Dokumentáció kódja:	FŐIG 7 SZ - AV
Oldalak száma:	68
Mellékletek száma:	4
Változatszám:	3. változat
Érvénybelépés időpontja:	2023. június 19.
1032 BUDAPEST, Bécsi út 132.	

BUDAPESTI
SZENT MARGIT
KÓRHÁZ

A
Budapesti Szent Margit Kórház
Adatvédelmi Szabályzata

Szabályzatot készítette:	Tóth László adatvédelmi tisztviselő	2023.06.07.
Aláírás:	Tóth László	
Szakmailag ellenőrizte:	dr. Nagy Mihály főigazgató	2023.06.15
Aláírás:		
Minőségügyi szempontból ellenőrizte:	Ralovich Csilla igazgatásszervezési és minőségirányítási referens	2023.06.15.
Aláírás:	Ralovich Csilla	
Jogi szempontból ellenőrizte:	Dr. Soós Ágnes Zsófia ügyvéd	2023.06.16.
Aláírás:	dr. Soós Ágnes	
Jóváhagyta:	dr. Nagy Mihály főigazgató	2023.06.19.
Aláírás:		

Budapesti Szent Margit Kórház 1. Főigazgató

Ph.

MÓDOSÍTÁSOK JEGYZÉKE:

Változat száma	Módosította Aláírás/dátum	Módosított oldalak száma
2	dr. Kósa Lehel	Teljes körű módosítás.
3	Tóth László adatvédelmi tisztviselő 2023.06.07.	Teljes körű módosítás

TARTALOMJEGYZÉK

A **Budapesti Szent Margit Kórház** (a továbbiakban: **Intézmény**, vagy **adatkezelő**) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló, 2016. április 27-i, 2016/679/EU európai parlamenti és tanácsi rendelet, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, valamint az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény alapján az Intézmény adatvédelmének, adatbiztonságának és adatkezelésének rendjére az alábbi szabályzatot alkotja.

ÁLTALÁNOS RÉSZ

I. A Szabályzat célja és hatálya

1. A Szabályzat célja

A Szabályzat célja, hogy meghatározza az Intézmény és a szabályzat hatálya alá tartozó egyéb szervezetek tevékenysége és működése során az általa kezelt természetes személyek személyes adatainak védelmére irányuló intézkedések és eljárások jogszerű rendjét, valamint biztosítsa az adatvédelem alapjogi elveinek, 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. Az Intézmény az általa 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 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.

2. A Szabályzat személyi hatálya

A Szabályzat személyi hatálya kiterjed

a) az Intézmény valamennyi szervezeti egységére, és az Intézmény nevében bármely jogviszony alapján tevékenységet végző természetes személyre, aki tevékenysége során személyes adatot kezel.

b) 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.

c) azon személyekre is, akik az Intézménnyel nem állnak az a) és b) pont szerinti jogviszonyban, illetve kapcsolatban, azonban személyes adataikat jogszabályi előírás folytán az Intézmény kezeli.

3. A Szabályzat tárgyi hatálya

A Szabályzat tárgyi hatálya kiterjed az Intézmény által bármely célból kezelt személyes adatra, különös tekintettel az egészségügyi adatok kezelésére és a személyes adatoknak az Intézménynél megtalálható valamennyi nyilvántartására, függetlenül azok megjelenési formájától.

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

II. Jogszabályi környezet

Az adatkezelés intézményi rendje az alábbi jogszabályok és előírások figyelembevételével került szabályozásra:

a) A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló, az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (a továbbiakban: GDPR)

b) Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: **Infotv.**)

c) Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (a továbbiakban: **Eüak.**)

d) Az egészségügyről szóló 1997. évi CLIV. törvény (a továbbiakban: **Eütv.**)

e) Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről rendelkező 62/1997. (XII.21.) NM rendelet (a továbbiakban: **Eünr.**)

f) Az egyes daganatos megbetegedések bejelentésének rendjéről szóló 24/1999. (VII.6.) EüM rendelet. (a továbbiakban: **Dbr.**)

g) Informatikai Tárcaközi Bizottság 8. sz. ajánlása.

III. A Szabályzat alkalmazásában használt fogalmak

A Szabályzat alkalmazása során a fogalmak az alábbiak szerint értelmezendők.

Személyazonosító adatok: az Eüak. alkalmazásában az olyan, az egészségügyi adat érintettjének azonosítására szolgáló személyes adat (pl. születési hely és idő; név, lakcím stb.), amelyet az

adatkezelő az egészségügyi adattal együtt, az egészségügyi adat kezelésével azonos vagy attól elválaszthatatlan céllal az egészségügyi dokumentáció részeként kezel.

Személyes adat: azonosított vagy azonosítható természetes személyre (a továbbiakban: **érintett**) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható. Jelen Szabályzat alkalmazásában valamennyi „adat" megjelölés alatt a személyes adatok értendők.

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.

Különleges adat: a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.

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.

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

Az érintett hozzájárulása: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.

Adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adat véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

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

Adattovábbítás: az adatnak egy meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges.

Felügyeleti hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH).

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 előre jelzésére használnak.

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.

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

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.

IV. 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, továbbá az elszámoltathatóság elvének megfelelően képesnek kell lennie e megfelelés igazolására is. A megfelelőség igazolása különösen az adatkezeléshez kapcsolódó döntéseket megalapozó körülmények és a döntések (pl. az adatkezelés feltételeit meghatározó döntéselőkészítő iratok), az érintetteknek szóló adatkezelési tájékoztatók, az 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.

V. Az adatvédelmi tevékenység szervezete és irányítása az Intézményben

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 megszűntetéséről, szükség szerint a felelősségre vonásról,

e) kinevezi az Intézmény adatvédelmi tisztviselőjét, és az adatvédelmi tisztviselő nevét és elérhetőségét bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak.

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

2. Az adatvédelmi tisztviselő feladatai

Az adatvédelmi tisztviselőt a főigazgató bízza meg. Az adatvédelmi tisztviselő közvetlenül és kizárólag a főigazgatónak 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. 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 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 vezetője, a belső ellenőr, illetve az információbiztonsági felelős.

Az adatvédelmi tisztviselő az adatvédelmi tisztviselői feladatokon kívül a főigazgató döntése alapján más munkakörhöz, feladatkörhöz 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 a 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) a jogi irodával és az informatikai osztállyal együttműködve felülvizsgálja az adatvédelmi szabályzatot, illetve az informatikai biztonsági szabályzatot, valamint közreműködik azok hatályosításában,

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) éves 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 adatvédelmi tisztviselő nyilvántartást vezet:

a) Az Intézménynél végzett adatkezelési tevékenységekről.

A nyilvántartás tartalmazza az adatkezelő szervezeti egység nevét és elérhetőségét, az adatokhoz való hozzáférésre jogosult személyek körének meghatározását (elsősorban munkakör szerint), 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 előirányzott határidőket, ha lehetséges, az adatvédelmi biztonsági technikai és szervezési intézkedések általános leírását, valamint az alkalmazott adatfeldolgozási technológia megnevezését.

A nyilvántartás tartalmazza továbbá az adatok forrását, az adatok kezelésének időtartamát, a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét, az adatkezelés kockázati besorolását, illetve az adatkezelés módszerének meghatározását (manuális, számítógépes, vegyes).

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

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 2. sz. mellékletében meghatározottak szerint.

c) Az Intézménynél végzett adattovábbításról.

Ha az adattovábbítás alkalomszerű, és valamely szerződéssel vagy jogi igénnyel kapcsolatban válik szükségessé, akkor az Intézmény köteles az adattovábbítási nyilvántartásban ezt rögzíteni. Az adattovábbítási nyilvántartás az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából tartalmazza a kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat a jelen szabályzat 3. sz. mellékletében meghatározottak szerint.

d) Az Intézmény által elutasított érintetti megkeresésekről, panaszokról.

A nyilvántartási célú adatállományt kezelő szervezeti egység vezetője az új adatállomány kialakítását a tevékenység megkezdése előtt 15 nappal bejelenti az adatvédelmi tisztviselőnek, aki azt adatkezelési nyilvántartásba bejegyzi.

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

Az adatkezelési nyilvántartással összefüggésben az adatvédelmi tisztviselő:

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

b) a Jogi Irodával együttműködve figyelemmel kíséri az adatkezelést érintő jogszabályok változását és a szükséges módosításokra felhívja az felsőfokú képesítéssel felelősök figyelmét;

c) 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 ismeretei fenntartásához 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 – a jogi iroda és 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 főigazgató-helyettes és a szervezeti egység adatvédelmi felelősének tájékoztatása mellett felhívni a mulasztó szervezeti egység vezetőjét az ellenőrzés során észlelt esetleges hiányosságok megszüntetésére.

3. **Az ágazati igazgatók és a szervezeti egységek vezetőinek** feladatai

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

a) betartják és betartatják az adat- és titokvédelmi, valamint a 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) tájékoztatják az adatvédelmi tisztviselőt az adatvédelmi felelős személyéről és elérhetőségi adatairól,

d) gondoskodnak arról, hogy az irányításuk alá tartozó szervezeti egységek felelősségi körébe tartozó nyilvántartási rendszerek naprakészek, megbízhatóak legyenek,

h) gondoskodnak arról, hogy az irányításuk alatt álló személyek az adatkezelés meghatározott feltételeinek megfelelően járjanak el [GDPR 32. cikk (4) bek.], az általa irányított szervezeti egység adatvédelmi felelősének előterjesztésére – az Intézmény döntéselőkészítésre vonatkozó szabályainak megfelelően – döntenek a jelen utasításban, illetve az adatkezeléssel járó folyamatot szabályozó egyéb belső szabályzatokban a feladat- és hatáskörébe utalt kérdésekben.

4. A Jogi iroda feladatai

A Jogi iroda

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) szakmai támogatást nyújt az adatkezeléssel összefüggő, valamint a nem adatvédelmi jogszabályok értelmezésében.

c) az eseti meghatalmazás keretei között biztosítja az Intézmény képviseletét az érintett által az Intézmény ellen az érintett adatvédelmi jogainak megsértése miatt indított, illetve az Intézmény által a Nemzeti Adatvédelmi és Információszabadság Hatóság határozatainak felülvizsgálata iránt indított perekben, illetve egyéb eljárásokban.

5. Az Informatikai osztály feladatai

Az Informatikai osztály:

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 incidensfelderítési 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.

6. A szervezeti egységek adatvédelmi felelőseinek feladatai

Adatvédelmi felelőst valamennyi szervezeti egységnél ki kell jelölni. Szakellátási területen adatvédelmi felelősnek orvosi végzettségű személyt kell kijelölni, egyéb esetben az adott szervezeti egység vezetője látja el az adatvédelmi felelős feladatait. Az adatvédelmi felelősnek kellő ismeretekkel kell rendelkeznie az adott szakterület működését és munkafolyamatait, illetve a szakterületek tevékenységét támogató informatikai rendszereket illetően.

Kijelölés hiányában az adatvédelmi felelős a szervezeti egység vezetője.

Az adatvédelmi felelős az őt foglalkoztató 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 közreműködik,

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) rendszeresen kapcsolatot tart az adatvédelmi tisztviselővel és tájékoztatja a szervezeti egységet érintő új adatkezelésekről, illetve a szervezeti egységet érintő minden más adatkezelési tevékenységgel összefüggő ügyről,

j) 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 vezetővel 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.

VI. Adatkezelők, közös adatkezelők és adatfeldolgozás

Az Intézménnyel mindazon, a jelen Szabályzat I.2 pontja szerint jogviszonyban álló személy, aki személyes adat birtokába jut, munkaköre vagy tisztsége alapján személyes adatot kezel, köteles védeni és őrizni a személyes adatokat, és minden erőfeszítést megtenni annak érdekében, hogy

azoknak megfelelő védelmét biztosítsa. A szervezeti egység keretében tevékenységet végzők munkaköri leírása, illetve feladatleírása tartalmazza a dolgozó személyes adatok kezelésével és védelmével kapcsolatos feladatait, felelősségi körét.

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 Intézménnyel jogviszonyban állók, illetve az Intézmény képviseletében eljáró személyek kötelesek bizalmasan kezelni minden olyan személyes adatot, amely előttük a jogviszonyukkal összefüggésben vált ismertté.

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

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 megfelelőség 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.

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 megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

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 azt, 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 állnak;

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 megválaszolása 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

- az adatvédelmi incidens tudomására jutása esetén az Intézmény adatvédelmi tisztviselőjét haladéktalanul értesíteni köteles,
- köteles együttműködni az Intézmény adatvédelmi tisztviselőjével és más közreműködő szervezeti egységével az adatvédelmi incidens okának feltárásában és következményeinek felszámolásában,

- 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.

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

Az adatbiztonsági intézkedések megfelelőségének megítélése az informatikai osztály vezetője 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.

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.

Amennyiben szükséges, az adatkezelő és az adatfeldolgozó további 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.

Az Intézmény minden adatkezelés során köteles megvizsgálni, hogy a közös adatkezelés szükségessége fennáll-e. A döntés meghozatalára az adatvédelmi tisztviselő álláspontjának ismeretében a főigazgató jogosult.

Amennyiben döntés születik a közös adatkezelés bevezetéséről, az adatkezelés tárgya szerint illetékes szervezeti egység vezetője az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő és az egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a Jogi Iroda 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.

A közös adatkezelésről szóló megállapodásban meg kell határozni különösen

a) az adatkezelés célját, a kezelendő adatok körét, az adatkezelés időtartamát, az alkalmazandó adatbiztonsági intézkedéseket, az adatkezelés egyéb feltételeit,

b) azt, hogy a közös adatkezelésben érintett egyes adatkezelők

- mely adatkezelési műveleteket (pl. hozzájáruló nyilatkozatok felvétele, adatok tárolása, adatok felhasználása stb.) végzik,
- az érintett tájékoztatását hogyan végzik (pl. melyik adatkezelő készíti el az adatkezelési tájékoztatót és bocsátja az érintettek rendelkezésére stb.),
- az érintett jogainak gyakorlását hogyan biztosítják (pl. egyesített vagy elkülönített ügyfélszolgálat stb.),
- az esetleges jogellenes adatkezelés következményeit milyen arányban viselik;
- 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 kötelesek 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 adatkezelés bevezetése és megszüntetése

1. Az adatkezelés bevezetésével kapcsolatos feladatok

Új adatkezeléssel járó tevékenység 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, valamin az alkalmazandó adatkezelési tájékoztatót, valamint hozzájáruláson alapuló adatkezelés esetén a hozzájáruló nyilatkozat mintáját.

Új, személyes adatokra is kiterjedő nyilvántartási kötelezettség bevezetése főigazgatói utasítással történik. A főigazgatói utasítás tartalmazza

a) az adatkezelésért felelős szervezeti egységnek és egyéb szervezeti egységeknek az adatkezeléssel kapcsolatos feladatait, így különösen:
   - az adatok felvételének, módosításának, törlésének rendjét,
   - adatszolgáltatási kötelezettségek meghatározását az adatok naprakészen tartása érdekében,
   - a nyilvántartási rendszerből történő adattovábbítást, az ahhoz való hozzáférés rendjét.

b) mellékletként
   - a GDPR-nak, az Infotv.-nek és egyéb alkalmazandó jogszabályoknak megfelelő adatkezelési tájékoztatót,
   - hozzájáruláson alapuló adatkezelés esetén a hozzájáruló nyilatkozat mintáját.

Az adatkezelésért felelős szervezeti egység adatvédelmi felelősét az új adatkezelés bevezetésére vonatkozó igény megfogalmazásától kezdve be kell vonni az adatkezelés feltételek kidolgozásának a folyamatába.

Amennyiben az új adatkezelés bevezetése több szervezeti egységet érint, az adatkezelésért felelős valamennyi érintett szervezeti egység adatvédelmi felelősét be kell vonni az adatkezelés feltételeinek kidolgozási folyamatába. A fejlesztési igényt megfogalmazó szervezeti egység vezetője az egyéb területek adatvédelmi felelősei bevonásának szükségességéről az érintett adatvédelmi felelősöket és az adatvédelmi tisztviselőt értesíti.

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.

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):
   - 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),
   - 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.],

- amennyiben az adatkezelés jogalapja a jogos érdek lehet, elkészíti az érdekmérlegelési teszt dokumentumának tervezetét [GDPR 6. cikk (1) bek. f) pont],
- az adatvédelmi tisztviselő véleményének kikérése után javaslatot tesz a főigazgatónak adatvédelmi hatásvizsgálat elvégzésére; a főigazgató erre vonatkozó pozitív döntése esetén – az Informatikai osztály adatvédelmi felelősének 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.],
- előterjesztést tesz a főigazgatónak arról, hogy az adatkezelést közös adatkezelésként indokolt-e ellátni, illetve indokolt-e adatfeldolgozót bevonni,
- javaslatot tesz automatizált döntéshozatali módszer, illetve profilalkotási módszer alkalmazására [GDPR 22. cikk (1) bek.],
- megszövegezi a hozzájáruló nyilatkozat mintáját [GDPR 7. cikk (2) bek.], illetve a megfelelő szerződéses rendelkezéseket,
- megfogalmazza az adatkezelésről szóló tájékoztatást (GDPR 13-14. cikk),
- az informatikai osztály közreműködésével szükség esetén gondoskodik az adatkezelésről szóló tájékoztatás könnyen hozzáférhető módon való közzétételéről [GDPR 12. cikk (1) bek.],
- 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.],
- 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,
- 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 osztály adatvédelmi felelőse a személyes adatot kezelő rendszer fejlesztése és beszerzése során közreműködik

- a célhoz kötött adatkezelés és az adattakarékosság elvének megfelelően gyűjtött adatokra vonatkozóan a beépített és alapértelmezett adatvédelem elveinek dokumentált érvényesüléséről,
- annak biztosításában, hogy az adathordozhatóság, adattörlés és adattisztítás célú módosítások szabályozott és visszakereshető módon valósuljanak meg,

- annak biztosításában, hogy az adatvédelmi tájékoztatók és nyilatkozatok könnyen elérhetők legyenek az érintettek számára,
- annak biztosításában, hogy az adatkezeléssel kapcsolatos ügyfélrendelkezéseket visszakereshető formában tárolják,
- az adatok sértetlenségével, bizalmasságuk megőrzésével kapcsolatos kontrollok tervezéskori érvényesítésében, illetve dokumentált meglétében,
- az a) pont szerinti döntések előkészítésében.

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.

A fentiek szerint meghozott döntések, javaslatok véglegesítése előtt ki kell kérni az adatvédelmi tisztviselő véleményét, úgy, hogy az adatvédelmi tisztviselőnek legalább nyolc munkanapja legyen a vélemény adására.

Az adatvédelmi tisztviselő véleményének kikéréséhez olyan dokumentumot, leírást kell benyújtani, amely kellő részletességgel meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, illetve a fentiek szerint meghatározott egyéb döntési javaslatokat.

Az adatvédelmi tisztviselő adatvédelmi jogi támogatást nyújt az adatvédelmi felelős által előkészített, megszövegezett, adatkezeléshez kapcsolódó dokumentumok elkészítésében és közreműködik azok véglegesítésében. Az adatvédelmi tisztviselő megvizsgálja a véleményezésre megküldött dokumentumot, leírást adatvédelmi jogi szempontból, és abból a szempontból, hogy azok milyen módon illeszthetők be az Intézmény informatikai rendszereibe, illetve nincs-e a tervezett adatkezeléssel azonos vagy hasonló adatkezelés.

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

Az érintett 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.

Amennyiben az adatkezelés feltételei kidolgozásában részt vevő adatvédelmi felelősök között véleményeltérés van, illetve a Jogi iroda 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.

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 adatvédelmi felelős feladatai az adatkezelés során

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) alkalomszerű adattovábbítás esetén értesíti az adatvédelmi tisztviselőt az adattovábbítás tényéről legalább a 3. sz. mellékletben meghatározott adattartalommal az adattovábbítási nyilvántartás kiegészítése érdekében,

d) 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.],

e) 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.],

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

Az adatkezelés során (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.

Az adatkezelés megváltozott adatait – a változást elrendelő döntés után – át kell vezetni az adatkezelési nyilvántartásban.

3. Az adatkezelés megszüntetésével kapcsolatos feladatok

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 adatkezelésért felelős szervezeti egység vezetője – az adatvédelmi tisztviselő és szükség esetén az informatikai osztály vagy más érintett szervezeti egység álláspontjának kikérése után – javaslatot tesz a döntésre jogosultnak:

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

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

Az adatkezelés megszüntetésével kapcsolatosan az adatvédelmi tisztviselő álláspontját is tartalmazó írásbeli előterjesztést kell készíteni. Az adatkezelés megszüntetéséről a főigazgató vagy a Szervezeti és Működési Szabályzat alapján illetékes más személy jogosult döntést hozni.

VIII. Hatásvizsgálat

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 értékelhetőek.

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.

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:

a) 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;

b) a személyes adatok különleges kategóriái, vagy büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése; vagy

c) nyilvános helyek nagymértékű, módszeres megfigyelése.

A hatásvizsgálat kiterjed legalább:

a) a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;

b) az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;

c) az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és

d) 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.

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

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

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

b) az adatkezelés jogalapját, célját (az adatkezeléstől várt előnyöket, az adatkezelés szükségességét), terjedelmét (időben és a kezelt adatok volumenében),

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

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

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

f) az adatkezelés folyamatának a leírását.

A hatásvizsgálat második részében ki kell fejteni és meg kell indokolni

a) az adatkezelés szükségességének és arányosságának garanciáit,

b) az érintett jogait biztosító garanciák érvényesülését.

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

A hatásvizsgálat negyedik része tartalmazza a tervezett adatkezelés értékelését:

a) az első, második, valamint a harmadik részben meghatározott szempontok értékelését a tekintetben, hogy azok egyenként megfelelőek, további intézkedésekkel megfelelőek lehetnek, illetve nem megfelelőek;

b) a tervezett kiegészítő intézkedések végrehajtásának ütemtervét;

c) annak egyértelmű rögzítését, hogy a tervezett adatkezelés valószínűsíthetően magas kockázattal jár-e a természetes személyek jogaira nézve, és ennek alapján az adatkezelés megkezdhető-e, illetve szükség van-e az adatvédelmi felügyeleti hatósággal való konzultációra.

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:

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

b) a tervezett adatkezelés céljairól és módjairól;

c) az érintettek GDPR értelmében fennálló jogainak és szabadságainak védelmében hozott intézkedésekről és garanciákról;

d) az adatvédelmi hatásvizsgálatról; és

e) a felügyeleti hatóság által kért minden egyéb információról.

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

IX. Az érintett hozzájárulása, mint az adatkezelés jogalapja

Amennyiben az adatkezelés jogalapja az érintett hozzájárulása, úgy az Intézménynek igazolnia kell, hogy az érintett személyes adatainak kezeléséhez megfelelően hozzájárult.

Az érintett hozzájárulása akkor tekinthető az adatkezelés érvényes jogalapjának, amennyiben az az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez. A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés nem minősül hozzájárulásnak.

Az érintett hozzájárulása során biztosítani kell azt, hogy valódi választási lehetőség álljon az érintett rendelkezésére. Nem minősül önkéntesnek a hozzájárulás akkor, ha az érintettnek nem áll módjában a hozzájárulás anélküli megtagadása vagy visszavonása, hogy ez kárára válna, vagy, ha az érintett és az adatkezelő között egyértelműen egyenlőtlen viszony áll fenn.

Nem tekinthető önkéntesnek a személyes adatok kezeléséhez való hozzájárulás, amennyiben az érintettnek nincs lehetősége külön-külön hozzájárulást adnia a különböző személyes adatkezelési műveletekhez.

Az Intézménynek biztosítania kell azt, hogy az érintett a hozzájárulását bármikor visszavonhassa. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tennie, mint annak megadását.

Ha az Intézmény írásbeli nyilatkozaton keresztül szerzi be az érintett hozzájárulását, akkor a nyomtatványon a hozzájárulás iránti kérelmet egyértelműen és világosan el kell választani a nyilatkozat többi részétől, valamint ezen kérelmet érthető és egyszerű nyelvezettel kell az Intézménynek megfogalmaznia.

X. Érdekmérlegelés

Amennyiben az Intézmény valamely adatkezelése az Intézmény vagy harmadik személy jogos érdekén alapul [GDPR 6. cikk (1) bekezdés f) pont], érdekmérlegelési tesztet kell elvégezni. A jogos érdeken alapuló adatkezelés kizárólag az érdekmérlegelési teszt elvégzését és az adatvédelmi tisztviselő véleményének beszerzését követően kezdhető meg.

Jogos érdek az a törvényes, kellően pontosan megfogalmazott, valós és fennálló, illetve elérhető előny, amelyet az adatkezelő származtat – vagy a harmadik személy származtathat – az adatkezelésből.

Az érdekmérlegelési tesztet a tervezett adatkezelésért felelős szervezeti egység adatvédelmi felelőse végzi el az adatvédelmi tisztviselő közreműködése mellett. Az érdekmérlegelési tesztet írásban kell elvégezni. Az elkészült dokumentumot az adatvédelmi tisztviselőnek kell megküldeni, aki azt szakmai szempontból véleményezi.

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.

Az érdekmérlegelési teszt részei:

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

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

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

d) Itt szükséges kifejteni, 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) preambulumbekezdése 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.

a) Az érintett érdekeinek, jogainak azonosítása.

b) Itt szükséges kifejteni, 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.

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

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

e) Itt kell kifejteni, 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.

f) Biztosítékok leírása.

g) A kockázatot megszüntető vagy mérséklő intézkedési terv meghatározását tartalmazza.

h) 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.

i) 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.

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

XI. Belső adatvédelmi ellenőrzés

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. A magas kockázatú adatkezelési tevékenységeket évente kell felülvizsgálni. 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 tervezetére 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 tárgyévet követő év február 28. napjáig összefoglaló jelentést készít az általa a tárgyévben lefolytatott ellenőrzésekről, amelyet a főigazgató részére köteles megküldeni.

XII. Az érintett jogai és azok érvényesítése

1. Az érintett jogai

Az érintettet a személyes adataival összefüggésben az alábbi jogok illetik meg:

a) előzetes tájékoztatáshoz való jog (az adatfelvételt megelőzően az adatkezelés részleteivel kapcsolatban);

b) hozzáférési jog (tájékoztatás azzal kapcsolatban, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a kapcsolódó információkhoz hozzáférést kapjon);

c) helyesbítéshez való jog (pontatlan személyes adatok helyesbítése);

d) törléshez való jog;

e) adatkezelés korlátozásához való jog;

f) adathordozhatósághoz való jog;

g) tiltakozáshoz való jog.

2. Az érintett azonosítása

a) Az Intézmény az érintetti jogok gyakorlása esetén minden esetben köteles az érintett személyt kétséget kizáró módon beazonosítani, személyazonosságáról meggyőződni. Erre sor kerülhet például az érintett arcképes személyazonosító okiratának megtekintése, vagy az érintett által ismert azonosító kód, jelszó, legalább négy adat egyeztetése, vagy más, az eset összes körülményeire figyelemmel célszerű módon.

b) Az érintett kérésére szóbeli tájékoztatás is adható. Szóbeli tájékoztatás esetén az Intézmény az érintettet az a) pont szerint azonosítja be. Az érintett részére az Intézmény telefonon keresztül is adhat szóbeli tájékoztatást, amennyiben az Intézmény már rendelkezik az érintett személyes adataival, mert azt az érintett korábban személyesen megadta, vagy az Intézmény részére átadott meghatalmazásban szerepel.

c) Elektronikus úton történő tájékoztatás elsődlegesen, amennyiben lehetséges, elektronikus hitelesített csatornán (pl. E-papír, EESZT) kell, hogy megvalósuljon. Amennyiben erre nincs lehetőség, úgy e-mailen keresztül kiküldött titkosított fájl formában is megtörténhet a tájékoztatás. A titkosított fájl megnyitásához szükséges kódot az Intézmény másik kommunikációs csatornán (pl. SMS-ben) küldi meg az érintett részére, amennyiben az lehetséges. Másik kommunikációs csatorna hiányában (pl. ha nem áll rendelkezésre az érintett mobiltelefonszáma) az érintett személyes adataiból (pl. a TAJ száma, születési dátuma, stb.) képzett jelszóval kell titkosítani a fájlt. Az Intézménynek a tájékoztatást elektronikusan a beteg által megadott e-mail címre kell továbbítani a beteg vagy az általa felhatalmazott személy részére.

3. 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 tisztviselője 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 vagy az érintettek számára korlátozás nélkül elérhető más módon köteles közzétenni.

A 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.

A tájékoztatást

a) az Intézménynél az egészségügyi szolgáltatást igénybe vevő érintett részére az egészségügyi szolgáltatás igénybevételét megelőzően – amennyiben ez nem lehetséges pl. eszméletlen állapot miatt, úgy azt követően, miután a tájékoztatás lehetségessé vált – az egészségügyi szolgáltatásra vonatkozó adatkezelési tájékoztató szerinti tartalommal,

b) az Intézménnyel munkaviszonyt, közalkalmazotti jogviszonyt, megbízási vagy munkavégzésre irányuló egyéb jogviszonyt létesítő személyek részére a jogviszony létrejöttekor, az általános tájékoztatás az Intézmény vonatkozó adatkezelési tájékoztatója szerinti tartalommal,

c) az Intézményhez álláspályázatot benyújtók számára az álláspályázati felhívásban vagy válasz-levélben az Intézmény vonatkozó adatkezelési tájékoztatója szerinti tartalommal,

d) az Intézmény szolgáltatásait szerződéses jogviszony alapján igénybe vevő személyek számára az Intézmény vonatkozó adatkezelési tájékoztatója szerinti tartalommal kell megadni.

A tájékoztatást az Intézmény honlapján és az Intézményben elhelyezett tájékoztatókra való figyelemfelhívással kell megadni. Az tájékoztatókat – amely alól a munkavállalók részére szóló tájékoztató kivételt képez – az Intézmény honlapján, tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell elhelyezni.

Az egészségügyi szolgáltatást igénybevevők részére szóló adatkezelési tájékoztatót az egyes osztályok információs pultjánál, papír alapon, a beteg részére jól látható helyen is el kell helyezni.

A b) pont szerinti tájékoztatást papír alapon, elektronikusan vagy a szerződés szövegébe építve, a d) pont szerinti tájékoztatást a szerződés szövegébe építve is meg kell adni, magyar nyelven, nem

magyar anyanyelvű személy esetében az öt világnyelv (angol, francia, német, orosz, spanyol) valamelyikén.

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.

4. Az érintett tájékoztatáshoz való joga (hozzáféréshez való jog)

Az érintett– jogosultsága igazolását követően befogadott – kérelmére az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi tisztviselő 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 kérelmére az Intézmény köteles az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátani.

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

5. A helyesbítéshez való jog

Az érintett– jogosultsága igazolását követően befogadott – kérelmére az adatkezelést végző illetékes ügyintéző az adatvédelmi tisztviselő előzetes tájékoztatása és jóváhagyását követően indokolatlan késedelem nélkül:

a) helyesbíti az érintettre vonatkozó pontatlan személyes adatokat;

b) figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését is.

6. Az adatkezelés korlátozásához való jog

Az érintett– jogosultsága igazolását követően befogadott – kérelmére az adatkezelést végző illetékes ügyintéző 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 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 adatkezelést végző illetékes ügyintéző az érintettet, akinek a kérésére korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

7. Az 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.

8. A törléshez való jog

Az érintett– jogosultsága igazolását követően befogadott – kérelmére az adatkezelést végző illetékes ügyintéző 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 a közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

Ha az Intézmény nyilvánosságra hozta a személyes adatot, és azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az ésszerűen elvárható

lépéseket – ideértve technikai intézkedéseket – a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlése érdekében. Az informatikai osztályvezető 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) népegészségügy területét érintő 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.

9. A tiltakozáshoz való jog

Amennyiben az Intézmény az érintett adatait az alábbi jogalapokon kezeli:

a) az adatkezelés közérdekű feladat végrehajtásához szükséges; vagy

b) az adatkezelés az Intézmény vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges,

az érintett az így kezelt 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 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 vezetőjének bevonása mellett.

10. Jogorvoslathoz való jog

Az érintett az adatkezeléssel kapcsolatos jogainak megsértése esetén– az adatkezelést végző ügyintéző útján vagy közvetlenül az adatvédelmi tisztviselőhöz fordulhat, aki a panaszt megvizsgálja, és ha az alapos, az adatkezelő az Intézmény főigazgatójánál intézkedést kezdeményez, ellenkező esetben a panaszt elutasítja. Amennyiben az érintett panaszát nem közvetlenül az adatvédelmi tisztviselő útján teszi meg, úgy a panaszt haladéktalanul továbbítani kell az adatvédelmi tisztviselő részére.

Az elutasításról a panaszost a kérelem kézhezvételét követő 30 napon belül írásban tájékoztatja, a kérelem elutasításának ténybeli és jogi indokait is közölve. A kérelem elutasítása esetén a panaszost tájékoztatni kell a bírósági jogorvoslat, továbbá a felügyeleti szervhez fordulás lehetőségéről is. Az elutasított kérelmekről az adatvédelmi tisztviselő nyilvántartást köteles vezetni.

XIII. Az adatkezelés biztonsága

1. Adatbiztonsági szabályok

Az adatbiztonság érdekében az Intézmény felméri és nyilvántartja az általa végzett valamennyi adatkezelési tevékenységet. A nyilvántartást az adatvédelmi tisztviselő vezeti.

Az adatkezelési tevékenységek nyilvántartása alapján az Intézmény 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 GDPR-ral összhangban történik. Ideértve, többek között, adott esetben:

a) a személyes adatok álnevesítését és titkosítását;

b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;

c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;

d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

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 tisztviselővel egyetértésben dönt.

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

A manuálisan kezelt személyes adatok elvesztésének megelőzése érdekében eredeti iratokat csak hivatalos ügyintézés, különösen bírósági eljárás vagy nyomozati eljárás során lehet kiadni. 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 pótolt adatokon a pótlás tényét fel kell tüntetni.

2. Adatvédelmi incidens 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 személy akár saját, akár más, az Intézmény nevében végzett adatkezelése körében adatvédelmi incidens megtörtént észleli, vagy arról szerez tudomást, azt haladéktalanul jeleznie kell az adatvédelmi tisztviselő számára a jelen szabályzat 1. mellékletében található adatvédelmi incidens bejelentő lap kitöltése mellett. Ennek elmulasztása esetén az észlelő személy felelősséggel tartozik.

Adatvédelmi incidens bekövetkezése esetén az adatvédelmi tisztviselő az incidenssel érintett szervezeti egység adatvédelmi felelőse közreműködésével megvizsgálja, és a súlyosságának megfelelően kategorizálja a bekövetkezett incidenst és meghatározza a következmények elhárítása érdekében szükséges további intézkedéseket. Az incidens kapcsán tett megállapításokat írásban rögzíteni szükséges.

Adatvédelmi incidens bekövetkezése esetén az Intézmény adatvédelmi tisztviselője a Jogi iroda és szükség esetén az Informatikai osztály vagy más érintett szervezeti egység adatvédelmi felelősének (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.

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

a) a bejelentés személyes adatot érint-e,

b) amennyiben a bejelentés személyes adatot érint, megállapítható-e a személyes adatok köre,

c) megállapítható-e az incidensben érintett személyek köre,

d) a hatályos jogszabályok és belső szabályok alapján megállapítható-e, hogy személyes adat jogellenes kezelése vagy feldolgozása történt,

e) az incidens valószínűsíthetően magas kockázattal jár-e az érintettek jogaira és szabadságaira nézve,

f) melyek az adatvédelmi incidensből eredő, valószínűsíthető következmények,

g) az Intézmény által alkalmazott technikai és szervezési védelmi intézkedések alkalmasak-e arra, hogy az incidensben érintett személyes adatokhoz való hozzáférésre nem jogosult személyek számára értelmezhetetlenné tegyék az adatokat (pl. álnevesítés útján).

Az adatvédelmi incidenst az adatvédelmi tisztviselő indokolatlan késedelem nélkül, legkésőbb 72 órával azután, hogy az adatvédelmi incidens észlelésre került, bejelenti a 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 incidens kockázati besorolását az eset összes körülményének vizsgálatát követően az alábbi szempontok figyelembevételével állapítja meg az incidensvizsgáló bizottság:

a) magas kockázatúnak minősül az az incidens, amely vagyoni vagy nem vagyoni károkat okozhat az érintetteknek, az érintettek elveszítik 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.

b) 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 szolgáltatáskiesés, 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 incidens bejelentés vagy az incidensről való tudomásszerzés közül a korábbi időpontot követő egy napon belül írásban tájékoztatja:

a) a főigazgatót;

b) informatikai rendszert is érintő incidens esetén az információbiztonsági felelőst és informatikai és dokumentációs feladatok ellátásáért felelős vezetőt;

c) az illetékes főigazgató-helyettest,

d) 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.

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

A felügyeleti hatóság felé történő bejelentésben legalább:

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

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

c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

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

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

Az incidens vizsgálata során elsősorban az alábbi módszerek alkalmazhatóak:

a) személyes megbeszélés az adatvédelmi incidensben érintett személyekkel, valamint az érintett szervezeti egységek munkatársaival és vezetőivel,

b) írásbeli tájékoztatás kérése az érintett szervezeti egységektől,

c) dokumentumok vizsgálata,

d) 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:

a) az incidensben érintett személyes adatok körét és számát,

b) az adatvédelmi incidenssel érintettek körét és számát,

c) az adatvédelmi incidens időpontját,

d) az adatvédelmi incidens körülményeit, hatásait,

e) az adatvédelmi incidens elhárítására megtett intézkedéseket,

f) az adatvédelmi incidenssel kapcsolatban adott tájékoztatások adatait

Az adatvédelmi incidensek vizsgálata során keletkezett iktatott dokumentumokat a Főigazgatói 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 a főigazgató döntése alapján – 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:

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

b) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

c) 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, ha a következő feltételek bármelyike teljesül:

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

b) az Intézmény az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;

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

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 kommunikációs vezető útján – az Intézmény honlapján vagy országos lefedettségű sajtótermékben közzétett hirdetmény 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.

Az incidens kivizsgálása során az az érintett szervezeti egységek vezetőjének bevonásával az adatvédelmi tisztviselő az egyes feladatok felelőseit és határidejét is meghatározó intézkedési tervet készít, az abban foglaltak jóváhagyására a főigazgató jogosult.

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

XIV. Adattovábbítás

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.

Adattovábbítási megkeresések teljesítése:

a) Olyan megkeresés, amely az Intézmény által kezelt személyes adat továbbítására irányul csak jogszabályi előírás alapján, vagy csak a b) pontban foglalt feltételek fennállása esetén teljesíthető. Minden más esetben az adattovábbítás teljesítését meg kell tagadni.

b) Olyan esetben, amikor az adattovábbítás nem jogszabályi kötelezettségen alapul, a megkeresés csak akkor teljesíthető, ha az érintett ehhez – részletes tájékoztatást követően – igazolható módon hozzájárul.

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 jogalapnak 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.

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 rendeletben 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.

Az EESZT-hez csatlakozásra kötelezett egészségügyi szolgáltatók[1] között informatikai rendszerek közötti adatcsere esetén egészségügyi adat kizárólag az EESZT útján továbbítható.

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 úgy adja át, hogy gondoskodik arról, hogy azt az érintettel ne lehessen kapcsolatba hozni.

[1] Az Eüak. 35/B. § (1) bekezdése alapján:

a) az egészségügyi szolgáltatás nyújtására az egészségügyi államigazgatási szerv által kiadott működési engedély alapján jogosult egészségügyi szolgáltató, aki finanszírozási jelentés benyújtására vagy elektronikus adatszolgáltatásra kötelezett;
b) a gyógyszertár;
c) az állami mentőszolgálat,
d) a miniszter által rendeletben meghatározott államigazgatási szerv és egyéb szervezet (a 39/2016. (XII.21.) EMMI rendelet szerint: a Nemzeti Egészségbiztosítási Alapkezelő; Emberi Erőforrások Minisztériuma; Nemzeti Népegészségügyi Központ; Országos Gyógyszerészeti és Élelmezés-egészségügyi Intézet);
e) * az ártámogatási szerződéssel rendelkező gyógyászatisegédeszköz-forgalmazó.

XV. Automatizált döntéshozatal, profilalkotás

Az Intézmény nem hoz kizárólag automatizált adatkezelésen alapuló döntést az érintettel összefüggésben, valamint a rendelkezésre álló személyes adatok alapján az Intézet nem alkot profilt az érintettről.

KÜLÖNÖS RÉSZ

I. Betegadatok kezelése

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) a beteg testi, értelmi vagy lelkiállapotára, kóros szenvedélyére, a megbetegedés vagy elhalálozás körülményeire, okaira vonatkozik,

b) 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,

c) 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 jogszerű 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. Az egészségügyi adatok kezelésének célja

A betegek adatainak kezelésére sor kerülhet:

a) az egészség megőrzésének, fenntartásának előmozdítása,

b) az eredményes gyógykezelés elősegítése,

c) az érintett egészségi állapotának nyomon követése,

d) a közegészségügyi és járványügyi érdekből szükségessé váló intézkedések megtétele,

e) a betegjogok érvényesítése céljából, valamint

f) megfelelő jogalap fennállása esetén más törvényes célból.

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 orvosszakértő kivételével – azzal a betegellátóval szemben is köti, aki a beteg gyógykezelésében nem működött közre, kivéve, ha az adatok az érintett személy további gyógykezelése érdekében szükséges. 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

- házastársát vagy élettársát, ennek hiányában
- gyermekét, ennek hiányában
- szülőjét, ennek hiányában
- testvérét, ennek hiányában
- nagyszülőjét, ennek hiányában
- unokáját;

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

- gyermekét, ennek hiányában
- szülőjét, ennek hiányában
- testvérét, ennek hiányában
- nagyszülőjét, ennek hiányában
- unokáját.

A korlátozottan cselekvőképes 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 cselekvőképes 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 cselekvőképes 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 betegadatok felvétele során

A beteg – amennyiben ezt egészségi állapota lehetővé teszi – köteles az Eütv. 26. § (2) h) pontja alapján a jogszabályban előírt személyes adatait hitelt érdemlő módon igazolni. A személyazonosság igazolására alkalmas okmányok különösen: állandó és ideiglenes személyazonosító igazolvány; útlevél vagy járművezetői engedély. 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.

Amennyiben a beteg egészségi állapota nem teszi lehetővé azt, hogy igazolja személyazonosságát, úgy a beteg akkor köteles majd személyazonosságát igazolni, miután egészségi állapota ezt lehetővé tette.

Ha egy beteg személyazonossága nem állapítható meg, úgy az egészségügyi államigazgatási szerv felé kell fordulni. Az egészségügyi államigazgatási szerv az Intézmény jelzése alapján az ismeretlen

személyazonosságú beteg körözési eljárás keretében történő azonosítását rendelheti el személyazonosságának megállapítása érdekében.

A beteg egészségügyi ellátásának megkezdését megelőzően tájékoztatni kell a beteget az a kezelt adatok köréről, az adatkezelés céljáról, időtartamáról, az esetleges adattovábbításról, valamint az adatkezeléssel összefüggő minden lényeges körülményről. A beteg tájékoztatása szóban történik meg, valamint az Intézmény honlapján kihelyezett adatkezelési tájékoztatóval és az Intézményben elérhető adatkezelési tájékoztató kihelyezésével. A beteget szóban tájékoztatni kell az adatkezelési tájékoztatók elérhetőségéről. Az adatkezelési tájékoztató megismerését az Intézménynek, mint adatkezelőnek szükséges dokumentálni a betegfelvételi lapon vagy az ambuláns lapon, amelyet a beteg köteles aláírásával igazolni.

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 betegek adatainak kezelésével kapcsolatos általános tájékoztatást bárki számára elérhető módon közzé kell tenni az Intézmény honlapján, továbbá papír alapon minden betegellátó osztályon.

5. Adatkezelés a betegellátás, gyógykezelés során

Az egészségügyi adatok felvétele a gyógykezelés része. A kezelés során felvételre kerülnek a kötelezően rögzítendő személyes adatok, továbbá a feladat ellátásához szükséges mértékű 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,

a) 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 fertőzéses 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,

b) 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 vizsgálok stb.) elvégzéséhez van szükség,

c) heveny mérgezés esetén,

d) ha valószínűsíthető, hogy az érintett az Eüak. 3. számú melléklet szerinti foglalkozási eredetű megbetegedésben szenved (pl. szilikózis, azbesztózis stb.),

e) ha az adatszolgáltatásra a magzat, illetve a kiskorú gyermek gyógykezelése, egészségi állapotának megőrzése vagy védelme érdekében van szükség,

f) ha bűnüldözés, bűnmegelőzés céljából, továbbá ügyészségi, bírósági eljárás, illetve szabálysértési vagy közigazgatási hatósági eljárás során az illetékes szerv a vizsgálatot elrendelte,

g) ha az adatszolgáltatásra a nemzetbiztonsági szolgálatokról szóló törvény szerinti ellenőrzés céljából van szükség.

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 indokolttá 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 ellátóhálózat 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 és 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, a kezelt adatok körét megismerheti, az egészségügyi dokumentációba betekinthet, valamint azokról másolatot kérhet.

A beteg gyógykezelésével kapcsolatos tájékoztatást a beteg kezelőorvosa, illetve a jogszabályok és belső szabályozások által lehetővé tett körben általa erre feljogosított dolgozó adhat.

A beteg kezelésével összefüggő tájékoztatás – kifejezetten eltérő jogszabályi rendelkezés, illetve főigazgatói utasítás hiányában – kizárólag személyesen adható. A beteg által megjelölt személyek részére a beteg általános állapotára vonatkozó információ kiadható. A beteg által, kizárt személyek részére – törvény eltérő rendelkezése hiányában – nem adható semmilyen információ. A betegdokumentációban megfelelően rögzíteni szükséges, hogy kinek adható, illetve nem adható információ a betegről. A tájékoztatás megtörténtét a betegdokumentációban rögzíteni kell dátum és hely megjelölésével. Továbbá azt is rögzíteni kell, hogy pontosan kinek, mikor és mely adatok kerültek ismertetésre.

Telefonon keresztül a beteg kezelésével összefüggésben személyes adat nem adható ki.

Telefonon keresztül – a beteg ellenkező tartalmú nyilatkozata hiányában – az egészségügyi adatok megismerésére jogosult személy részére legfeljebb a kórházi tartózkodás tényéről adható információ.

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 meghatalmazást az egészségügyi dokumentáció részeként meg kell őrizni. A beteg egészségügyi ellátásának befejezését követően – törvény eltérő rendelkezése hiányában - csak a beteg által adott teljes bizonyító erővel rendelkező magánokiratban felhatalmazott személy jogosult az egészségügyi dokumentációba való betekintésre, és arról másolat készítésére.

A beteg lázlapja vagy más olyan dokumentum, amely a betegre vonatkozó személyes adatokat tartalmaz, kizárólag abban az esetben kerülhet kifüggesztésre, ha ehhez a beteg vagy törvényes képviselője előzetes tájékoztatást követően írásbeli hozzájárulást adott. Így például a lázlapok nem tarthatók a betegágy végén vagy másutt a kórteremben, illetve szabadon hozzáférhetően nem tárolhatók, kivéve a vizit idejét. A betegek nevét nem lehet a kórtermek ajtajánál kifüggeszteni. A kórlapokat nem lehet a nővérpulton vagy másutt úgy tárolni, hogy a személyazonosító adatok a helyiségben tartózkodók, a beteg ellátásában részt nem vevők által hozzáférhetők legyenek.

Betegazonosító karszalag 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 (például kódszám). képezhető

6. Egészségügyi dokumentáció vezetése és megsemmisítése

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 kötelező tartalmi elemeit az Eütv. 136. § (2) bekezdése tartalmazza. Az egészségügyi dokumentációt úgy kell vezetni, hogy az a valóságnak megfelelően tükrözze az ellátás folyamatát.

Az egészségügyi dokumentáció részeként meg kell őrizni:

a) az egyes vizsgálatokról készült leleteket;

b) a gyógykezelés és a konzílium során keletkezett iratokat;

c) az ápolási dokumentációt;

d) a képalkotó diagnosztikus eljárások felvételeit, valamint

e) a beteg testéből kivett szövetmintákat.

Az egészségügyi dokumentáció részét képező ápolási, fizioterápiás és dietetikai dokumentációt az egészségügyi szolgáltatások nyújtásához szükséges szakmai minimumfeltételekről szóló 60/2003. (X.20.) ESZCSM rendelet 4. mellékletében meghatározott formai és tartalmi követelmények szerint kell vezetni.

A betegdokumentáció megőrzési ideje:

Dokumentum típusa	Megőrzési ideje
Fekvőbeteg dokumentáció	30 év
Zárójelentés	50 év

Járóbeteg dokumentáció, ambuláns ellátási lap, vizsgálatkérő lapok	30 év
Képalkotó diagnosztikai eljárással készült felvételt az annak készítésétől számított	10 év
Képalkotó diagnosztikai eljárással készült felvételről készített leletet a felvétel készítésétől számított	30 év
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 év

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. 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.

Az adatmegőrzés érdekében folyamatosan biztosítani kell, hogy az adathordozó az adott technikai feltételek mellett olvasható maradjon, vagy olvasható állapotba kerüljön. 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 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.

Az egészségügyi dokumentáció selejtezéséről minden osztály vezetője köteles gondoskodni az Intézmény iratkezelési szabályzatának selejtezéséről szóló fejezete szerint.

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.

Jogszabály 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, fertőzéses eredetű betegségek, mérgezések fennállását, illetve kórokozóik jelenlétét valószínűsíti vagy igazolja. A betegellátó továbbítja az egészségügyi államigazgatási szervnek az Eüak. 1. számú melléklet A) pontja szerinti fertőzések, fertőzéses 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 kórházhigiénikusát 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

a) miniszteri rendeletben meghatározott vegyi anyag hatásának van kitéve, és szervezetében az anyag koncentrációja a megengedett mértéket meghaladja, valamint

b) 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 a főigazgató adja meg, az adatvédelmi tisztviselő álláspontjának ismeretében.

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 kutatási kérelmekről és a megadott engedély alapján személyes adatokat megismerő személyekről a Főigazgatóság 10 évig nyilvántartást vezet.

A kutatás során a tárolt adatokról 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.

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.

11. Népegészségügyi célból történő adatkezelés

Amennyiben az érintett beteg (ideértve a magzatot is) jogszabályban meghatározott veleszületett rendellenességben szenved, a rendellenességet észlelő orvos az észleléstől számított 30 napon belül az érintett személyazonosító és egészségügyi adatait, valamint – kiskorú esetén – törvényes képviselője nevét és lakcímét – miniszteri rendeletben meghatározott módon – továbbítja a Veleszületett Rendellenességek Országos Nyilvántartása részére.

Amennyiben a magzatnál olyan elváltozást észlelnek – ideértve a spontán vagy indukált magzati halálozás, illetve halvaszületés esetét is – amely veleszületett rendellenességet eredményezhet, az előző bekezdés szerint kell eljárni azzal, hogy az érintett személyazonosító adatain a várandós nő adatait kell érteni.

Az észlelő orvos és az érintett gondozását végző védőnő együttműködik a Veleszületett Rendellenességek Országos Nyilvántartását végző szervvel a veleszületett rendellenességek okainak feltárása céljából, azok megelőzése, a betegek gyógykezelésének nyomon követése érdekében. Spontán vagy indukált magzati halálozás, illetve halvaszületés esetén a kezelőorvos jár el.

Daganatos eredetű betegség észlelése esetén a betegellátó továbbítja az érintett egészségügyi és személyazonosító adatait a külön jogszabály szerint vezetett Nemzeti Rákregiszternek.

Szívinfarktussal diagnosztizált betegség észlelése esetén a betegellátó továbbítja az érintett személyazonosító és a szívinfarktus megbetegedésre vonatkozó adatait a Nemzeti Szívinfarktus Regiszter részére, és szükség esetén adategyeztetést folytat a Regiszterrel.

A lakossági célzott szűrővizsgálatok, a népegészségügyi szűrővizsgálatok, valamint a népegészségügyi szűrővizsgálatok körébe is tartozó szűrést végző egészségügyi szolgáltatók szűrővizsgálatai eredményeinek értékelése, monitorozása érdekében az egészségügyi szolgáltató a szűrővizsgálatban részt vett személyek személyazonosító adatait és a szűrővizsgálatra vonatkozó egészségügyi adatait, valamint a szűrővizsgálat időpontját továbbítja az egészségügyi államigazgatási szerv részére.

12. Egészségügyi szakemberképzés

A gyógykezelés során szakember-képzés céljából – tekintettel arra, hogy az Intézmény oktatásra is kijelölt intézmény - jelen lehet az érintett hozzájárulása nélkül is orvos, orvostanhallgató, egészségügyi szakdolgozó, valamint egészségügyi főiskola, szakközépiskola, szakiskola hallgatója, tanulója. Erről az érintettet (törvényes képviselőjét) a fekvőbeteg ellátás esetén legkésőbb a beutaláskor, beutaló hiányában a felvételt megelőzően, egyéb ellátás esetén legkésőbb a gyógykezelés megkezdése előtt tájékoztatni kell.

II. Munkatársi adatok kezelése

1. Pályázók adatainak kezelése

Az Intézmény által egészségügyi szolgálati jogviszony létrehozását megelőző pályázati eljárás során az érintett adatainak kezelése hozzájárulás alapján történik.

A pályázat 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 az érintett önkéntes hozzájárulása esetén, 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 az érintett kifejezett, írásbeli hozzájárulása hiányában a pályázati eljárás befejezésekor törölni kell.

A pályázók adatainak kezelésével kapcsolatos általános tájékoztatást valamennyi pályázó számára elérhetővé kell tenni.

2. Munkatársak adatainak kezelése

Az egészségügyi szolgálatijogviszonyban foglalkoztatott munkatársak esetében kizárólag a munkavégzéssel összefüggő célból, a 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 elengedhetetlenül szükségesek és a dolgozó személyhez fűződő jogait nem sértik.

A munkatársak 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 adatokhoz 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.

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

A munkatársak személyes adatainak kezelésével kapcsolatos általános tájékoztatást az érintettek számára elérhetővé kell tenni, valamint az abban foglaltakról a munkatársakat dokumentált formában tájékoztatni kell.

III. Szerződő partnerek adatainak kezelése

Az adatkezelés célja 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 általános tájékoztatást bárki számára elérhető módon közzé kell tenni az Intézmény honlapján.

IV. Manuálisan kezelt személyes adatok

Az Intézménynek az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lennie a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választania, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az Intézménynek

A manuálisan kezelt személyes adatok biztonsága érdekében az alábbi intézkedéseket kell foganatosítani:

a) az irattári kezelésbe vett iratokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben kell elhelyezni;

b) a folyamatos aktív kezelésben lévő iratokhoz csak az illetékes ügyintézők férhetnek hozzá, a személyzeti, a bér- és munkaügyi iratokat biztonságosan elzárva kell tartani,

c) a jelen szabályzatban meghatározott adatkezelések iratainak archiválását rendszeresen el kell végezni, az archivált iratokat az Intézmény iratkezelési és selejtezési szabályzatának, valamint az irattári terveknek megfelelően kell szétválogatni és irattári kezelésbe venni.

Az b) pont szerinti helyiségek, illetve szekrények kulcsához való hozzáférés rendjét az adatkezelő szervezeti egység vezetője állapítja meg, melyet az adatvédelmi tisztviselő részére tájékoztatásul megküld.

Amennyiben az iratok tárolását külső cég végzi, abban az esetben az Intézménynek szerződésben kell rögzítenie az irattároló cég részére a biztonságos és szakszerű irattárolás követelményeit.

V. Elektronikusan kezelt személyes adatok

Amennyiben az Intézmény olyan elektronikus rendszerben kezel személyes adatot, amelybe csak a hozzáférési listára felvett, nyilvántartott, illetékes személy léphet be, úgy az illetékes személynek egyéni, titkos jelszóval kell bejelentkeznie a rendszerbe. Az adatkezelés befejeztével a rendszerből ki kell lépni. A rendszerben történt, jelszóval védett adatkezelésért az adatkezelő felel. Az adatvédelmi incidensek elkerülése érdekében az illetékes adatkezelő kötelessége az egyén jelszavának a védelme. Az egyéni jelszó az illetékes adatkezelőn kívül kizárólag az adatkezelési szoftver fejlesztését, üzemeltetését ellátó informatikai munkatársak, által ismerhető meg, ha az az Intézménynél elvégzendő feladatuk ellátásához szükségessé válik.

Az adatkezelésre használt számítógépek adatbevitelre, lekérdezésre alkalmas állapotban történő, felügyelet nélkül hagyása tilos.

Az Intézmény kizárólag olyan adatkezelési rendszert alkalmazhat, amely a rendszerbe történt belépést regisztrálja, illetve a rögzített adatokról megállapítható, hogy az adatrögzítés ki által és milyen időpontban történt.

A személyes adatok vagy azokat tartalmazó dokumentáció megismerése érdekében elektronikus úton küldött beadványok/megkeresések csak a következő feltételek együttes érvényesülése esetén válaszolhatók meg elektronikus úton:

a) a kérelmező (adatkérő) egyértelműen azonosított (pl. Hivatali Kapun vagy E-papír szolgáltatáson keresztül, vagy az Intézménynél meglévő személyes adatok összevetése nyomán a kérelmező által megadott személyes adatokkal);

b) a kérelmező a hozzáférési jogosultságát igazolta;

c) az a személy, akinek a személyes adatait vagy egészségügyi dokumentációját kérik, egyértelműen azonosított;

d) a kért személyes adatok (egészségügyi dokumentáció), a beadványt/megkeresést fogadó egészségügyi intézményben keletkeztek, és elektronikus továbbításra alkalmas vagy azzá tehető formában rendelkezésre állnak;

e) az elektronikus adattovábbítás során a személyes adatok biztonsága mind az adatkezelő, mind az adatkérő oldalán biztosított (hitelesített csatorna, vagyis például EESZT vagy E-papír szolgáltatás vagy titkosított e-mail).

Nem biztonságos levelezőrendszeren (pl. gmail, outlook) keresztül személyes adatot tartalmazó dokumentum csak abban az esetben továbbítható, amennyiben elektronikus hitelesített csatorna nem áll rendelkezésre. Ebben az esetben a csatolt dokumentumot jelszóval kell levédeni és a titkosítés feloldásához szükséges jelszót egy másik kommunikációs csatornán (pl. sms, postai út) keresztül kell megküldeni a címzett részére.

A levelezőrendszer által felkínált levelezési felületen (pl.: outlook, gmail) személyazonosítást lehetővé tévő személyes adatok nem továbbíthatóak.

VI. Elektronikus beléptető rendszer

Az Intézménynél alkalmazott elektronikus beléptető rendszer célja az Intézmény által használt ingatlanba történő illetéktelen belépések, és az esetleges vagyon elleni bűncselekmények megtörténtének megakadályozása. Az elektronikus beléptető rendszert az Intézmény üzemelteti.

Az Intézménynél alkalmazott elektronikus beléptető rendszer által védett területre csak az arra jogosultak léphetnek be, illetőleg tartózkodhatnak. A jogosultság állandó belépésre jogosító belépőkártyával igazolható.

Állandó belépésre jogosító kártyával (ún. kulcs) az Intézménnyel munkaviszony, megbízási vagy más munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatottak rendelkeznek.

Az Intézmény az állandó belépésre jogosító kártyák használóiról nyilvántartást vezet (kártyanyilvántartás). A kártyanyilvántartás alábbi adatokat kezeli: (i) kártyaszám; (ii) a kártyahasználó neve.

A kártyabirtokos épületen belüli mozgásának rögzítésére a rendszer nem alkalmas.

A belépésre jogosultaknak az elektronikus beléptető rendszer működtetéséhez kezelt azonosító adatait az Intézmény a belépésre való jogosultság megszűnésekor haladéktalanul megsemmisíti, a kártyanyilvántartásból adatait a kártya leadást követően törli.

VII. Elektronikus térfigyelő rendszer

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 képfelvételek készülnek.

Az elektronikus térfigyelő rendszer adatkezelésére vonatkozó részletes szabályokat külön dokumentum tartalmazza.

VIII. Saját eszközzel történő munkavégzés

1. Jogosultak köre

Az Intézmény nevében, bármely jogviszony alapján tevékenységet végző természetes személy abban az esetben jogosult a munkavégzéséhez saját eszközt használni, amennyiben azt a főigazgató előzetesen, írásban engedélyezte.

2. Alkalmazott saját eszköz

Saját eszközzel történő munkavégzéshez személyi számítógép, laptop, táblagép vagy mobiltelefon használható.

A munkavégzéshez használt saját eszköz szervizelésére, az engedélyezett operációs rendszerekre, azok frissítési szintjére, vírus- és adatvédelmére, valamint egyéb IT biztonsági rendelkezésekre vonatkozóan az Intézmény Informatikai Biztonsági Szabályzata tartalmaz rendelkezéseket.

3. Saját eszközön történő munkavégzés szabályai

A munkatárs a saját eszközére az Intézmény kezelésében lévő adatokat, dokumentumokat nem tölthet le. Amennyiben mégis sor kerül letöltésre (például webmail használata esetén a munkatárs rákattint egy levél csatolmányára, ami így letöltődik a munkatárs saját eszközére), úgy a munkatárs köteles a letöltött állományt visszaállíthatatlanul törölni a saját eszközéről.

A távoli asztalon történő munkavégzés során a munkatárs köteles arról gondoskodni és úgy végezni a munkát, hogy harmadik személy (ideértve a családtagokat is) a saját eszközének képernyőjére semmilyen szögből ne lásson rá.

Amennyiben a munkatárs bármely okból, bármilyen rövid időre elhagyja a saját eszközét, úgy azt köteles zárolni.

A munkatárs a munkavégzést követően köteles kilépni az Intézmény által biztosított, saját eszközzel elért szolgáltatásból, továbbá – távoli munkavégzés esetén – lezárni a megnyitott biztonságos adatkapcsolatot (VPN-kapcsolatot) az Intézményi hálózat felé.

ZÁRÓ RENDELKEZÉSEK

Jelen Szabályzatot az Intézmény valamennyi szervezeti egysége számára folyamatosan hozzáférhetővé kell tenni.

Jelen Szabályzat aláírását követő napon lép hatályba. Jelen szabályzat hatálybalépésével egyidejűleg valamennyi, azonos tárgykörben kiadott szabályzat hatályát veszti. Jelen Szabályzat visszavonásig hatályos.

Kelt: Budapest, 2023. június 19.

Dr. Nagy Mihály
főigazgató

Budapesti Szent Margit Kórház 1. főigazgató

MELLÉKLETEK

1. sz. melléklet

Adatvédelmi incidens bejelentőlap

Kérjük a tudomásszerzést követően haladéktalanul kitölteni, és a **Budapesti Szent Margit Kórház** adatvédelmi tisztviselőjéhez eljuttatni szkennelten, e-mailen üzenetben (e-mail cím: adatvedelem@sztmargit.hu)!

I. Adatvédelmi incidensről tudomást szerző munkatárs

- neve:
- beosztása:
- munkahelyi elérhetősége:

II. Az adatvédelmi incidens

- az adatvédelmi incidensről való tudomásszerzés időpontja (év/hó/nap/időpont) és módja (pl.: panaszlevél; napló fájlból):

- rövid leírása:

- feltételezett időpontja, helye:

- által érintett személyek kategóriái és hozzávetőleges száma:
  - ☐ beteg
  - ☐ hozzátartozó, törvényes képviselő
  - ☐ munkavállaló
  - ☐ szerződött partner
  - ☐ egyéb2:
- által érintett személyes adatok köre és hozzávetőleges száma:

---

[2] Az „egyéb" szó után célszerű pontosan megjelölni, hogy milyen érintettekről van szó (pl. látogató).

- ☐ természetes személyazonosító adatok
- ☐ elérhetőségi adatok
- ☐ egészségi állapotra vonatkozó adatok
- ☐ pénzügyi adatok (pl. számlaszám, bankkártya szám stb.)
- ☐ egyéb3:

- 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)

_____

[3] Az „egyéb" szó után célszerű pontosan megjelölni, hogy milyen típusú személyes adatok sérültek (pl. fényképek).

2. sz. melléklet

Adatvédelmi incidens nyilvántartás

Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (GDPR) 33. cikk (5) bekezdésének való megfelelés, valamint a GDPR 5. cikk (2) bekezdésében foglalt elszámolhatóság érvényesítése érdekében a **Budapesti Szent Margit Kórház** az alábbi adatvédelmi incidens nyilvántartást vezeti.

#	Az adatvédelmi incidens időpontja, helye	Az adatvédelmi incidenssel érintettek köre, száma	Az érintett személyes adatok köre	GDPR 9. cikk, vagy 10. cikk szerinti adatot érint	harmadik országba továbbítás történt.	Az adatvédelmi incidens körülményei, az adatkezelést előíró jogszabályban meghatározott egyéb adatok	Az adatvédelmi incidens hatásai	Az adatvédelmi incidens elhárítására a megtett intézkedések	Bejegyzés dátuma, bejegyző neve, aláírása
1.									
2.									
3.									
4.									
5.									

3. sz. melléklet

Adattovábbítási nyilvántartás

Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (GDPR) preambulumának (111) bekezdésében foglalt elvárások teljesítésének ellenőrizhetősége, a GDPR 5. cikk (2) bekezdésében foglalt elszámolhatóság érvényesítése érdekében a **Budapesti Szent Margit Kórház az alábbi adattovábbítási nyilvántartást vezeti.**

#	Személyes adatok továbbításának időpontja	Az adatszolgáltatást teljesítő szervezeti egység megnevezése	Az adattovábbítás jogalapja és célja	A továbbított személyes adatok körének meghatározása	Az adattovábbítás címzettje	Harmadik országba történt adattovábbítás	az adatkezelést előíró jogszabályban meghatározott egyéb adatok, további megjegyzés	Bejegyzés dátuma, bejegyző neve, aláírása
1.								
2.								
3.								
4.								
5.								

4. sz. melléklet

Az érintett hozzáférési jogával kapcsolatos intézkedésekről szóló nyilvántartás

Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (GDPR) 5. cikk (2) bekezdésében foglalt elszámolhatóság érvényesítése, valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 25/E.§ (1) bekezdésében foglalt kötelezettségének teljesítése érdekében a **Budapesti Szent Margit Kórház** az alábbi nyilvántartást vezeti.

#	A hozzáférési jogát érvényesíteni kívánó érintett neve, elérhetősége	Az érintett érvényesíteni kívánt hozzáférési jogának jellege (kérelem tartalma)	A jogérvényesítési kérelem benyújtásának dátuma	A hozzáférési jogát érvényesíteni kívánó érintett esetében történő adatkezelés jogalapja	A jogérvényesítési kérelem teljesítése érdekében tett intézkedés	A jogérvényesítési kérelem teljesítésének dátuma	A hozzáférési jogot korlátozó vagy megtagadó intézkedések jogi és ténybeli indokai	Bejegyzés dátuma, bejegyző aláírása
1.								