPR szerinti jogok gyakorlását érintő panasz megalapozottsága esetén az adatvédelmi tisztviselő az adatkezelésért felelős szervezeti egységeknél intézkedést kezdeményez a panasz kiváltó okainak orvoslására, az érintett folyamatok felülvizsgálatára, valamint – szükség esetén – a személyi felelősség megállapítására,
- az adatvédelmi tisztviselő dönt abban a kérdésben, hogy a jelen szabályzat VIII. pontjának 1. alpontjában meghatározott tárgyú beadvány egyértelműen megalapozatlan vagy túlzó-e,



- az érintettnek saját adatairól tájékoztatás csak egyértelmű azonosítás után adható,
- a főigazgató vagy az SZMSZ szerinti helyettese vagy a főigazgató által írásban megbízott dolgozó bármely beadvány esetén kérheti az adatvédelmi tisztviselő véleményét a tekintetben, hogy a beadvány a jelen szabályzat VIII. pontjának 1. alpontjában meghatározott tárgyú-e, illetve, hogy az érintett kérte-e az adatkezelés korlátozását (zárolás, GDPR 18. cikk), és kérés esetén az adatvédelmi tisztviselő az informatikai és dokumentációs főosztályvezető közreműködésével intézkedik annak az informatikai rendszerekben történő megvalósításáról. Az adatkezelés korlátozásának (zárolásának) feloldásáról az adatvédelmi tisztviselő külön tájékoztatja az érintett informatikai rendszer(ek)e)t üzemeltető szervezet egységeket,
- az Intézmény szervezeti egységei a jelen szabályzat VIII. pontjának 1. alpontjában meghatározott tárgyú ügyekben készített válaszlevél-tervezetét előzetes jóváhagyás végett kötelesek bemutatni az adatvédelmi tisztviselőnek.

IX. Az érintettek jogai, azok érvényesítése

1. Tájékoztatási kötelezettség

Az érintettek részére a személyes adatok megszerzésének időpontjában tájékoztatást kell adni a személyes adatok kezelésének tényéről, céljáról, jogalapjáról, a kezelt adatok köréről, az adatkezelés módjáról, időtartamáról vagy az időtartam meghatározásának szempontjairól, az adattovábbítás szabályairól, a felügyeleti hatósághoz címzett panasz benyújtásának jogáról, az Intézmény adatvédelmi tisztviselőjének nevéről és elérhetőségéről.

Amennyiben az érintettek köre pontosan nem határozható meg vagy az adatvédelmi tisztviselő álláspontja szerint ez indokolt, az adatkezelési tájékoztatót az Intézmény honlapjának bármely aloldaláról közvetlenül vagy hivatkozás útján elérhető módon köteles közzétenni. A közzétételért a kommunikációért felelős munkatárs és az informatikai osztály felelős.

Ezen tájékoztatás mellett az érintett figyelmét kifejezetten fel kell hívni a tiltakozáshoz való jog érvényesítésének lehetőségére, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

Egyéb esetben az Intézmény olyan módon köteles eleget tenni tájékoztatási kötelezettségének, hogy az az érintettek számára elérhető legyen (például intraneten történő közzététellel, a szerződés mellékleteként csatolva, papír alapon kihelyezve a helyben szokásos módon, stb.)

Az Intézmény honlapján vagy intranetes hálózatán közzétett adatkezelési tájékoztatók archiválása és megőrzése – az érvényességi időtartam megjelölésével – az informatikai osztály feladata.



Az Intézmény minden olyan címzettet tájékoztat a személyes adatot érintő valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölte, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az Intézmény tájékoztatja ezen címzettek köréről.

2. Az érintett tájékoztatáshoz való joga – hozzáféréshez való jog

Az érintett – jogosultsága igazolását követően befogadott – kérelmére az Intézmény az adatkezelést tárgya szerint illetékes vezetője útján a kérelem beérkezésétől számított 30 napon belül tájékoztatást ad az érintett vonatkozásában, folyamatban lévő adatkezelésről.

Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő maximum további két hónappal meghosszabbítható a tájékoztatást kérő személy előzetes tájékoztatása mellett.

Az érintett jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

- a) az adatkezelés céljai,
- b) az érintett személyes adatok kategóriái,
- c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket,
- d) adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,
- e) az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen,
- f) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga,
- g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ,
- h) automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

A személyes adatokhoz való hozzáférést úgy kell biztosítani, hogy ez alatt az érintett más személy adatait ne ismerhesse meg.

Az érintett részére készítendő válasz tervezetét az adatkezelés tárgya szerint illetékes szervezeti egység adatvédelmi felelőse köteles összeállítani, az adatvédelmi tisztviselővel együttműködve.



3. A helyesbítéshez való jog

Az érintett – jogosultsága igazolását követően befogadott – kérelmére az adatkezelést végző szervezeti egység adatvédelmi felelőse az adatvédelmi tisztviselő előzetes tájékoztatása és jóváhagyása mellett indokolatlan késedelem nélkül helyesbíti az érintettre vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését is.

4. Az adatkezelés korlátozásához való jog

Az érintett – jogosultsága igazolását követően befogadott – kérelmére az adatkezelést végző szervezeti egység adatvédelmi felelőse tájékoztatása alapján az adatvédelmi tisztviselő korlátozza az adatkezelést, ha az alábbi feltételek valamelyike teljesül:

- a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi tisztviselő ellenőrizze a személyes adatok pontosságát,
- b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását,
- c) az Intézménynek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy
- d) az érintett tiltakozási jogával élt az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Ha az adatkezelés korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

Az adatvédelmi tisztviselő az érintettet, akinek a kérésére korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

5. Adathordozhatósághoz való jog

Az érintett jogosult arra, hogy a rá vonatkozó, általa az Intézmény rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa, ha:

- a) az adatkezelés az érintett hozzájárulásán, vagy az érintettel kötendő vagy megkötött szerződésen alapul és



b) az adatkezelés automatizált módon történik.

Az adatok hordozhatóságához való jog gyakorlása során az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását. Az adattovábbításhoz való jog érvényesítésére irányuló igény technikai megvalósíthatóságáról, illetve annak feltételeiről az informatikai osztályvezető dönt és döntéséről tájékoztatja az adatvédelmi tisztviselőt.

Az adatok hordozhatóságához való jog gyakorlása nem sértheti az adatok törléséhez való jog érvényesítését, és nem érintheti hátrányosan mások jogait és szabadságait, különös tekintettel a joggal való visszaélés szabályaira.

Az adatok hordozhatóságához való jog nem érvényesül abban az esetben, ha az adatkezelés közérdekű feladat végrehajtásához szükséges.

6. A törléshez való jog

Az érintett– jogosultsága igazolását követően befogadott – kérelmére az adatkezelést végző szervezeti egység adatvédelmi felelőse az adatvédelmi tisztviselő előzetes tájékoztatása és jóváhagyása mellett indokolatlan késedelem nélkül törli az érintett személyes adatait vagy azoknak az érintett által meghatározott körét, feltéve, hogy az alábbi esetek valamelyike fennáll:

- a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték,
- b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja,
- c) az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,
- d) a személyes adatokat jogellenesen kezelték,
- e) a személyes adatokat az Intézményre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell,
- f) a személyes adatok gyűjtésére az információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

Ha az Intézmény nyilvánosságra hozta a személyes adatot, és a fentiek értelmében azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve az indokolt és szükséges technikai intézkedéseket – a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlése érdekében. Az informatikai és dokumentációs főosztályvezető a technikai lehetőségekről előzetesen tájékoztatja az adatvédelmi tisztviselőt és haladéktalanul gondoskodik a személyes adatok törléséről.

Az Intézmény a személyes adatok törlését a jogszerű kérelem ellenére sem végezheti el, amennyiben az adatkezelés szükséges:

- a) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából,



- b) a személyes adatok kezelését előíró, az Intézményre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése céljából,
- c) közérdekből végzett feladat végrehajtása céljából,
- d) közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben az adattörlés valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést,
- e) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

7. A tiltakozáshoz való jog

Amennyiben az Intézmény az érintett adatait azon a jogalapon kezeli, miszerint

- a) az adatkezelés közérdekű feladat végrehajtásához szükséges, vagy
- b) az adatkezelés az Intézmény vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges,

úgy az érintett ezen személyes adatok kezelése ellen tiltakozhat, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben az Intézmény a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

A tiltakozáshoz való jog érvényesítésére irányuló érintetti megkeresések vizsgálata és megválaszolása az adatvédelmi tisztviselő kötelezettsége, az adatkezelés tárgya szerint illetékes szervezeti egység adatvédelmi felelősének bevonása mellett.

8. Jogorvoslathoz való jog

Adatkezeléssel kapcsolatos jogainak megsértése esetén az érintett – elsősorban az adatkezelést végző szervezeti egység adatvédelmi felelőse útján vagy közvetlenül – az adatvédelmi tisztviselőhöz fordulhat, aki a panaszt megvizsgálja, és ha azt megalapozottnak találja, az adatkezelő szervezeti egységet irányító szakmai igazgatónál intézkedést kezdeményez, ellenkező esetben a panaszt elutasítja. Amennyiben az érintett panaszát nem közvetlenül az illetékes adatvédelmi felelős vagy az adatvédelmi tisztviselő útján teszi meg, úgy a panaszt haladéktalanul továbbítani kell az adatvédelmi tisztviselő részére.

Az Intézmény a panasz elutasításáról a panaszost a kérelem kézhezvételét követő 30 napon belül írásban tájékoztatja, a kérelem elutasításának ténybeli és jogi



indokait is közölve. A panaszost tájékoztatni kell a bírósági jogorvoslat, továbbá a felügyeleti szervhez fordulás lehetőségéről és módjáról.

Az érintett bejelentéssel élhet a Nemzeti Adatvédelmi és Információszabadság Hatóságnál, valamint lehetősége van személyes adatainak védelme érdekében bírósághoz fordulni, amely az ügyben soron kívül jár el. A per során az Intézményt terheli annak bizonyítása, hogy a sérelmezett adatkezelés a jogszabályi előírásoknak megfelelően történt.

X. Az adatkezelés biztonsága

1. Adatkezelési nyilvántartás, kockázatelemzés, adatbiztonság

A személyes adatok biztonságának biztosítása érdekében az Intézmény felméri és nyilvántartja az általa végzett valamennyi személyes adatkezelési tevékenységet. Az adatkezelési nyilvántartást az adatvédelmi tisztviselő vezeti.

Az adatkezelési nyilvántartás célja az Intézmény, mint adatkezelő adatkezelési tevékenysége átláthatóságának biztosítása, és ezzel a szükségtelen, párhuzamos adatkezelések elkerülése.

Az adatkezelési tevékenységek nyilvántartása alapján az Intézmény a XII. pontban meghatározott módszertan szerint kockázatelemzést végez annak felmérése érdekében, hogy az egyes adatkezelés mely szervezeti egysége által, milyen feltételek szerint valósul meg, illetve az adatkezelés során mely kockázati tényezők milyen mértékű sérelmet, milyen lehetséges adatvédelmi incidenst okozhatnak.

A kockázatelemzést a ténylegesen megvalósuló adatkezelési tevékenység alapján kell elvégezni. A kockázatelemzés célja olyan biztonsági szabályok, valamint intézkedések meghatározása, amelyek az Intézmény működéséhez, tevékenységéhez igazodva hatékonyan biztosítják a személyes adatok megfelelő védelmét.

Az Intézmény az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a személyes adatok kezelésére vonatkozó jogszabályi előírásokkal összhangban történjen. Ilyen intézkedés lehet például:

- a) a személyes adatok álnevesítése és titkosítása,
- b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítása, integritása, rendelkezésre állása és ellenálló képessége,
- c) fizikai vagy műszaki incidens esetén az arra való képessége, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen állítani,
- d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelése, felmérése és értékelése.



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

Az Intézmény megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

Személyes adatot tartalmazó irat nem hagyható olyan helyen, ahol harmadik személy is hozzáférhet. Az ilyen iratok elzárásáról azokban az irodákban, illetve személyzeti helyiségekben is gondoskodni kell, ahol az illetékes iratkezelőkön kívül más, harmadik személy is megfordulhat.

Az adathordozó képek és dokumentációk elhelyezésének-, fizikai védelmének biztonságáról az adatkezelő szervezeti egység vezetője az adatvédelmi felelős bevonása mellett az adatvédelmi tisztviselővel, illetve az információbiztonsági felelőssel egyetértésben dönt.

A szervezeti egységeknél kialakítandó adatkezelési rendszer környezetének védelméről a helyi adottságok figyelembevételével az adatvédelmi felelős közreműködésével az illetékes vezetőknek kell gondoskodni, beleértve az adatsértések megelőzését is.

A manuálisan kezelt személyes adatok elvesztésének megelőzése érdekében eredeti iratokat kizárólag kivételesen, hivatalos ügyintézés, bírósági eljárás, nyomozati eljárás vagy más hatósági eljárás során lehet kiadni, amennyiben az eljárás során a másolat kiadása nem elegendő. A kiadást megelőzően az eredeti iratokról az illetékes szervezeti egységnél történő megőrzés céljára hiánytalan másolatot kell készíteni.

Személyes adatokat ért sérülés vagy megsemmisülés esetén a rendelkezésre álló egyéb adatforrásokból meg kell kísérelni a lehetséges mértékig a károsodott adatok pótlását. A sérült adat pótlására annak a szervezeti egységnek a vezetője felelős, ahol a sérülés bekövetkezett. Az adatpótlásba be kell vonni azon illetékes adatkezelő személyt, aki az adatok rögzítésében közreműködött. A pótolat adatokon a pótlás tényét fel kell tüntetni.

2. Adatvédelmi hatásvizsgálat és előzetes konzultáció

Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az Intézmény az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a



tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetők.

Az Intézmény az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő szakmai tanácsát köteles kikérni.

Az adatvédelmi hatásvizsgálat elvégzését a tervezett adatkezelésért felelős szervezeti egység adatvédelmi felelőse koordinálja. A hatásvizsgálat megállapításait írásban kell rögzíteni. Az elkészült hatásvizsgálati dokumentációt az adatvédelmi tisztviselőnek kell megküldeni, aki azt nyolc munkanapon belül szakmai szempontból véleményezi és szükség esetén beszerzi az információbiztonsági felelős véleményét is. Ha az adatvédelmi felelős úgy ítéli meg, hogy az adatkezelés nem jár magas kockázattal, úgy meg kell indokolnia és dokumentumokkal igazolnia az előzetes hatásvizsgálat mellőzésének okát. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg. Az adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

- természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;
- a személyes adatok különleges kategóriái, vagy büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése; vagy
- nyilvános helyek nagymértékű, módszeres megfigyelése.

A hatásvizsgálat kiterjed legalább:

- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
- az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és
- a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

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.

A hatásvizsgálat módszertanát minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani.

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

- az adatkezelésért felelős szervezeti egységet és a tervezett adatfeldolgozó megjelölését,



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

A hatásvizsgálat második részében ki kell fejteni és meg kell indokolni

- az adatkezelés szükségességének és arányosságának garanciáit,
- az érintett jogait biztosító garanciák érvényesülését.

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

A hatásvizsgálat negyedik része tartalmazza a tervezett adatkezelés értékelését:

- az első, második, valamint a harmadik részben meghatározott szempontok értékelését a tekintetben, hogy azok egyenként megfelelőek, további intézkedésekkel megfelelőek lehetnek, illetve nem megfelelőek;
- a tervezett kiegészítő intézkedések végrehajtásának ütemtervét;
- annak egyértelmű rögzítését, hogy a tervezett adatkezelés valószínűsíthetően magas kockázattal jár-e a természetes személyek jogaira nézve, és ennek alapján az adatkezelés megkezdhető-e, illetve szükség van-e az adatvédelmi felügyeleti hatósággal való konzultációra.

Az Intézmény – a kereskedelmi érdekek vagy a közérdek védelmének vagy az adatkezelési műveletek biztonságának sérelme nélkül – kikérheti az érintettek vagy képviselőik véleményét a tervezett adatkezelésről.

Az Intézmény szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése a korábban lefolytatott adatvédelmi hatásvizsgálatnak megfelelően történik-e.

Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az adatvédelmi tisztviselő konzultál a felügyeleti hatósággal (előzetes konzultáció). Az Intézmény az adatvédelmi tisztviselő útján a felügyeleti hatósággal folytatott konzultáció során a felügyeleti hatóságot tájékoztatja:

- adott esetben az adatkezelésben részt vevő adatkezelő, közös adatkezelők és adatfeldolgozók feladatköreiről, különösen vállalkozáscsoporton belüli adatkezelés esetén;



- a tervezett adatkezelés céljairól és módjairól;
- az érintettek GDPR értelmében fennálló jogainak és szabadságainak védelmében hozott intézkedésekről és garanciákról;
- az adatvédelmi hatásvizsgálatról; és
- a felügyeleti hatóság által kért minden egyéb információról.

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

3. Adatvédelmi incidens, és kezelése

Az adatvédelmi incidensre vonatkozó szabályokat kell alkalmazni az Intézmény által kezelt személyes adatokat érintően bekövetkező valamennyi adatvédelmi incidensre, függetlenül attól, hogy a személyes adatok kezelése papír alapon vagy elektronikusan történik. Az információbiztonsági incidens egyben adatvédelmi incidensnek is minősül, amennyiben az személyes adatokat érint. A jelen szabályzat adatvédelmi incidens kezelésére vonatkozó rendelkezéseinek alkalmazása nem mentesít az elektronikus információs rendszereket érintő biztonsági vagy egyéb események kezelésére vonatkozó szabályok betartása alól, ilyen esetben a jelen szabályzat rendelkezéseit az Informatikai biztonsági szabályzat előírásaival párhuzamosan kell alkalmazni.

Amennyiben az Intézmény nevében eljáró adatkezelő személy akár saját, akár más, az Intézmény nevében végzett adatkezelése körében adatvédelmi incidens megtörténtét észleli, vagy arról szerez tudomást, azt haladéktalanul jeleznie kell az adatvédelmi tisztviselő számára. Az adatvédelmi incidensnek az adatvédelmi tisztviselő felé történő bejelentésére szolgáló űrlapot a szabályzat 2. sz. melléklete tartalmazza. Az incidens bejelentése más, írásbeli módon is történhet, amennyiben az maradéktalanul tartalmazza az űrlapon meghatározott információkat. A bejelentés elmulasztása esetén az észlelő személy felelősséggel tartozik a bejelentés elmulasztásával vagy késedelemével okozott károkért.

Az adatvédelmi incidenst az Intézmény az adatvédelmi tisztviselő útján indokolatlan késedelem nélkül, legkésőbb 72 órával az után, hogy az adatvédelmi incidens észlelésre került, bejelenti az adatvédelmi felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, a bejelentéshez mellékelni kell a késedelem igazolására szolgáló indokokat is.

Az adatvédelmi felügyeleti hatóság felé történő bejelentésben legalább:

- ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- feltüntetni a bejelentő nevét és elérhetőségét;
- közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;



- ismertetni kell az Intézmény által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

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

Adatvédelmi incidens bekövetkezése esetén az Intézmény adatvédelmi tisztviselője a jogi feladatokkal megbízott főigazgató-helyettes, a jogi iroda és szükség esetén az informatikai osztály, vagy más érintett szervezeti egység kijelölt munkatársának (a továbbiakban együttesen: incidensvizsgáló bizottság) közreműködésével megvizsgálja, és a súlyosságának megfelelően kategorizálja a bekövetkezett incidenst és meghatározza az esetleges elhárítás érdekében szükséges további intézkedéseket. Az incidensvizsgáló bizottságot az adatvédelmi tisztviselő hívja össze. Az incidensvizsgáló bizottság munkáját az adatvédelmi tisztviselő koordinálja, és képviseli az Intézmény egyéb szervezeti egységei felé. Az incidensvizsgáló bizottság üléseiről írásbeli jegyzőkönyvet, vizsgálatáról pedig intézkedési javaslatokat is tartalmazó írásbeli jelentést kell készíteni. Az incidensvizsgáló bizottság szükség esetén ülés tartása nélkül, írásbeli nyilatkozatok megtétele útján jár el.

A bekövetkezett incidens előzetes vizsgálata során az alábbi szempontokat szükséges figyelembe venni:

- a bejelentés személyes adatot érint-e,
- amennyiben a bejelentés személyes adatot érint, megállapítható-e a személyes adatok köre,
- megállapítható-e az incidensben érintett személyek köre,
- a hatályos jogszabályok és belső szabályok alapján megállapítható-e, hogy személyes adat jogellenes kezelése vagy feldolgozása történt,
- az incidens valószínűsíthetően magas kockázattal jár-e az érintettek jogaira és szabadságaira nézve,
- melyek az adatvédelmi incidensből eredő, valószínűsíthető következmények,
- az Intézmény által alkalmazott technikai és szervezési védelmi intézkedések alkalmasak-e arra, hogy az incidensben érintett személyes adatokhoz való hozzáférésre nem jogosult személyek számára értelmezhetetlenné tegyék az adatokat (pl. álnevesítés útján).

Az incidensvizsgáló bizottság az incidens kockázati besorolását az eset összes körülményének vizsgálatát követően állapítja meg. Ennek során az alábbi szempontokat veheti figyelembe:

- magas kockázatúnak minősül az az incidens, amely vagyoni vagy nem vagyoni károkat okozhat az érintetteknek, az érintettek elvesztik a személyes adataik feletti rendelkezés jogát, fennáll annak a reális lehetősége, hogy az incidens hátrányos megkülönböztetést, személyazonosság-lopást vagy személyazonossággal való visszaélést eredményezhet, a jó hírnév sérelmével jár, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését



eredményezheti, az olyan adatsérülés és adatvesztés, amely esetében az adatok helyreállítása nem lehetséges, stb.

- alacsony kockázatúnak minősül az az incidens, amely az érintettek jogaira és szabadságaira nézve reális kockázatot nem jelent, pl. az Intézmény munkavállalói által használt belső rendszerekben bekövetkező adatsérüléssel vagy adatvesztéssel nem járó átmeneti szolgáltatás kiesés, amely rövid idő alatt helyreállítható, vagy a rendszer, adathordozó sérülése, megsemmisülése miatt bekövetkező adatsérülés vagy adatvesztés, amely különösebb nehézség nélkül, rövid időn belül helyreállítható.

Az incidensvizsgáló bizottság – az adatvédelmi tisztviselő útján – az előzetes vizsgálat eredményéről, a GDPR 33. cikkében írt hatósági bejelentés szükségességéről, valamint arról, hogy szükséges-e az incidens részletes vizsgálata, legkésőbb az incidensről való tudomásszerzés időpontját követő egy napon belül írásban tájékoztatja:

- a főigazgatót;
- informatikai rendszert is érintő incidens esetén az informatikai biztonságvédelmi felelőst és az ÉKC stratégiai főigazgató-helyettest;
- az illetékes főigazgató-helyettest,
- az érintett szervezeti egység vezetőjét.

Az incidensvizsgáló bizottság javaslata alapján a főigazgató legkésőbb a bejelentésre rendelkezésre álló 72 órás határidő leteltét megelőzően dönt a GDPR 33. cikkében írt hatósági bejelentés szükségességéről.

Az adatvédelmi incidens részletes vizsgálatának szükségességéről az incidensvizsgáló bizottság dönt és a részletes vizsgálatot a vizsgálat megkezdésének napjától számított 15 munkanapon belül le kell zárni.

A vizsgálat során elsősorban az alábbi módszerek alkalmazhatóak:

- személyes megbeszélés az adatvédelmi incidensben érintett személyekkel, valamint az érintett szervezeti egységek munkatársaival és vezetőivel,
- írásbeli tájékoztatás kérése az érintett szervezeti egységektől vagy személyektől,
- dokumentumok vizsgálata,
- informatikai rendszerek vizsgálata.

Amennyiben az incidensvizsgáló bizottság a részletes vizsgálat során úgy ítéli meg, hogy azonnali intézkedések szükségesek annak biztosítására, hogy az incidens bekövetkezéséhez vezető okból eredő újabb incidens ne valósuljon meg, úgy a szükséges intézkedések megtétele érdekében haladéktalanul tájékoztatja az érintett szervezeti egységek vezetőit.

Az incidensvizsgáló bizottság legkésőbb a vizsgálat megkezdését követő tizenöt munkanapon belül vizsgálati jelentést készít. A vizsgálati jelentés tartalmazza az adatvédelmi incidens elhárításához és további incidens megelőzéséhez szükséges intézkedésekre vonatkozó, az illetékes vezető részére tett javaslatot.

A jelentés alapján a vizsgálatban érintett szervezeti egységek vezetői tizenöt napon belül intézkedési tervet készítenek és megküldik az adatvédelmi tisztviselőnek.



Az intézkedési tervet és a megvalósításhoz szükséges határidőt tartalmazó szakterületi javaslatot az incidensvizsgáló bizottság jóváhagyásra megküldi a főigazgató részére.

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

Az adatvédelmi tisztviselő elektronikusan nyilvántartja az adatvédelmi incidenseket, feltüntetve különösen az alábbiakat:

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

Az Intézmény az incidens kivizsgálásával kapcsolatos papíralapú és elektronikus dokumentumokat tíz évig köteles megőrizni, amennyiben az iratkezelési szabályzat ennél hosszabb őrzési időt nem állapít meg. Az adatvédelmi incidensek vizsgálata során keletkezett iktatott dokumentumokat az igazgatósági titkárság az incidens vizsgálatának lezárásától számított tíz évig őrzi meg, illetéktelenek számára hozzá nem férhető, zárt helyen.

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Intézmény – elsősorban az adatvédelmi tisztviselő útján – indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a következő információkat és intézkedéseket:

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

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

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



- az Intézmény az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg,
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

Abban az esetben, ha az érintettek elérhetősége nem áll rendelkezésre vagy az érintettek pontosan meg nem határozható körére tekintettel a közvetlen tájékoztatás nem lehetséges, a főigazgató döntése alapján az Intézmény az érintetteket – a kommunikációért felelős munkatársútján – az Intézmény honlapján, vagy országos lefedettségű sajtótermékben közzétett hirdetés útján is értesítheti.

Az adatvédelmi incidensre tekintettel meghozott intézkedések végrehajtását követően az Intézmény felméri az intézkedések hatékonyságát, szükség esetén az érintett adatkörben újabb kockázatelemzést végez.

4. Belső adatvédelmi ellenőrzési eljárás

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

Az adatvédelmi tisztviselő éves ellenőrzési tervet készít. Az éves ellenőrzési tervnek az ellenőrzés alá vont szervezeti egység nevét és az ellenőrzés megkezdésének várható időpontját, továbbá az ellenőrzés tárgykörét kell tartalmaznia. Az éves ellenőrzési terveket úgy kell elkészíteni, hogy négyéves időtartam alatt lehetőség szerint minden igazgatóság és a főigazgatónak közvetlenül alárendelt szervezeti egység ellenőrzésére sor kerüljön. Az éves ellenőrzési tervet legkésőbb a tárgyév február 28. napjáig kell elkészíteni és a főigazgató részére bemutatni. Az éves ellenőrzési tervet a főigazgató hagyja jóvá.

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

Az ellenőrzés során az adatvédelmi tisztviselő a szervezeti egység munkavégzésre szolgáló helységeibe beléphet, a szervezeti egység – ellenőrzés tárgyával összefüggésben kezelt – irataiba betekinthet, a szervezeti egység munkatársaitól tájékoztatást, felvilágosítást kérhet az adott üggyel kapcsolatos adatkezelésről.

Az adatvédelmi 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 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 tervezetere a szervezeti egység vezetője tíz napon belül észrevételt tehet. Az észrevételezés elmaradása a szervezeti egység vezetőjének egyetértését jelenti.

Ha az adatvédelmi 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 tisztviselő rendkívüli ellenőrzést is lefolytathat, 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 a főigazgató előzetesen engedélyezi.

Az adott ellenőrzéssel kapcsolatban a főigazgató külön tájékoztatást kérhet az adatvédelmi tisztviselőtől, egyébként az adatvédelmi tisztviselő évente egy alkalommal, legkésőbb a tárgyévét követő év február 28. napjáig összefoglaló jelentést készít az általa a tárgyévben lefolytatott ellenőrzésekről, amelyet a főigazgató részére köteles megküldeni.

XI. Adattovábbítás szabályai

Az Intézmény szervezeti rendszerén belül a személyes adatok – a feladat elvégzéséhez szükséges mértékben és ideig – olyan szervezeti egységhez, személyhez továbbíthatók, amelynek az Intézménynél végzett feladatának ellátásához a személyes adatok megismerése és kezelése szükséges.

Az Intézménynél különböző célra irányuló adatkezelések csak törvényes céloknak megfelelően, indokolt esetben kapcsolhatók össze.

Olyan megkeresés, amely az Intézmény által kezelt személyes adat továbbítására irányul, csak jogszabályi előírás alapján, az adattovábbításhoz megfelelő jogalap és adatkezelési cél fennállása esetén, vagy a fenti feltételek fennállása esetén teljesíthető. Minden más esetben az adattovábbítás teljesítését meg kell tagadni.

Harmadik országba irányuló adattovábbítás esetén az adattovábbítást végzőnek külön meg kell győződnie arról, hogy a külföldre történő adattovábbítás GDPR-ban előírt feltételei fennállnak-e. Ennek kapcsán vizsgálandó, hogy az adattovábbítás a GDPR-ban meghatározott valamely jogalaphoz megfelelően történik-e, és az adatok megfelelő védelmi szintje az adatokat átvevő adatkezelőnél biztosított-e. Ha az adattovábbítás az Európai Gazdasági Térség valamely tagállamába irányul, úgy a személyes adatok megfelelő szintű védelmét nem kell vizsgálni.



Harmadik országba történő adattovábbítás esetén az érintett szervezeti egység köteles az adatvédelmi tisztviselő véleményét kérni az adattovábbítás lehetséges szükségességéről, megengedhetőségéről, illetve az adattovábbítás lehetséges módjáról. Az adatvédelmi tisztviselő – szükség esetén a jogi feladatok ellátásáért felelős főigazgató-helyettes és az informatikai és dokumentációs főosztály vezető állásfoglalásának ismeretében – javaslatot tesz az adattovábbítás módjára, az adatátadás során alkalmazandó biztosítékok körére.

Olyan személyes adatok továbbítására – ideértve a személyes adatok harmadik országból vagy nemzetközi szervezettől egy további harmadik országba vagy további nemzetközi szervezet részére történő újbóli továbbítását is –, amelyeket harmadik országba vagy nemzetközi szervezet részére történő továbbításukat követően adatkezelésnek vetnek alá vagy szándékoznak alávetni, csak abban az esetben kerülhet sor, ha az adatkezelő és az adatfeldolgozó egyaránt teljesíti a GDPR-ban rögzített feltételeket.

Személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására sor kerülhet, ha az Európai Bizottság megállapította, illetve az Európai Unió Hivatalos Lapjában és annak honlapján közzétette, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít (megfelelőségi határozat). Az ilyen adattovábbításhoz nem szükséges külön engedély.

Személyes adatok továbbítása során, amennyiben az postai küldeményként történik, biztosítani kell, hogy a küldemény zártan kerüljön feladásra.

Az Intézmény vállalja, hogy a személyes adatokat statisztikai célra kizárólag olyan formában adja át, amely az érintett azonosítására nem alkalmas.

XII. Az adatvédelmi kockázatelemzés szabályai

Az adatvédelmi kockázatelemzés az adatkezelési folyamatok során felmerülő kockázatok meghatározására szolgál, a kockázati tényezők meghatározását, azok értékelését, a kockázatokra adott válaszreakciókat és a kockázatok felülvizsgálatát foglalja magában. Megfelelő kockázatkezelési tevékenység révén az Intézmény csökkentheti az adatvédelmi jellegű kockázatok hatásait, illetve megelőzheti a feltárt kockázatok tényleges bekövetkezését.

A kockázatkezeléssel kapcsolatos tevékenységek sorrendben az alábbiak:

1. A kiemelt kockázati tényezők beazonosítása, feltárása, amelyek az Intézmény működését, kiemelt céljainak elérését veszélyeztetik, valamint az azokhoz kapcsolható keretek meghatározása.
2. A kockázatok elemzése, rangsorolása jellegük, felmerülési helyük, hatásuk súlyossága és bekövetkezési valószínűségük szerint, a kockázatok értékelése (a kockázatok kvalitatív elemzése, a kritikus tényezők kiválasztása, ennek eredménye alapján a kockázatok kvantitatív elemzése).
3. Az elfogadható kockázati szint meghatározása. Az Intézmény egészére, valamint azon belül az egyes szervezeti egységekre vonatkozó ún.



„tűrőhatárok” meghatározása, amelyek felett intézkedéseket kell fogantatosítani.

4. A beazonosított és relevánsnak minősített kockázatokhoz kapcsolódó, azok lehetséges csökkentése vagy megszüntetése érdekében javasolt intézkedések azonosítása.
5. A kritikus tényezők kezelésére kockázatkezelő javaslatok megfogalmazása, döntés a kockázatok kezeléséről: a kockázatok, illetve hatásukat milyen módon kívánja a vezetés mérsékelni, elkerülni, és/vagy bekövetkezési valószínűségüket csökkenteni.
6. A válaszintézkedés beépítése, az adatvédelmi kockázatkezelési tevékenység folyamatának felülvizsgálata.

Az Intézmény adatvédelmi szabályzata része az Intézmény belső kontrollrendszerének, és tartalmazza mindazon elveket, eljárásokat és belső szabályzatokat, amelyek alapján az Intézmény érvényesíti az általa kezelt valamennyi személyes adat védelmét és az adatkezelés során alkalmazott adatvédelmi rendszerek és rendszerelemek hatékony működtetését.

Az adott szervezeti egység által végzett adatkezelési folyamatok keretében felmerülő kiemelt kockázati tényezők beazonosítása, feltárása, valamint a kockázatok elemzése, rangsorolása és értékelése az illetékes adatvédelmi felelős vagy felelősök kötelezettsége.

A kockázatelemzést az adatkezelési tevékenység bevezetését vagy módosítását megelőzően, illetve amennyiben ez nem lehetséges, az adatkezelés megkezdését követően haladéktalanul köteles elvégezni. A kockázatelemzést minden negyedik év október 31. napjáig felül kell vizsgálni. Az adatvédelmi felelősök által összeállított kockázatelemzést az adatvédelmi tisztviselő hagyja jóvá.

A költségvetési szerv vezetésének a kockázatokra való reagálását döntő mértékben határozza meg a kockázatok bekövetkezésének gyakorisága, és a költségvetési szervre gyakorolt hatása. Emiatt válik fontossá, hogy minden egyes kockázat tekintetében meghatározásra kerüljön az Intézményre gyakorolt hatásának mértéke és a bekövetkezés gyakorisága, mivel e két tényező együttes értékelésével alakítható ki a kockázatok rangsora, és az a módszer, illetve gyakorlat, amely alkalmas a kockázatok kezelésére.

A kockázatfelmérést követő lépés az azonosított kockázati tényezők értékelése, amely a legjobban áttekinthető módon a kockázatelemzési kritérium mátrix (KKM) elkészítésével oldható meg. A KKM az Intézmény folyamataira vonatkozó, következetes kockázatelemzés végrehajtásának elsődleges eszköze, amelynek segítségével meghatározható a vizsgált folyamat kockázatosága. A mátrix alapja, hogy minden kockázat alapvetően két kritérium alapján értékelhető

- a bekövetkezési valószínűség és
- a szervezet céljaira gyakorolt negatív hatás alapján.

Az értékelés következetességét a KKM biztosítja, mert egy azonosított kockázat hatásának megítélésére számszerűsíthető értéket ad, amelynek alapján a kockázatok magas, közepes és alacsony hatású kategóriába lehet sorolni.

Kockázatok értékelése a kockázat jellemzői szerint:



- kockázat hatása (KH)
- kockázat bekövetkezésének valószínűsége (KV)
- a kockázat értéke (KÉ)

A kockázatok azonosítását követően a kockázat valószínűsége (KV) és a kockázat hatása (KH) szerint tételesen értékelni kell azokat, majd az értékelés alapján meg kell határozni a kockázati értéket (KÉ) az alábbiak szerint:

$$\begin{aligned} A \text{ kockázat értéke (KÉ)} &= \\ &= \text{kockázat valószínűsége (KV)} * \text{kockázat hatása (KH)} \\ KÉ &= KV * KH \end{aligned}$$

A kockázat bekövetkezésének valószínűsége (KV):

A becslést egyedi események esetén az előfordulás gyakorisága vagy a kockázati esemény előfordulási valószínűségi %-a (kockázat becsült gyakorisága az esemény gyakoriságához viszonyítva) szerint kell elvégezni.

KV értéke	Esemény gyakorisága	Előfordulás valószínűsége
1.	1 évnél ritkább	0,01 % alatt
2.	évente	0,01-0,1%
3.	havonta	0,1-1%
4.	hetente	1-10%
5.	naponta	10% felett

A kockázat hatása (KH):

Az értékelés során azt kell figyelembe venni, hogy a kockázati esemény bekövetkezése esetén az milyen hatással van a szervezetre nézve.

KH értéke	Hatás leírása
1.	Kis munkával, alacsony költséggel helyreállítható, jogszabályt nem sértő, munkavégzést nehezíti, de nem akadályozza.
2.	Többször erőforrás bevonását igényli, de a funkciók ellátását nem akadályozza meg, munkavégzést nehezíti.
3.	Egyes határidők, követelmények nem teljesülnek, anyagi károkat okozhat.
4.	Kárt okoz (akár anyagi is), funkció ellátását akadályozza, a szervezet hírnevét befolyásolja.
5.	Jelentős (akár anyagi) kárt okoz, alapfunkció nem működik, a szervezet hírnevét súlyosan befolyásolja, ellene jogi lépések, perek indulhatnak.



Elfogadható kockázati szint (tűrőhatár) meghatározása

A kockázati tűrőhatárt a sorba rendezett kockázati értékek (KÉ) alapján kell meghatározni, amely során a kockázatokat két csoportba kell osztani:

1. nem elfogadható kockázatok: (a KÉ kockázati tűrőhatár feletti kockázatok) minden ilyen esetben kockázatsökkentő intézkedésről kell dönteni;
2. elfogadható, szinten tartható kockázatok: (a KÉ kockázati tűrőhatár alatti kockázatok) a kockázatokat és a megtett intézkedéseket felügyelet alatt kell tartani azért, hogy a kockázat ne növekedjen, de új intézkedést nem kötelező alkalmazni a kezelésükre.

A kockázati tűrőhatár a kockázati kitettségnek azt a szintjét jelenti, ami felett a szervezet mindenképpen válaszigintézkedést tesz a felmerülő kockázatokra. Minél kevésbé elfogadható az Intézmény számára egy kockázat bekövetkezése, annál nagyobb hangsúlyt kell fektetni a válaszlépések megtételére. A legmagasabb prioritású kockázati tényezőket szükségeszerű folyamatosan figyelni, és az Intézmény vezetésének magasabb szintjein foglalkozni velük.

Fontos, hogy a tűrőhatárok a szervezet minden szintjén ismertté váljanak, és az érintettek azonosuljanak velük, mert ez biztosítja az alapot a releváns kockázatok mennyiségi és minőségi méréséhez, valamint a szükséges válaszlépések meghozatalához. A kockázattűrő képesség meghatározása meglehetősen szubjektív, azonban a megfelelő kockázati stratégia kialakításának elengedhetetlen feltétele.

A kockázati tűrőhatárhoz szorosan kapcsolódik a „tolerancia szint”, ami azt a százalékos (esetleg abszolút számban kifejezett) mértéket jelenti, amilyen mértékű plusz-mínusz irányú eltérést az Intézmény még megengedhetőnek tart az eredetileg kitűzött céltól. Ezt a kockázati tűrőhatárt a főigazgató határozza meg. A feltárt kockázattal kapcsolatos reakciókat az adott szervezet által elviselhetőnek ítélt kockázati szint meghatározásával együtt kell eldönteni. Az ezt a szintet meghaladó kockázatokra intézkedéseket kell hozni.

A kockázati tűrőhatár felett elhelyezkedő minden egyes kockázat esetében a válaszlépésnek tükröznie kell a szervezet vezetési filozófiáját, tolerancia szintjét, valamint a közérdek képviselését. A vezetésnek a válaszlépés melletti döntés meghozatalakor figyelemmel kell lennie arra, hogy az adott kockázat

- milyen mértékű hatást gyakorol az Intézményre; és
- a célhierarchia melyik szintjét érinti.

A szervezeten belül a kockázatok nyilvántartásáért az adatvédelmi felelősök által szolgáltatott adatok alapján az adatvédelmi tisztviselő felelős.

KÜLÖNÖS RÉSZ

XIII. Betegek adatainak kezelése, nyilvántartása



1. Az egészségügyi adatok kezelésének és védelmének alapvető intézményi szabályai

Az adatvédelmi jog rendszerében a különleges személyes adatnak minősülő egészségügyi adat – jellegéből adódóan – különös védelmet igényel. Ennek megfelelően a személyes adatok védelmére vonatkozó jogszabályok az általánostól eltérő, szigorúbb szabályokat állapítanak meg az egészségügyi adatok kezelésére vonatkozóan.

Az egészségügyi adatok kezelése során az Intézmény nevében egészségügyi adatokat kezelő vagy feldolgozó valamennyi személy köteles betartani a GDPR, az Infotv. az Eüak. és más ágazati jogszabályok, továbbá a jelen szabályzat rendelkezéseit.

Az egészségügyi adatok körébe tartozik mindazon információ, amely

- a beteg testi, értelmi vagy lelkiállapotára, kóros szenvedélyére, a megbetegedés vagy elhalálozás körülményeire, okaira vonatkozik,
- a beteg gyógykezelése, ellátása során a kezelőorvos vagy az egészségügyi ellátás nyújtásában részt vevő más személy állapít meg vagy észlel, illetve a beavatkozások, vizsgálatok elvégzése során tudomására jut,
- az előzőekben foglaltakkal kapcsolatba hozható, így például a beteget érő környezeti hatások, a beteg magatartása, foglalkozása, családi körülményei stb.

Az egészségügyi adatok kezelése során az Intézmény kiemelt biztonsági intézkedéseket tesz és biztosítja, hogy azokhoz kizárólag jogoszerű célból, a feladat ellátásához szükséges mértékben és ideig férjenek hozzá. Az Intézményen belül az egészségügyi és személyazonosító adat kezelésére - amennyiben az Eüak. másként nem rendelkezik – jogosult a betegellátó, a főigazgató, valamint az adatvédelmi tisztviselő.

2. Adatkezelés célja

A betegek adatainak kezelésére sor kerülhet:

- az egészség megőrzésének, fenntartásának előmozdítása,
- az eredményes gyógykezelés elősegítése,
- az érintett egészségi állapotának nyomon követése,
- a közegészségügyi és járványügyi érdekből szükségessé váló intézkedések megtétele,
- a betegjogok érvényesítése céljából, valamint
- megfelelő jogalap fennállása esetén más törvényes célból.

A betegek adatainak kezelésére sor kerülhet továbbá törvényben meghatározott esetekben az Eüak. 4. § (2) bekezdésében meghatározott célokból.

3. Titoktartási kötelezettség

A beteg egészségi állapotával kapcsolatos adat és személyes adat időbeli korlátozás nélkül titoktartási kötelezettség alá esik, függetlenül attól, hogy az adatok milyen módon váltak megismerhetővé.



A titoktartási kötelezettség a szabályzat személyi hatálya alá tartozó valamennyi személyre irányadó, nem korlátozódik a beteg egészségügyi ellátásában részt vevő dolgozókra. A titoktartási kötelezettség a betegellátót – a gyógykezelt személy választott háziorvosa, valamint az igazságügyi orvos szakértő kivételével – azzal a betegellátóval szemben is köti, aki a beteg gyógykezelésében nem működött közre, kivéve, ha az adatok az érintett személy további gyógykezelése érdekében szükségesek. A titoktartás alól kizárólag jogszabály vagy az érintett, illetve törvényes képviselője adhat felmentést.

Amennyiben a betegről készült egészségügyi dokumentáció más személy magántitokhoz való jogát érintő adatokat is tartalmaz, annak csak a betegre vonatkozó része tekintetében gyakorolható a betekintési, illetve egyéb jogosultság.

A beteg jogosult arra, hogy az egészségügyi ellátásában részt vevő személyek az ellátása során tudomásukra jutott információkat, különösképpen a beteg egészségügyi és személyes adatait csak az arra jogosulttal közöljék, és azokat a vonatkozó jogszabályok szerint kezeljék (a továbbiakban: orvosi titok).

A betegnek joga van arról nyilatkozni, hogy betegségéről, annak várható kimeneteléről kiknek adható felvilágosítás, illetve kiket zár ki egészségügyi adatainak részleges vagy teljes megismeréséből.

Az érintett beteg egészségügyi adatait annak hozzájárulása hiányában is közölni kell, amennyiben ezt törvény elrendeli vagy mások életének, testi épségének és egészségének védelme szükségessé teszi.

Az érintett beteg hozzájárulása nélkül a beteg további ápolását, gondozását végző személlyel közölni lehet azokat az egészségügyi adatokat, amelyek ismeretének hiánya a beteg egészségi állapotának károsodásához vezethet.

A betegnek joga van megnevezni azt a személyt, akit fekvőbeteg-gyógyintézetbe történő elhelyezéséről, egészségi állapotának alakulásáról értesíthetnek, illetve joga van bármely személyt ebből kizárni. A beteg által megnevezett személyt a fekvőbeteg-gyógyintézet köteles értesíteni a beteg elhelyezéséről és annak megváltoztatásáról, valamint egészségi állapotának jelentős mértékű változásáról.

Cselekvőképtelen beteg dokumentációjába való betekintési jog az Eütv. 16. § (1) és (2) bekezdése szerinti személyt, azaz törvény eltérő rendelkezése hiányában cselekvőképes állapotban közokiratban, teljes bizonyító erejű magánokiratban, vagy írásképtelensége esetén két tanú együttes jelenlétében megtett nyilatkozattal megnevezett személyt, ilyen személy hiányában a megjelölt sorrend szerint az alábbi személyeket illeti meg:

- a) a beteg törvényes képviselőjét, ennek hiányában
- b) a beteggel közös háztartásban élő, cselekvőképes
 - ba) házastársát vagy élettársát, ennek hiányában
 - bb) gyermekét, ennek hiányában
 - bc) szülőjét, ennek hiányában
 - bd) testvérét, ennek hiányában
 - be) nagyszülőjét, ennek hiányában
 - bf) unokáját;



c) a b) pontban megjelölt hozzátartozója hiányában a beteggel közös háztartásban nem élő, cselekvőképés

- ca) gyermekét, ennek hiányában
- cb) szülőjét, ennek hiányában
- cc) testvérét, ennek hiányában
- cd) nagyszülőjét, ennek hiányában
- ce) unokáját.

A korlátozottan cselekvőképés kiskorú és cselekvőképességében az egészségügyi ellátással összefüggő jogok gyakorlása tekintetében részlegesen korlátozott személy dokumentációjába való betekintési jog a beteget, az Eütv. 16. § (1) bekezdés a) pontja szerint megnevezett személyt, azaz törvény eltérő rendelkezése hiányában, cselekvőképés állapotban, közokiratban, teljes bizonyító erejű magánokiratban, vagy írásképtelensége esetén két tanú együttes jelenlétében megtett nyilatkozattal megnevezett személyt, ilyen személy hiányában a törvényes képviselőt illeti meg.

A beteg cselekvőképés állapotban, közokiratban, teljes bizonyító erejű magánokiratban, vagy írásképtelensége esetén két tanú együttes jelenlétében megtett nyilatkozatával bármely, a fentiek szerint az egészségügyi adatainak megismerésére jogosult személyt kizárhat, ennek tényét a betegdokumentációban megfelelően rögzíteni kell. A beteg ezen nyilatkozata nem érinti az egészségügyi adatok megismerésére jogszabály alapján önállóan jogosult, kizárt személy megismerési, betekintési, másolatkészítési jogát.

A beteg jogosult az adott betegségével kapcsolatos egészségügyi ellátásának ideje alatt az általa meghatározott személyt írásban felhatalmazni a rá vonatkozó egészségügyi dokumentációba való betekintésre, illetve arra, hogy azokról másolatot készíttessen.

A beteg egészségügyi ellátásának befejezését követően csak a beteg által adott teljes bizonyító erővel rendelkező magánokiratban felhatalmazott személy jogosult az egészségügyi dokumentációba való betekintésre, és arról másolat készítésére.

A beteg életében, illetőleg halálát követően házastársa, egyeneságbeli rokona, testvére, valamint élettársa - írásos kérelme alapján - akkor is jogosult az egészségügyi adat megismerésére, ha az egészségügyi adatra a házastárs, az egyeneságbeli rokon, a testvér, illetve az élettárs, valamint leszármazóik életét, egészségét befolyásoló ok feltárása, illetve ezen személyek egészségügyi ellátása céljából van szükség; és az egészségügyi adat más módon való megismerése, illetve az arra való következtetés nem lehetséges. Ilyen esetben csak azoknak az egészségügyi adatoknak a megismerése lehetséges, amelyek ezen okkal közvetlenül összefüggésbe hozhatók. Az egészségügyi adatokra vonatkozó tájékoztatást a beteg kezelőorvosa, illetve az orvosigazgató adja meg, az orvosi tájékoztatásra vonatkozó előírásoknak megfelelően, - szükség esetén - a kérelmező kezelőorvosával való szakmai konzultáció alapján.

A beteg halála esetén törvényes képviselője, közeli hozzátartozója, valamint örököse - írásos kérelme alapján - jogosult a halál okával összefüggő vagy összefüggésbe hozható, továbbá a halál bekövetkezését megelőző gyógykezeléssel kapcsolatos egészségügyi adatokat megismerni, az egészségügyi dokumentációba



betekinteni, valamint azokról kivonatot, másolatot készíteni vagy saját költségére másolatot kapni.

4. Adatkezelés a betegfelvétel során

A beteg egészségügyi ellátásának megkezdését megelőzően tájékoztatni kell a beteget a kezelt adatok köréről, az adatkezelés céljáról, időtartamáról, az esetleges adattovábbításról, valamint az adatkezeléssel összefüggő minden lényeges körülményről.

A betegek adatainak kezelésével kapcsolatos általános tájékoztatást az Intézmény bárki számára elérhető módon elérhetővé teszi a honlapján, továbbá papír alapon minden betegellátó osztályon.

Amennyiben az eset összes körülményeire figyelemmel az Intézmény által biztosított általános tájékoztatás nem alkalmas az érintett megfelelő tájékoztatására – így különösen az érintett beteg fogyatékossága miatt –, a szükséges, érintett számára érthető tájékoztatás biztosításáért a beteg kezelőorvosa tartozik felelősséggel.

A betegfelvétel során a betegfelvételt végző köteles a beteg azonosítását elvégezni és a beteg jogszabályok által meghatározott személyazonosító és személyes adatait és egészségügyi dokumentációban rögzíteni. Jogszabály kifejezett előírása hiányában a személyazonosító okiratok másolatának őrzése tilos.

5. Adatkezelés a betegellátás során

Az egészségügyi adatok felvétele a gyógykezelés része. A kezelés során dokumentálásra kerülnek a kötelezően rögzítendő személyes és személyazonosító adatok, továbbá a feladat ellátásához szükséges mértékű és a betegellátás során keletkező egészségügyi adat.

A felvett személyes adatok rögzítője, illetve kezelője mindenkor egyértelműen azonosítható kell legyen.

Az egészségügyi és a személyazonosító adatoknak az érintett részéről történő szolgáltatása - az egészségügyi ellátás igénybevételéhez kötelezően előírt személyazonosító adatok és az Eüak. 13. §-ban foglaltak kivételével - önkéntes. Abban az esetben, ha az érintett önként fordul az egészségügyi ellátóhálózathoz, a gyógykezeléssel összefüggő egészségügyi és személyazonosító adatainak kezelésére szolgáló hozzájárulását - ellenkező nyilatkozat hiányában - megadottnak kell tekinteni, és erről az érintettet (törvényes képviselőjét) tájékoztatni kell. 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,

- ha valószínűsíthető vagy beigazolódott, hogy az Eüak. 1. számú mellékletben felsorolt valamely betegség (pl. influenza, lyme-kór, veszettség, SARS-koronavírus stb.) kórokozója által fertőződött, vagy fertőzőes eredetű mérgezésben, illetve fertőző betegségben szenved,



- kivéve, ha az érintett annak megállapítása érdekében, hogy HIV vírusával fertőződött-e - személyazonosságának előzetes felfedése nélkül - szűrővizsgálaton kíván részt venni,
- ha arra az Eüak. 2. számú mellékletben felsorolt szűrő- és alkalmassági vizsgálatok (pl. munkaköri, szakmai, egészségi alkalmassági orvosi vizsgálatok, katonai egészségi alkalmasság, közúti járművezetésre való alkalmasság megállapítására irányuló vizsgálatok stb.) elvégzéséhez van szükség,
 - heveny mérgezés esetén,
 - ha valószínűsíthető, hogy az érintett az Eüak. 3. számú melléklet szerinti foglalkozási eredetű megbetegedésben szenved (pl. szilikózis, asbesztózis stb.),
 - ha az adatszolgáltatásra a magzat, illetve a kiskorú gyermek gyógykezelése, egészségi állapotának megőrzése vagy védelme érdekében van szükség,
 - ha bűnüldözés, bűnmegelőzés céljából, továbbá ügyészségi, bírósági eljárás, illetve szabálysértési vagy közigazgatási hatósági eljárás során az illetékes szerv a vizsgálatot elrendelte,
 - ha az adatszolgáltatásra a nemzetbiztonsági szolgálatokról szóló törvény szerinti ellenőrzés céljából van szükség.

A felvett adatoknak hitelesnek, pontosnak, teljesnek és időszerűnek kell lenniük. A személyazonosító adatok (pl. név, születési idő, TAJ szám) felvétele a hatósági igazolványok megtekintése, az egyéb személyes adatok (pl. kórelőzmény, hozzátartozói minőség) az érintett által biztosított okiratok, dokumentumok vagy a beteg elmondása alapján történik, a gyógykezeléssel kapcsolatos személyes adatokat a beteg kezelésében részt vevők rögzítik. A diagnózis és a kapcsolódó kódok ellenőrzése az adatbevitellel egyidejűleg kell, hogy megtörténjen.

A betegnek joga van ahhoz, hogy vizsgálata és gyógykezelése során csak azok a személyek legyenek jelen, akiknek részvétele az ellátásban szükséges, illetve azok, akiknek jelenlétéhez a beteg hozzájárult, kivéve, ha törvény másként nem rendelkezik, joga van továbbá ahhoz, hogy vizsgálatára és kezelésére olyan körülmények között kerüljön sor, hogy azt beleegyezése nélkül mások ne láthassák, illetve ne hallhassák, kivéve, ha a sürgős szükség és a veszélyeztető állapot esetén ez elkerülhetetlen.

A gyógykezelés során a kezelést végző orvoson és az egyéb betegellátó személyeken kívül csak az lehet jelen, akinek 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 hivatásos állományú tagja, amennyiben a gyógykezelésre fogvatartott személy esetében kerül sor,
- c) a büntetés-végrehajtási szervezet szolgálati jogviszonyban álló tagja, amennyiben a gyógykezelésre olyan személy esetében kerül sor, aki a büntetés-végrehajtási intézetben szabadságelvonással járó büntetését tölti, és a gyógykezelést végző betegellátó biztonsága, illetve szökés megakadályozása céljából erre szükség van,



- d) a b)-c) pontok szerinti személyek, ha bűnüldözési érdekből a beteg személyi biztonsága ezt indokoltá teszi, és a beteg nyilatkozattételre képtelen állapotban van.

Az egészségügyi szakember-képzés céljából - a betegellátó kivételével - az érintett (törvényes képviselője) hozzájárulásával lehet jelen a gyógykezelés során orvos, orvostanhallgató, egészségügyi szakdolgozó, egészségügyi főiskola hallgatója, illetve egészségügyi szakképző intézmény tanulója. Az egészségügyi ellátó hálózat egészségügyi szakember-képzésre kijelölt intézményeiben az érintett (törvényes képviselője) hozzájárulására nincs szükség. Erről az érintettet (törvényes képviselőjét) fekvőbeteg-intézmény esetén legkésőbb az intézménybe történő beutaláskor, beutaló hiányában a felvételt közvetlenül megelőzően, az egészségügyi ellátóhálózat egyéb intézményei esetén legkésőbb a gyógykezelés megkezdése előtt tájékoztatni kell.

Az érintett hozzájárulása nélkül is jelen lehet továbbá az, aki az érintettet az adott betegség miatt korábban gyógykezelte, továbbá akinek erre a főigazgató vagy az adatvédelmi tisztviselő szakmai-tudományos célból engedélyt adott, kivéve, ha ez ellen az érintett kifejezetten tiltakozott.

Az érintett jogosult tájékoztatást kapni az egészségügyi ellátással összefüggő valamennyi adatkezelésről, így különösen jogosult a kezelt adatok körét megismerni, az egészségügyi dokumentációba betekinteni, valamint azokról másolatot kérni.

A beteg gyógykezelésével kapcsolatos tájékoztatást a beteg kezelőorvosa, illetve a jogszabályok és belső szabályozások által meghatározott körben erre feljogosított dolgozó adhat. Tájékoztatás – kifejezetten eltérő jogszabályi rendelkezés hiányában – elsősorban személyesen adható, telefonon a beteg kezelésével összefüggésben személyes adat kizárólag abban az esetben adható ki, ha a telefonáló azonosítása kétséget kizáró módon megtörtént!

A beteg ellenkező tartalmú nyilatkozata hiányában az egészségügyi adatok megismerésére jogosult személy részére legfeljebb a kórházi tartózkodás tényéről adható információ. A beteg által megjelölt személyek részére a beteg általános állapotára vonatkozó információ adható. A beteg által kizárt személyek részére a beteggel kapcsolatosan nem adható semmiféle információ. A betegdokumentációban megfelelően rögzíteni szükséges, hogy kinek adható, illetve nem adható információ a betegről, rögzíteni kell továbbá azt is, hogy pontosan kinek, mikor és mely adatok kerültek ismertetésre.

A beteg jogosult az adott betegségével kapcsolatos egészségügyi ellátásának ideje alatt az általa meghatározott személyt írásban felhatalmazni a rá vonatkozó egészségügyi dokumentációba való betekintésre, illetve arra, hogy azokról másolatot készítsen. A beteg egészségügyi ellátásának befejezését követően csak a beteg által adott teljes bizonyító erővel rendelkező magánokiratban felhatalmazott személy jogosult az egészségügyi dokumentációba való betekintésre, és arról másolat készítésére.

A beteg életében, illetőleg halálát követően házastársa, egyeneságbeli rokona, testvére, valamint élettársa - írásos kérelme alapján - jogosult az egészségügyi adat megismerésére, ha az egészségügyi adatra a házastárs, az egyeneságbeli rokon, a testvér, illetve az élettárs, valamint leszármazóik életét, egészségét



befolyásoló ok feltárása, illetve ezen személyek egészségügyi ellátása céljából van szükség; és az egészségügyi adat más módon való megismerése, illetve az arra való következtetés nem lehetséges.

A betegellátás során a beteg névtáblája, lázlapja vagy más olyan dokumentum, amely a betegre vonatkozó személyes adatokat tartalmaz, kizárólag abban az esetben kerülhet kifüggesztésre, ha ehhez a beteg vagy a beteg helyett nyilatkozattételre jogosult törvényes képviselője előzetes tájékoztatást követően írásbeli hozzájárulást adott.

A betegazonosító csuklószalag felhelyezésére az Intézmény Szervezeti és működési szabályzatában meghatározott esetekben kerülhet sor. A betegazonosító csuklószalag nem tartalmazhat olyan személyes adatokat vagy megkülönböztető jelzést, amely alapján az érintett betegségére, állapotára, személyazonosságára vagy személyes adataira vonatkozó egyértelmű következtetés vonható le, betegazonosító kizárólag álnevesítéssel képezhető.

6. Egészségügyi dokumentáció vezetése

Az 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.

Az egészségügyi dokumentáció részeként meg kell őrizni:

- az egyes vizsgálatokról készült leleteket,
- a gyógykezelés és konzílium során keletkezett iratokat,
- az ápolási dokumentációt,
- a képalkotó diagnosztikus eljárások felvételeit és az arról készült leletet,
- a beteg testéből származó szövetmintákat.

Az egészségügyi dokumentációt - a képalkotó diagnosztikai eljárással készült felvételek, az arról készített leletek, valamint az Eüak. 30. § (7) bekezdése szerinti vények kivételével - az adatfelvételtől számított legalább 30 évig, a zárójelentést legalább 50 évig kell megőrizni. A kötelező nyilvántartási időt követően gyógykezelés vagy tudományos kutatás érdekében - amennyiben indokolt - az adatok továbbra is nyilvántarthatók. Ha a további nyilvántartás nem indokolt a nyilvántartást meg kell semmisíteni.

Képalkotó diagnosztikai eljárással készült felvételt az annak készítésétől számított 10 évig, a felvételtől készített leletet a felvétel készítésétől számított 30 évig kell megőrizni.

Amennyiben az egészségügyi dokumentációnak tudományos jelentősége van, a kötelező nyilvántartási időt követően át kell adni az illetékes levéltár részére. Ebben az esetben a nyilvántartás nem semmisíthető meg.

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 expedálás 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 gyógyszertertárban forgalmazható gyógyászati segédeszköz Eüak. 35/B. § szerint 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.

Az egészségügyi dokumentációban az adatokat nem lehet törölni. Az egészségügyi dokumentációban szereplő hibás egészségügyi adatot - az adatfelvételt követően - úgy kell kijavítani vagy törölni, hogy az eredetileg felvett adat megállapítható legyen.

A nyilvántartott adatokról, az egészségügyi dokumentációról az adatkezelő hiteles másolatot készít, ha ezt az adatbiztonság vagy a tárolt adatok fizikai védelme, illetve az e törvényben előírt adatközlési kötelezettség szükségessé teszi. A hiteles másolat adattartalmára vonatkozóan is biztosítani kell az egészségügyi és személyazonosító adatok kezelése és feldolgozása során az adatok biztonságát véletlen vagy szándékos megsemmisítéssel, megsemmisüléssel, megváltoztatással, károsodással, nyilvánosságra kerüléssel szemben, továbbá, hogy azokhoz illetéktelen személy ne férjen hozzá.

Az egészségügyi dokumentációt – Intézményen belüli vagy azon kívüli – továbbítása esetén tételes átadás-átvétel keretében kell átadni. Ennek során tételesen rögzíteni kell az átadott dokumentáció típusát (pl. kórlap, lázlap, ápolási lap, dekurzus, lelet stb.), annak oldalszámát, darabszámát is jelölve. Eredeti egészségügyi dokumentáció átadására kizárólag indokolt esetben, a jogszabály alapján arra feljogosított szerv határozata (így különösen bírósági határozat vagy ügyészi felhívás) alapján lehet helye.

Az egészségügyi dokumentáció elvesztése, megsemmisülése, megrongálódása esetén a főigazgatót, az orvosigazgatót és az adatvédelmi tisztviselőt haladéktalanul írásban tájékoztatni kell, továbbá az érintett dokumentumok és az eset körülményeinek leírása mellett jegyzőkönyvet kell felvenni és szükség esetén gondoskodni kell a dokumentáció pótlása iránt.

A betegek adatainak kezelésével kapcsolatos általános tájékoztatást bárki számára hozzáférhető módon elérhetővé kell tenni a honlapon, továbbá papír alapon minden betegellátó osztályon.



7. Betegadatok statisztikai célú kezelése

Az érintett egészségügyi adatai személyazonosításra nem alkalmas módon statisztikai célra korlátozás nélkül kezelhetők.

Az érintett személyazonosításra alkalmas egészségügyi és személyazonosító adatai statisztikai célra az érintett vagy törvényes képviselője tájékoztatáson alapuló, írásbeli hozzájárulásával kezelhető.

Jogszáály alapján kötelezően teljesítendő adatszolgáltatási kötelezettség esetén az ott megjelölt terjedelemben az adatok továbbítása kötelező. Ennek keretében az Intézmény köteles a Központi Statisztikai Hivatal, illetőleg az illetékes anyakönyvvezető részére az élve születéssel, illetve a halálozással kapcsolatos adatokat átadni. Így az Intézmény élve születés esetén a gyermek szülei, halálozás esetén az életben lévő házastárs adatait jogosult megismerni és az illetékes szervek részére továbbítani.

A betegek adatainak kezelésével kapcsolatos általános tájékoztatást bárki számára elérhető módon elérhetővé kell tenni a honlapon, továbbá papír alapon minden betegellátó osztályon.

8. Adatkezelés közegészségügyi, járványügyi célból

A közegészségügyi és járványügyi célból történő adatkezelésre kizárólag a jogszabályban meghatározott esetekben és feltételek betartásával van lehetősége az Intézménynek.

Az Intézmény haladéktalanul továbbítja az egészségügyi államigazgatási szervnek az adatfelvétel során tudomására jutott egészségügyi és személyazonosító adatot, ha az Eüak. 1. számú melléklet A) pontjában szereplő fertőző betegséget észlel vagy annak gyanúja merül föl.

Az Eüak. 1. számú mellékletben nem szereplő fertőző, illetve az 1. számú melléklet B) pontjában felsorolt betegségek előfordulása esetén a betegellátó személyazonosító adatok nélkül csak az egészségügyi adatokat jelentheti az egészségügyi államigazgatási szervnek. Az egészségügyi államigazgatási szerv közegészségügyi vagy járványügyi közérdekre hivatkozva - az anonim szűrővizsgálat keretében vizsgált HIV fertőzött és AIDS beteg kivételével - kérheti az érintett személyazonosító adatait.

Az Intézmény továbbítja az egészségügyi államigazgatási szervnek azon személyek egészségügyi és személyazonosító adatait, akiknél a mikrobiológiai laboratóriumi vizsgálati eredmény az Eüak. 1. számú melléklet A) pontja szerinti fertőzések, fertőzőes eredetű betegségek, mérgezések fennállását, illetve kórokozók jelenlétét valószínűsíti vagy igazolja. A betegellátó továbbítja az egészségügyi államigazgatási szervnek az Eüak. 1. számú melléklet A) pontja szerinti fertőzések, fertőzőes eredetű betegségek, mérgezések közül a miniszteri rendeletben meghatározott betegségekre vonatkozó azon vizsgálati eredményt is, amely a korábbi valószínűsítés ellenére nem igazolja az adott betegség fennállását.



A kezelőorvos a fentiek szerinti fertőző betegség észlelése vagy gyanúja esetén köteles értesíteni az Intézmény kórházhigiénés osztályát és gondoskodni az adatok megfelelő továbbításáról.

A tüdőgondozó intézetek a tuberkulózis, illetve a bőr- és nemibeteg ellátás intézményei az Eüak. 1. számú mellékletben szereplő nemi betegségek előfordulása esetén - további személyek veszélyeztetésére tekintettel - egymás között továbbíthatják az érintett kontaktusaira vonatkozó személyazonosító adatok közül a családi és utónevet, a leánykori nevet, valamint a lakó- és tartózkodási helyet.

Az Intézmény az életkorhoz kötött oltáshoz szükséges oltóanyag igénylése és elszámolása során továbbítja az oltandó személyek nevét és társadalombiztosítási azonosító jelét az egészségügyi államigazgatási szervnek, továbbá az életkorhoz kötött kötelező és önkéntes védőoltások esetén, valamint megbetegedési veszély elhárítása céljából kötelező védőoltások esetén a védőoltásban részesültek személyazonosító adatait - miniszteri rendeletben meghatározott módon elektronikus úton is - továbbítja az egészségügyi államigazgatási szervnek.

Az észlelő orvos köteles haladéktalanul továbbítani a munkavédelmi hatóságnak a munkavállaló egészségügyi és személyazonosító adatát, ha az Eüak. 3. számú melléklet szerinti foglalkozási eredetű megbetegedést észlel, vagy annak gyanúja merül fel, vagy az érintett foglalkozása gyakorlása közben, azzal összefüggésben

- miniszteri rendeletben meghatározott vegyi anyag hatásának van kitéve, és szervezetében az anyag koncentrációja a megengedett mértéket meghaladja, valamint
- zaj esetében a 4000 Hz-en 30 dB bármely fülön bekövetkező halláscsökkenés fordul elő.

9. Tudományos kutatás céljából történő adatkezelés

Tudományos kutatás céljából engedélyezhető az Intézmény által tárolt adatokba történő betekintés.

A kutatási kérelemben meg kell jelölni a kutatás megnevezését, időtartamát, a megismerni kívánt adatok körét és forrását, a kutatás célját, az adatkezelés folyamatát és az érintettek jogait biztosító körülményeket. A kutatásra az engedélyt az intézményi kutatásetikai bizottság javaslatára a főigazgató adja meg, az adatvédelmi tisztviselő álláspontjának ismeretében. A kutatási kérelmekről és a megadott engedély alapján személyes adatokat megismerő személyekről az igazgatósági titkárság 10 évig nyilvántartást vezet.

Az Intézmény alapos okból jogosult megtagadni az engedély kiadását, ez ellen azonban a kérelmező bírósághoz fordulhat és kérheti az engedély megadását. A bíróság engedélye alapján az adatokba történő betekintést engedélyezni kell.

A kutatás során a kutatást végző személy titoktartási kötelezettség vállalása mellett a dokumentációba betekinthez, a tárolt adatokról azonban nem készíthető az érintett azonosítására alkalmas személyes adatokat tartalmazó másolat, kizárólag anonimizált formában kezelhetők adatok. Tudományos kutatás során



kezelt adat az Európai Unión kívüli országba kizárólag az érintett hozzájárulásával továbbítható. A kutatás eredményében (így elsősorban közleményben, előadáson stb.) nem szerepelhet az érintett azonosítására alkalmas egészségügyi és személyes adat.

A betegek adatainak kezelésével kapcsolatos általános tájékoztatást bárki számára elérhető módon elérhetővé kell tenni a honlapon, továbbá papír alapon minden betegellátó osztályon.

10. A társadalombiztosítási igazgatási szervek adatkezelése

A társadalombiztosítási igazgatási szervek részére kizárólag abban az esetben továbbítható egészségügyi és személyazonosító adat, amennyiben arra az érintett társadalombiztosítási ellátásra való jogosultságának megállapítása, folyósítása céljából van szükséges vagy az jogszabályi kötelezettség teljesítéséhez egyébként szükséges.

A társadalombiztosítási igazgatási szervek részéről sor kerülhet az érintett adatainak kezelésére egyrészt akkor, ha az érintett olyan társadalombiztosítási ellátás, juttatás igénybevételére jogosult, amelynek megállapítása az egészségi állapot alapján történik, másrészt akkor, ha a társadalombiztosítási alapokból származó bevételek felhasználását kívánják ellenőrizni.

A betegek adatainak kezelésével kapcsolatos általános tájékoztatást bárki számára elérhető módon közzé kell tenni a honlapon, továbbá papír alapon minden betegellátó osztályon.

11. Adattovábbítás az egészségügyi ellátó hálózaton kívülre

Az érintett első ízben történő orvosi ellátásakor, ha az érintett nyolc 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 - a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény 17. §-ára is tekintettel - az ellátást végző egészségügyi szolgáltató ezzel megbízott orvosa köteles az egészségügyi szolgáltató telephelye szerint illetékes gyermekjóléti szolgálatot haladéktalanul értesíteni, ha feltételezhető, hogy a gyermek sérülése vagy betegsége bántalmazás, illetve elhanyagolás következménye, vagy a gyermek egészségügyi ellátása során bántalmazására, elhanyagolására utaló körülményekről szerez tudomást.

Ilyen esetben az adattovábbításhoz az érintett, illetve az adattal kapcsolatosan egyébként rendelkezésre jogosult beleegyezése nem szükséges.

Amennyiben valamely hivatalos szerv (így különösen bíróság, ügyészség, közigazgatási szerv, rendőrség) az Intézmény által kezelt személyes adatok megismerése iránt megkeresést intéz az Intézmény felé, a megkeresés jogszerűsége esetén a személyes adatok kiadása nem tagadható meg. Amennyiben a megkeresésből az adatkezelés pontos célja és a kért adatok köre nincs



meghatározva, meg kell tagadni az adatszolgáltatást és a megkereső szervet fel kell hívni a megkeresés pontosítására.

Az illetékes ügyintéző az előkészített válaszlevelet és annak mellékleteit köteles megküldeni a kiadmányozásra jogosult vezető részére. A válasz előkészítése során a dokumentáció és irattár vagy a kért adatokkal rendelkező más szervezeti egység köteles együttműködni és a szükséges dokumentumokat vagy azok másolatát haladéktalanul rendelkezésre bocsátani. Amennyiben a megkeresés teljesítéséhez a személyes adatokat tartalmazó eredeti dokumentáció kiadása válik szükségessé, az illetékes ügyintéző az eredeti dokumentációról hitelesített másolatot köteles készíteni és a kiadás tényét, időpontját és címzettjét arra rávezetni.

Amennyiben az érintett vagy más személy az egészségügyi adatok megismerését (a dokumentációba történő betekintést, másolat készítését) kezdeményezi, az adatok megismeréséhez való jogosultságát minden esetben ellenőrizni kell. A jogosultság hitelt érdemlő igazolásának vagy az azonosítás megtagadása esetén az Intézmény a megkeresést köteles elutasítani. A személyes adatok megismerhetőségének biztosítása előtt az illetékes ügyintéző köteles megbizonyosodni az érintett személyazonosságáról, ennek hiányában az adatok kiadása nem lehetséges. Az azonosítás során a személyazonosító igazolványokról másolat készítése tilos. A betekintés engedélyezésére, illetve a másolatok kiadására kizárólag ezt követően, az adatigénylő azonosítását követően kerülhet sor.

Az adatokba történő betekintés, illetve az személyes adatok kiadásának tényét, okát (célját) időpontját, címzettjét és a kiadást fogantató orvos nevét és bélyegzőlenyomatát a dokumentációban rögzíteni kell.

Amennyiben a kért adatokba történő betekintés biztosítása, illetve azok kiadhatósága az illetékes ügyintéző vagy kiadmányozásra jogosult vezető számára kétséges, a megkeresés jogszerűségéről és az adatok kiadhatóságáról az adatvédelmi tisztviselő álláspontjának ismeretében az igazgatási, jogi és humánpolitikai főigazgató-helyettes dönt, szükség esetén a jogi iroda állásfoglalásának kikérése mellett.

Hivatalos szervek (bíróságok, hatóságok) megkeresésére a megkeresésben meghatározott, illetve az abban foglaltak teljesítéséhez szükséges személyes adatok (ideértve az egészségügyi személyes adatokat is) és dokumentáció másolatának megküldése térítésmentesen, a hatóság által meghatározott módon papír alapon vagy elektronikus úton történik.

Az Intézmény az igényelt személyes adatok másolatát - a GDPR 15. cikk (3) bekezdésével összhangban - első alkalommal ingyenesen bocsátja az érintett rendelkezésére. Az érintett által kért további másolatokért az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel, amelynek mértékét a Térítési díj szabályzat állapítja meg. Amennyiben a másolok biztosítása térítési díj köteles, a másolat kiadására kizárólag a díj megfizetésének igazolását és a bizonylat dokumentációhoz csatolását követően kerülhet sor.

Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell a rendelkezésére bocsátani, kivéve, ha az érintett másként kéri.

XIV. A gyermekek adatainak kezelésére vonatkozó különös szabályok

Az adatkezelés során mindenkor figyelemmel kell lenni arra, hogy az általános adatvédelmi jogok (jog a tájékoztatáshoz, hozzáféréshez, helyesbítéshez, korlátozáshoz, az adat hordozhatóságához, a tiltakozáshoz vagy a jogorvoslathoz) a gyermeket önállóan, illetve a törvényes képviselőjével közösen ugyanúgy megilletik, mint bármely más érintett.

Az Intézmény nem utasíthatja el a gyermek érintetti joggyakorlását, így például tájékoztatási vagy helyesbítési kérelmét arra hivatkozással, hogy gyermekkorú, szükség esetén azonban kérhető a törvényes képviselő nyilatkozata is. Ezeket a kérelmeket minden esetben egyedileg kell elbírálni, az eset összes körülményére tekintettel.

A gyermekek részére számukra érthető módon és nyelvezettel szükséges a tájékoztatást biztosítani és egyidejűleg a törvényes képviselőt is megfelelően tájékoztatni kell. A megfelelő tájékoztatás kifejezetten fontos akkor, mikor az adatkezelés jogalapja az adatkezelő vagy harmadik fél jogos érdekeinek érvényesítésén alapul, amely esetben az érdekmérlegelési teszt elkészítése során az ezzel kapcsolatos szempontokat különös súllyal figyelembe kell venni.

A polgári törvénykönyvről szóló 2013. évi V. törvény értelmében a cselekvőképtelen 14 év alatti gyermekek jognyilatkozata - a mindennapi élet csekély jelentőségű ügyleteit leszámítva - semmis, nevükben a törvényes képviselő jár el, a 14. életévét betöltött korlátozottan cselekvőképes kiskorú által tett jognyilatkozat érvényességéhez szükséges a törvényes képviselő hozzájárulása azzal, hogy a cselekvőképessé válás után az érintett maga dönthet a függő jognyilatkozatok sorsáról.

Amennyiben a hozzájárulás az adatkezelés jogalapja, az adatkezelőnek a gyermek tudomására kell hoznia, hogy milyen feltételek esetén veheti igénybe a szolgáltatást, és ezeknek a feltételeknek milyen módon kell eleget tenni. Amennyiben a gyermekek nem vehetik igénybe a szolgáltatást, azt számukra érthető módon és formában kell tudomásukra hozni.

Adatvédelmi incidens esetén a gyermek érintetteket is megfelelő módon értesíteni szükséges, a törvényes képviselő egyidejű tájékoztatása mellett.

XV. A cselekvőképességében korlátozott nagykorú személyek adatainak kezelésére vonatkozó különös szabályok

Az adatkezelés során mindenkor figyelemmel kell lenni arra, hogy az általános adatvédelmi jogok (jog a tájékoztatáshoz, hozzáféréshez, helyesbítéshez, korlátozáshoz, az adat hordozhatóságához, a tiltakozáshoz vagy a jogorvoslathoz) a cselekvőképtelen vagy cselekvőképességében korlátozott nagykorú személyt önállóan, illetve a törvényes képviselőjével közösen ugyanúgy megilletik, mint bármely más érintett.

Az Intézmény nem utasíthatja el a cselekvőképességében korlátozott nagykorú személy érintetti joggyakorlását, így például tájékoztatási vagy helyesbítési kérelmét arra hivatkozással, hogy cselekvőképességében korlátozott, szükség esetén azonban kérhető a törvényes képviselő nyilatkozata is. Ezeket a kérelmeket minden esetben egyedileg kell elbírálni, az eset összes körülményére tekintettel. Amennyiben az érintett cselekvőképtelen, nyilatkozatához minden esetben szükséges a törvényes képviselő



nyilatkozata, a cselekvőképességében korlátozott személyek esetén vizsgálni szükséges, hogy az érintett cselekvőképessége a nyilatkozat megtételéhez szükséges ügycsoportban korlátozott-e. Amennyiben igen, a nyilatkozatához szükséges a törvényes képviselő nyilatkozata.

A cselekvőképességükben korlátozott nagykorú személyek részére számukra érthető módon és nyelvezettel szükséges a tájékoztatást biztosítani és szükség esetén egyidejűleg a törvényes képviselőt is megfelelően tájékoztatni kell. A megfelelő tájékoztatás kifejezetten fontos akkor, mikor az adatkezelés jogalapja az adatkezelő vagy harmadik fél jogos érdekeinek érvényesítésén alapul, amely esetben az érdekmérlegelési teszt elkészítése során az ezzel kapcsolatos szempontokat különös súllyal figyelembe kell venni.

A polgári törvénykönyvről szóló 2013. évi V. törvény értelmében a cselekvőképtelen nagykorú személyek jognyilatkozata - a mindennapi élet csekély jelentőségű ügyleteit leszámítva - semmis, nevükben a törvényes képviselő jár el, a cselekvőképességében részlegesen korlátozott nagykorú személy által tett jognyilatkozat érvényességéhez szükséges a törvényes képviselő hozzájárulása azzal, hogy a cselekvőképessé válás után az érintett maga dönthet a függő jognyilatkozatok sorsáról.

Adatvédelmi incidens esetén a cselekvőképességükben korlátozott nagykorú érintetteket is megfelelő módon értesíteni kell, szükség esetén a törvényes képviselő egyidejű tájékoztatása mellett.

XVI. A cselekvőképtelen állapotban lévő személyek személyes adatainak kezelésére vonatkozó különös szabályok

A cselekvőképtelen állapotban lévő, azonban cselekvőképességében nem korlátozott személyek (pl. eszméletlen állapotú betegek) személyes adatainak kezelése során az Intézmény fokozott figyelemmel köteles lenni az adatkezelés jogalapjára.

A cselekvőképtelen állapotban lévő személy személyes adatai a GDPR 6. cikk (1) bekezdés a) pontja szerint adott érintetti hozzájárulás alapján kizárólag abban az esetben kezelhetők, ha az érintett ezen nyilatkozatát a cselekvőképtelen állapotba kerülését megelőzően, megfelelő módon tette meg.

A cselekvőképtelen állapotban lévő személyről tájékoztatás kizárólag az érintett korábban megtett nyilatkozata szerint, illetve a jogszabályi előírások keretei között, a lehető legszűkebb körben biztosítható az arra jogosultak részére.

Abban az esetben, ha az érintett cselekvőképtelen állapota megszűnik, az Intézmény – az általános szabályok szerint – köteles biztosítani az érintetti jogok gyakorlását.

XVII. A látássérültek személyes adatainak kezelésére vonatkozó különös szabályok

Az Intézmény törekszik arra, hogy a személyes adatok kezelésével összefüggésben nyújtott tájékoztatás minden esetben akadálymentes formában is elérhető legyen. Így az elektronikusan közzétett tájékoztatókat és az érintett személyes adatainak kezeléséhez kapcsolódó más dokumentumokat széles körben elterjedt, géppel is olvasható módon köteles elérhetővé tenni, továbbá az alkalmazott betűtípusnak és méretnek, a szöveg



háttérének és színeinek elő kell segítenie az információk vakok és gyengénlátók számára történő befogadását.

Az érintett személyes adatainak kezeléséhez kapcsolódó, papír alapú dokumentumokat a vakok és gyengénlátók számára is olvasható (pl. Braille-írással, nagy betűmérettel nyomtatott) formában is elérhetővé kell tenni vagy a tájékoztatást más módon kell biztosítani.

Szükség esetén gondoskodni kell arról, hogy a látássérült érintett számára a szükséges információk szóbeli tájékoztatás útján átadásra kerüljenek.

XVIII. Dolgozói adatok kezelése, nyilvántartása

1. Pályázók adatainak kezelése

Az Intézmény által egészségügyi szolgálati jogviszony vagy egyéb munkavégzésre irányuló jogviszony létrehozását megelőző pályázati eljárás során a pályázótól kizárólag olyan személyes adatok megadása kérhető, amely a pályázat elbírálásához és az érintett ezzel összefüggő tájékoztatása érdekében elengedhetetlenül szükséges.

Az elbírálás során a képességek felmérésére és az alkalmasság megállapítására kizárólag a cél eléréséhez szükséges, arányos eszközökkel kerülhet sor.

A pályázó alkalmassági vizsgálata során a pályázó közösségi oldalakon bárki számára elérhető módon közzétett személyes adatait kizárólag abban az esetben lehet megtekinteni, ha az Intézmény ennek lehetőségéről és módjáról az érintettet előzetesen tájékoztatta és a pályázat benyújtására ennek ismeretében került sor.

Az eredménytelenül pályázók személyes adatait – jogszabály eltérő rendelkezése, vagy az érintett kifejezett, írásbeli hozzájárulása hiányában – a pályázati eljárás befejezésekor törölni kell.

A pályázók adatainak kezelésével kapcsolatos részletes tájékoztatást külön adatkezelési tájékoztató tartalmazza.

2. Dolgozók adatainak kezelése

Az egészségügyi szolgálati jogviszonyban vagy egyéb munkavégzésre irányuló jogviszonyban foglalkoztatott dolgozókról kizárólag a munkavégzéssel összefüggő célból, megfelelő jogalap fennállása esetén kezelhetők adatok.

A dolgozók adatai közül kizárólag azon személyes adatok kezelhetők, valamint olyan munkaköri orvosi alkalmassági vizsgálatok végezhetők, amelyek a jogviszony létesítéséhez, fenntartásához és megszüntetéséhez, illetve a szociális-jóléti juttatások biztosításához, vagy más jogszerű célból elengedhetetlenül szükségesek és a dolgozó személyhez fűződő jogait nem sértik.

A dolgozó személyes adatait tartalmazó iratokat és személyi anyagokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés, megsemmisítés, véletlen megsemmisülés és sérülés ellen. A személyes adatokat az illetékes ügyintéző a feladat ellátásához szükséges mértékben kezelheti.



A jogviszonnyal összefüggő személyi irat, dokumentum kizárólag személyesen vagy meghatalmazott útján vehető át, valamint tértivevénnyel postázható az érintett lakcímére, vagy megfelelő biztonsági szintet nyújtó elektronikus úton adható át a címzett részére.

A dolgozóra vonatkozó személyazonosításra nem alkalmas statisztikai adat az érintett hozzájárulása nélkül is kezelhető.

A dolgozók adatainak kezelésével kapcsolatos adatkezelési tájékoztatót az érintettek számára megismerhetővé kell tenni.

XIX. Szerződő partnerek adatainak kezelése, nyilvántartása

Az adatkezelés célja elsődlegesen az Intézmény és az érintett közötti szerződés létrehozása érdekében szükséges lépések megtétele, illetve a szerződésből eredő jogok érvényesítése és a szerződésből fakadó kötelezettségek teljesítése, valamint a szerződéssel összefüggő vagy üzleti kapcsolattartás lehet.

Az adott szerződés vonatkozásában minden esetben kizárólag az adatkezelési cél eléréséhez elengedhetetlenül szükséges adatok kezelésére kerül sor. A szerződésben rögzített személyes adatokat kizárólag a szerződés teljesítésében részt vevő, azzal kapcsolatosan feladatot ellátó munkatársak jogosultak kezelni, a feladat elvégzéséhez szükséges mértékben. Ilyen feladat lehet különösen a szerződés teljesítése érdekében történő kapcsolattartás, a számlázási feladatok ellátása, a térítési díj ellenében igénybe vehető szolgáltatások teljesítése, stb.

A szerződő partnerek adatainak kezelésével kapcsolatos adatkezelési tájékoztatót külön dokumentum tartalmazza.

XX. A papír alapon kezelt személyes adatok

A papír alapú dokumentumok kezelésére vonatkozó részletes előírásokat az Iratkezelési szabályzat tartalmazza.

A dokumentumok elhelyezésénél kiemelten ügyelni kell arra, hogy azokhoz illetéktelen személyek ne férhessenek hozzá, megfelelő zárható szekrényben kerüljenek megőrzésre. A tárolás kizárólag olyan helyen történhet, ahol a dokumentumok tűz és víz elleni védelme biztosított legyen.

Az egészségügyi dokumentációknak kezelési gyakoriságuk szerint három szintjét különböztetjük meg:

- **„A” szint:** a mindennapi kezelésre szoruló dokumentációk. Ezek azok a dokumentációk, amelyek a jelenleg is az Intézményben kezelt érintettek iratait tartalmazzák. Tárolásuk a betegellátó szervezeti egységnél történik, olyan helyen, hogy biztosítva legyen a kezelőorvos és a gyógykezelésben részt vevő más személyek hozzáférése, de védett legyen az érintett kezelésében részt nem vevők (így különösen hozzátartozók, látogatók, egyéb dolgozók) hozzáférése ellen.
- **„B” szint:** az egy irattári éven belüli dokumentációk. Ezeket a dokumentumokat a szervezeti egységek kézi irattárában kell elhelyezni. A kézi irattár kialakításánál biztosítani kell a dokumentáció védelmét és ki



kell alakítani a hozzáférés rendszerét. A kézi irattárba helyezett dokumentációkat nyilvántartási sorszámuk szerint kell raktározni, tűztől és víztől védett, biztonsági zárral ellátott tárolószekrényben, vagy biztonsági zárral ellátott helyiségben.

- „C” szint: az egy irattári éven túli dokumentációk. Ezeket a központi irattárban kell elhelyezni, ahol télen-nyáron biztosítható a megfelelő páratartalom (55-65%) és a 17-18 °C hőmérséklet, tűz és vízbiztos helyen van, közművezeték nem halad át a helyiségen. Az irattárat stabil vagy mobil, vasból vagy acélból készült állványokkal kell berendezni úgy, hogy a hozzáférhetőség és a munkavédelmi szempontok biztosítva legyenek. A dokumentáció nyilvántartására szolgáló regisztereket külön dobozban vagy szekrényben kell tárolni, évek szerinti bontásban.

XXI. Elektronikusan kezelt személyes adatok

Az elektronikusan tárolt dokumentumokra, adatokra, személyes adatokra vonatkozó részletes előírásokat az Informatikai biztonsági szabályzat tartalmazza.

Az elektronikusan kezelt személyes adatot védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés, megsemmisítés, véletlen megsemmisülés és sérülés ellen. A személyes adatokhoz az illetékes ügyintéző a feladat ellátásához szükséges mértékben férhet hozzá.

Személyes adatok elektronikus kezelését olyan rendszerek útján kell biztosítani, amelyek alkalmasak az egyes felhasználók által végzett feladatellátáshoz szükséges mértékű felhasználói jogosultságok beállítására, az adatkezelő személyének azonosítására és az adatokkal végzett műveletek regisztrálására, naplózására.

XXII. Elektronikus térfigyelési rendszerre vonatkozó alapvető szabályok

Az Intézmény elektronikus térfigyelő rendszert üzemeltet, ennek célja az épületbe történő illetéktelen belépések és az ebből fakadó esetleges vagyon elleni bűncselekmények megtörténtének megakadályozása.

Az elektronikus térfigyelő rendszer működtetése során személyes adatokat tartalmazó kép-, hang-, vagy kép- és hangfelvételek készülnek.

A kamerák elhelyezése során figyelemmel kell lenni arra, hogy az elektronikus térfigyelő rendszer nem sérthet emberi méltóságot, a térfigyelő rendszer által a foglalkoztatottak magánélete nem ellenőrizhető, valamint arra is, hogy a kamera látószöge kizárólag a céljával összhangban álló területre irányulhat.

Az Intézmény gondoskodik arról, hogy az Intézmény épületeibe belépő személyeket a jogszabályban előírt részletességgel, előzetesen tájékoztassa az elektronikus térfigyelő rendszerrel kapcsolatos adatkezelés lényeges követelményeiről.

Az érintettek tájékoztatásáról az elektronikus térfigyelő rendszer működtetője köteles gondoskodni. A tájékoztató minden egyes kamera vonatkozásában ki kell, hogy térjen arra, hogy az adott kamera milyen célból került elhelyezésre az adott területen és milyen területre irányul a kamera látószöge.

Az Intézmény figyelemfelhívó jelzést köteles elhelyezni a megfigyelt területeken. Az Intézmény által alkalmazott térfigyelő rendszer közvetlen megfigyelésre (élőkép)



használható, közvetlen megfigyelésre kizárólag az erre feljogosított munkatársainak és kizárólag a munkakörük ellátásához szükséges mértékben van joga. A képfelvételek megtekintésére és esetleges visszanezítésére szolgáló monitort úgy kell elhelyezni, hogy a képfelvételek sugárzása alatt azokat a jogosultsági körön kívüli személyek ne láthassák.

A rögzített felvételek felhasználására kivételes esetben kerülhet sor, arra kizárólag a jogszabály által feljogosított szerv vagy személy jogosult. A tárolt felvételek visszanezítését, az adattovábbítást és az esetleges mentést dokumentálni kell.

Az elektronikus térfelügyeleti rendszerre vonatkozó részletes tájékoztatást külön adatkezelési tájékoztató tartalmazza.

XXIII. Záró rendelkezések

Jelen szabályzatot a személyi hatálya alá tartozó valamennyi személy köteles megismerni és betartani. Ennek érdekében a szabályzatot valamennyi szervezet, szervezeti egység, valamint személy rendelkezésére kell bocsátani és a megismerés tényét dokumentálni kell.

A jelen szabályzatot a személyi hatálya alá tartozók részére folyamatosan elérhetővé kell tenni.

Jelen szabályzat az intézményvezető főigazgató aláírását követő napon lép hatályba és hatálybalépésével egyidejűleg valamennyi, azonos tárgykörben kiadott korábbi szabályzat hatályát veszti. Jelen szabályzat visszavonásig hatályos.

1.számú melléklet: Incidens nyilvántartás sablonja

#	Az adatvédelmi incidens időpontja, helye	Az adatvédelmi incidenssel érintettek köre, száma	Az érintett személyes adatok köre	Az adatvédelmi incidens körülményei, az adatkezelést előíró jogszabályban meghatározott egyéb adatok	Az adatvédelmi incidens hatásai	Az adatvédelmi incidens elhárítására megtett intézkedések	Bejegyzés dátuma, bejegyző neve, aláírása
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
...							



2. számú melléklet: Adatvédelmi incidens bejelentőlap

Kérjük a tudomásszerzést követően haladéktalanul kitölteni, és az Intézmény adatvédelmi tisztviselőjéhez eljuttatni!

I. Adatvédelmi incidensről tudomást szerző munkatárs

- neve:
- beosztása:
- szervezeti egység:
- munkahelyi elérhetősége:

II. Az adatvédelmi incidens

- jellege:
- észlelésének időpontja, módja:
- bekövetkezésének feltételezett időpontja, helye, módja:
- által érintett személyek kategóriái és hozzávetőleges száma:
- által érintett személyes adatok köre és hozzávetőleges száma:
- észlelt vagy lehetséges következményei:
- orvoslására tett vagy tervezett intézkedés és az intézkedés elrendelője, valamint végrehajtója (név és beosztás szerint):

III. Az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve: IGEN / NEM

IV. Egyéb észrevétel:

Budapest, 20.... (év) (hó).(nap)