Kiosztási lista

Köteles példányt kapnak:

Minőségirányítási Cs.		
Jogi Iroda		

További kiosztandó példányok:

Példány-szám	Szervezeti egység / dolgozó	Példány-szám	Szervezeti egység / dolgozó

A módosult Változat			Adminiszt-
száma	hatályba lép	által érintett helyek (pontok, oldalszámok...)	rálta

Koordinátor:	Minőségirányítási felülvizsgáló:	Jóváhagyó:
Dr. Berta Lilla adatvédelmi tisztviselő	György Béláné minőségirányítási előadó	Dr. Vácity József főigazgató Dátum: 2023. 09. 20

I. Tartalomjegyzék

II. Általános rendelkezések

II.1. A szabályzat célja

Jelen Szabályzat célja, annak biztosítása, hogy aHeves Vármegyei Markhot Ferenc Oktatókórház és Rendelőintézet(továbbiakban: Intézmény, vagy Adatkezelő) által folytatott adatkezelések megfeleljenek a hatályos jogszabályi előírásoknak. A Szabályzat célja továbbá, hogy az Európai Parlament és a Tanács (EU) 2016/679. sz. rendelete 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 rendeletnek (a továbbiakban: GDPR, vagy Rendelet), és az abban megfogalmazott, a személyes adatok kezelésére vonatkozó elveknek (5. cikk) való megfelelés Intézmény általi igazolására szolgáljon.

II.2. A szabályzat tárgyi hatálya

A szabályzat tárgyi hatálya kiterjed azIntézménynél végzett minden adatkezelésre és adatfeldolgozásra, függetlenül azok kezelési módjától.

II.3. A szabályzat alanyi hatálya

A szabályzat alanyi hatálya kiterjed azIntézményvalamennyi szervezeti egységére, ésazIntézménnyel munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álló szervezetekre, személyekre.

A Szabályzat hatálya nem terjed ki az olyan adatok kezelésre, amelyek jogi személyekre vonatkoznak, beleértve a jogi személy nevét és formáját, valamint a jogi személy elérhetőségére vonatkozó adatokat.

II.4. Kapcsolódó jogszabályok

II.4.1.1. Kapcsolódó jogszabályok a következők:

- az Európai Parlament és a Tanács (EU) 2016/679. sz. rendelete 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 (a továbbiakban: GDPR, vagy Rendelet)

- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (a továbbiakban: Infotv.)
- 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (továbbiakban: Szvtv.)
- 2013. évi V. törvény a Polgári Törvénykönyvről (továbbiakban: Ptk.)
- 2000. évi C. törvény a számvitelről (továbbiakban: Számv. tv.)
- 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről (továbbiakban: Eüat.)
- 1997. évi CLIV. törvény az egészségügyről (a továbbiakban: Eütv.)
- 62/1997. (XII. 21.) NM rendeletaz egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről (továbbiakban: Eüakr.)

II.5. Fogalmak

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

„adatkezelés”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

„az adatkezelés korlátozása”: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

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

„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;

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

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

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

„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;

„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 adatok véletlen vagy jogellenes megsemmisítését, elvesztését,

megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

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

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

„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;

„tevékenységi központ”:

- az egynél több tagállamban tevékenységi hellyel rendelkező Adatkezelő esetében az Unión belüli központi ügyvitelének helye, ha azonban a személyes adatok kezelésének céljaira és eszközeire vonatkozó döntéseket az Adatkezelő egy Unión belüli másik tevékenységi helyén hozzák, és az utóbbi tevékenységi hely rendelkezik hatáskörrel az említett döntések végrehajttatására, az említett döntéseket meghozó tevékenységi helyet kell tevékenységi központnak tekinteni;
- az egynél több tagállamban tevékenységi hellyel rendelkező adatfeldolgozó esetében az Unión belüli központi ügyvitelének helye, vagy ha az adatfeldolgozó az Unióban nem rendelkezik központi ügyviteli hellyel, akkor az adatfeldolgozónak az az Unión belüli tevékenységi helye, ahol az adatfeldolgozó tevékenységi helyén folytatott tevékenységekkel összefüggésben végzett fő adatkezelési tevékenységek zajlanak, amennyiben az adatfeldolgozóra e rendelet szerint meghatározott kötelezettségek vonatkoznak;

„képviselő”: az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az Adatkezelő vagy adatfeldolgozó által a 27. cikk alapján írásban megjelölt természetes vagy jogi személy, aki, illetve amely az Adatkezelőt vagy adatfeldolgozót képviseli az Adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában;

„vállalkozás”: gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is;

„vállalkozáscsoport”: az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások;

„kötelező erejű vállalati szabályok”: a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező Adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli Adatkezelő vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ;

„felügyeleti hatóság”: egy tagállam által a GDPR 51. cikknek megfelelően létrehozott független közhatalmi szerv;

„érintett felügyeleti hatóság”: az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint:

- az Adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel;
- az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy
- panaszt nyújtottak be az említett felügyeleti hatósághoz;

„személyes adatok határokon átnyúló adatkezelése”:

- személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező Adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy
- személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az Adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket;

„releváns és megalapozott kifogás”: a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy ezt a rendeletet megsértették-e, illetve hogy az Adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira

és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét;

„az információs társadalommal összefüggő szolgáltatás”: az (EU) 2015/1535 európai parlamenti és tanácsi irányelv (19) 1. cikke (1) bekezdésének b) pontja értelmében vett szolgáltatás;

„nemzetközi szervezet”: a nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei, vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre, vagy amely ilyen megállapodás alapján jött létre.

„Adatállomány”: az egy nyilvántartásban kezelt adatok összessége;

III. Az adatkezelés alapelvei

Jogszerűség, tisztességes eljárás és átláthatóság elve:

A személyes adatok felvételének és kezelésének tisztességesnek és jogszerűnek kell lennie. Az adatok kezelését az érintett számára átlátható módon kell végezni.

Célhozkötöttség elve:

A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, azok nem kezelhetők ezekkel a célokkal össze nem egyeztethető módon. Nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.

Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának. A célhoz kötöttség elve nem felülírható vagy pótolható az adatalany hozzájárulásával.

Szükségszerűség/adattakarékosság elve:

Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlenül szükséges és a cél elérésére alkalmas (megfelelő, releváns). A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

Pontosság elve:

A személyes adatoknak pontosnak és naprakésznek kell lenniük; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul törlésre vagy helyesbítésre kerüljenek.

Korlátozott tárolhatóság:

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 közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor.

Integritás és bizalmas jelleg:

A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, ideértve az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is.

Beépített és alapértelmezett adatvédelem:

Az Adatkezelőnek - mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során - az adatvédelem elveinek és az érintett jogainak védelméhez szükséges garanciák érvényesülését biztosító megoldásokat (technikai és szervezési intézkedéseket, pl. álnevesítés) kell beépítenie az adatkezelés teljes folyamatába.

Ezen intézkedések és garanciák megvalósítása során az alábbi szempontokat kell figyelembe venni:

- a tudomány és a technika adott fejlettségi szintje;
- a megvalósítás költségei;
- az adatkezelés jellege, hatóköre, körülményei és céljai;
- a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat

Az Adatkezelőnek az adatkezelés folyamatában minden lépésben biztosítani kell, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerülhessen csak sor, amelyek az adott konkrét adatkezelési cél elérése szempontjából feltétlenül szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre egyaránt.

Elszámoltathatóság elve:

Az Adatkezelő felelős az adatkezelés elveinek a maradéktalan betartásáért, az azoknak való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására

IV. Az adatkezelés jogszerűsége, célja

IV.1. Az adatkezelés jogalapja

A GDPR szerint a személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül, azaz valamelyik az Adatkezelő rendelkezésére áll.

a) érintett hozzájárulása: az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez. Az érintett hozzájárulása csak abban az esetben tekinthető megfelelőnek, ha az önkéntes és megfelelő tájékoztatáson alapul.Ha az adatkezelés hozzájáruláson alapul, az Adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult, ezért az érintett hozzájárulását írásba kell foglalni vagy egyéb módon kell bizonyíthatóvá tenni. Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely egyidejűleg más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Amennyiben az érintett hozzájárulása nem állapítható meg egyértelműen, illetve nem igazolható, hogy az megfelelő tájékoztatáson alapult, a hozzájárulást nem szolgálhat az adatkezelés jogalapjaként. Az érintett hozzájárulásának is az egyes ügyek vonatkozásában jól elkülöníthetőnek kell lennie. A hozzájáruló nyilatkozat bármely olyan része, amely a GDPR rendelkezéseivel ellentétes, érvénytelennek kell tekinteni. Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. 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, világos, és egyértelmű módon kell lehetővé tenni, mint annak megadását.

b) Szerződés teljesítése: az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges.

c) Jogi kötelezettség teljesítése: az adatkezelés az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges. Jogi kötelezettség alatt az uniós vagy tagállami jogszabályi rendelkezéseket kell érteni.

d) Jogos érdek: az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.A jogos érdeken alapuló adatkezelés meghatározása előtt el kell végezni az ún. érdekmérlegelési tesztet, amelynek során először azonosítani kell az Adatkezelő jogos érdekét, a súlyozás ellenpontját képező adatalanyi érdeket és az érintett alapjogot, végül a súlyozás elvégzése alapján meg kell állapítani, hogy kezelhető-e a személyes adat.

   Érdekmérlegelés alapján személyes adat kezelésére az érintett további külön hozzájárulása nélkül valamint a hozzájárulásának a visszavonását követően kerülhet sor az alábbi feltételek fennállása esetén:

   - a személyes adatok felvételére az érintett hozzájárulásával került sor,
   - az adatkezelésre az Adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából vagy
   - az Adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából kerül sor, feltéve, hogy ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

e) Létfontosságú érdek: az adatkezelés az érintett életének vagy más természetes személy létfontosságú érdekeinek védelmében történik. Más természetes személy létfontosságú érdekeire hivatkozással személyes adatkezelésre elvben csak akkor kerülhet sor, ha a szóban forgó adatkezelés egyéb jogalapon nem végezhető. (Létfontosság érdekre hivatkozással történhet pl. az adatkezelés humanitárius katasztrófák esetében, ideértve, azt az esetet is, ha arra a járványok és terjedéseik nyomon követéséhez van szükség.)

IV.2. Az adatkezelés célja

A GDPR 5. cikk (1) bekezdésének b) pontja alapján a személyes adatok kezelése csak meghatározott, egyértelmű és jogszerű célból történhet, azok nem kezelhetők ezekkel a célokkal össze nem egyeztethető módon.

Az Eüat. az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelése vonatkozásában célként az alábbiakat határozza meg:

a) az egészség megőrzésének, javításának, fenntartásának előmozdítása,

b) a betegellátó eredményes gyógykezelési tevékenységének elősegítése, ideértve a szakfelügyeleti tevékenységet is,

c) az érintett egészségi állapotának nyomon követése,

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

e) a betegjogok érvényesítése.

Ezen célokon felül – törvényben meghatározott esetekben –személyes adatok az alábbi célokból is kezelhetőek:

a) egészségügyi szakember-képzés,

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

c) statisztikai vizsgálat,

d) hatásvizsgálati célú anonimizálás és tudományos kutatás,

e) az egészségügyi adatot kezelő szerv vagy személy hatósági vagy törvényességi ellenőrzését, szakmai vagy törvényességi felügyeletét végző szervezetek munkájának elősegítése, ha az ellenőrzés célja más módon nem érhető el, valamint az egészségügyi ellátásokat finanszírozó szervezetek feladatainak ellátása,

f) a társadalombiztosítási, illetve szociális ellátások megállapítása, amennyiben az az egészségi állapot alapján történik, valamint a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról szóló törvény szerinti rendvédelmi egészségkárosodási ellátás megállapítása,

g) az egészségügyi ellátásokra jogosultak részére a kötelező egészségbiztosítás terhére igénybe vehető szolgáltatások rendelésének és nyújtásának, valamint a gazdaságos gyógyszer-, gyógyászati segédeszköz- és gyógyászati ellátás rendelési szabályai betartásának a vizsgálata, továbbá a külön jogszabály szerinti szerződés alapján a jogosultak részére nyújtott ellátások finanszírozása, illetve az ártámogatás

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

h) bűnüldözés, továbbá a rendőrségről szóló 1994. évi XXXIV. törvényben meghatározott feladatok ellátására kapott felhatalmazás körében bűnmegelőzés,

i) a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben meghatározott feladatok ellátása, az abban kapott felhatalmazás körében,

j) közigazgatási hatósági eljárás,

k) szabálysértési eljárás,

l) ügyészségi eljárás,

m) bírósági eljárás,

n) a munkavégzésre való alkalmasság megállapítása függetlenül attól, hogy ezen tevékenység munkaviszony, közalkalmazotti, kormányzati szolgálati, közszolgálati vagy állami szolgálati jogviszony, hivatásos szolgálati viszony vagy egyéb jogviszony keretében történik,

o) közoktatás, felsőoktatás és szakképzés céljából az oktatásra, illetve képzésre való alkalmasság megállapítása,

p) a katonai szolgálatra, illetve a személyes honvédelmi kötelezettség teljesítésére való alkalmasság megállapítása,

q) munkanélküli ellátás, foglalkoztatás elősegítése, valamint az ezzel összefüggő ellenőrzés,

r) az egészségügyi ellátásokra jogosultak részére vényen rendelt gyógyszer, gyógyászati segédeszköz és gyógyászati ellátás folyamatos és biztonságos kiszolgáltatása, illetve nyújtása érdekében,

s) a munkabalesetek, foglalkozási megbetegedések - ideértve a fokozott expozíciós eseteket is - kivizsgálása, nyilvántartása és a szükséges munkavédelmi intézkedések megtétele,

t) az egészségügyi dolgozókkal szemben lefolytatott etikai eljárás,

u) eredményesség alapú támogatásban részesülő gyógyszerek, gyógyászati segédeszközök eredményességének, támogatásának megállapítása, és ezen gyógyszerekkel kezelt kórképek finanszírozási eljárásrendjének alkotása,

v) betegút-szervezés,

w) az egészségügyi szolgáltatások minőségének értékelése és fejlesztése, az egészségügyi szolgáltatások értékelési szempontjainak rendszeres felülvizsgálata és fejlesztése,

x) az egészségügyi rendszer teljesítményének ellenőrzése, mérése és értékelése,

y) az egészségügyi ellátásokra jogosult részére a hatásos és biztonságos gyógyszerelés elősegítése, valamint a költséghatékony gyógyszeres terápia kialakítása érdekében,

Nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.

Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának.

V. A személyes adatok különleges kategóriáinak kezelése

A különleges adatok kategóriái különösen: faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre, stb. utaló személyes adatok; **egészségügyi adat**, biometrikus adat, genetikai adat.

Főszabály szerint a különleges kategóriájú adatok kezelése GDPR szerint tilos. Az alábbi kivételes esetekben lehet különleges adatot kezelni:

- az érintett kifejezett hozzájárulását adta az említett személyes adatok meghatározott célból történő kezeléséhez, és uniós vagy tagállami jog nem tiltja a hozzájárulás-adást;
- az adatkezelés az Adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi;
- az adatkezelés létfontosságú érdek védelméhez szükséges, feltéve, hogy az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;
- az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
- az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges;
- az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása érdekében szükséges

VI. Tájékoztatás

VI.1. Általános követelmények

Az érintett részére adott tájékoztatásnak tömörnek, átláthatónak, érthetőnek és könnyen hozzáférhetőnek kell lennie. Írásban vagy más módon, világos és közérthető formában kell megfogalmazni. Az elszámoltathatóság (bizonyíthatóság) érdekében minden esetben ajánlott az írásbeli forma.

VI.2. Tájékoztatásra vonatkozó szabályok, ha a személyes adatok az érintettől származnak (előzetes tájékoztatás)

Ha a személyes adatok az érintettől származnak, azIntézmény, mint Adatkezelő a személyes adatok felvételének, rögzítésének időpontjában köteles az érintett rendelkezésére bocsátani az alábbi információkat (előzetes tájékoztatás):

- az Adatkezelőnek és az adatkezelő képviselőjének a megnevezése és elérhetőségei (Adatkezelő neve; postai címe, e-mail címe, honlapcíme; nem kötelező jelleggel telefonszám, egyéb azonosító adat – pl. cégjegyzékszám; képviselő neve, céges e-mail címe);
- azadatvédelmi tisztviselő elérhetőségei; (azIntézménynél nem kötelező az az adatvédelmi tisztviselő kijelölése, ennél fogva ez nem szerepel a tájékoztatóban)
- a tervezett adatkezelés célja (konkrét, pontos megjelölés, valós célok elfedése nélkül), valamint az adatkezelés jogalapja;
- jogos érdeken alapuló adatkezelés esetén, az Adatkezelőnek vagy harmadik félnek az érdekmérlegelési teszt alapján kimutatott jogos érdeke;
- adattovábbítás esetén a személyes adatok címzettjei, illetve a címzettek kategóriái;
- harmadik országba, nemzetközi szervezethez történő adattovábbítás ténye és garanciái;
- a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- az érintett jogainak ismertetése, miszerint kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését, kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való joga;

- hozzájáruláson alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonási joga;
- a Felügyeleti hatósághoz címzett panasz benyújtásának joga;
- arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása;
- automatizált döntéshozatal ténye (ideértve a profilalkotást is), logikája, és hogy ennek milyen következményei lehetnek az érintettre vonatkozóan.

A tájékoztatást egyébként a személyes adatok felvételével együtt járó eljárás (pl. telephelyre való belépés, munkaviszony megkezdése, érintettel való kapcsolatfelvétel, stb.) megkezdésével egyidejűleg kell az érintettek részére megadni. A tájékoztatás megadása történhet az adatkezelésre vonatkozó tájékoztató papír alapon történő átadásával, vagy – amennyiben az adatkezelés jellegéből adódóan az érintettnek lehetősége van az Adatkezelő honlapjának előzetes megtekintésére – az Adatkezelő honlapján elhelyezett adatkezelési tájékoztatás megjelölésével.

Az Adatkezelési Tájékoztatót a személyesen jelen lévő érintett kérésére nyomtatott formában át kell adni.

VI.3. Tájékoztatás, ha a személyes adatok nem az érintettől származnak (utólagos tájékoztatás)

AzIntézménynek, mint Adatkezelőnek – amennyiben a személyes adatokat nem az érintettől szerezte – az adatok megszerzésétől számított ésszerű határidőn, de legkésőbb egy hónapon belül kell az adatkezelésre vonatkozó tájékoztatást az érintett részére megadnia.

Ez a határidő az alábbi feltételek esetén a következőképpen módosul:

- ha az Adatkezelő a személyes adatokat az érintettel való kapcsolattartás céljára akarja felhasználni, legalább az érintettel való első kapcsolatfelvétel alkalmával;
- ha az Adatkezelő más címzettel is közölni akarja az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor;
- ha az Adatkezelő a személyes adatokon a megszerzésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően kell tájékoztatnia az érintettet erről az eltérő célról és minden releváns kiegészítő információról.

Ha a személyes adatok nem az érintettől származnak, azIntézmény, mint Adatkezelő a fenti időpontokban köteles az érintett rendelkezésére bocsátani az alábbi információkat:

- az Adatkezelőnek és – ha van ilyen – az Adatkezelő képviselőjének a kiléte és elérhetőségei (Adatkezelő neve; postai címe, e-mail címe, honlapcíme; nem kötelező jelleggel telefonszám, egyéb azonosító adat – pl. cégjegyzékszám; képviselő neve, céges e-mail címe);
- azadatvédelmi tisztviselő elérhetőségei; (azIntézménynél nem kötelező az az adatvédelmi tisztviselő kijelölése, ennél fogva ez nem szerepel a tájékoztatóban)
- a tervezett adatkezelés célja (konkrét, pontos megjelölés, valós célok elfedése nélkül), valamint az adatkezelés jogalapja;
- az érintett személyes adatok kategóriái;
- adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái;
- harmadik országba, nemzetközi szervezethez történő adattovábbítás ténye és garanciái;
- a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- jogos érdeken alapuló adatkezelés esetén, az Adatkezelőnek vagy harmadik félnek az érdekmérlegelési teszt alapján kimutatott jogos érdeke;
- az érintetti jogok ismertetése, miszerint kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését, kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való joga;
- hozzájáruláson alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonási joga;
- a felügyeleti hatósághoz címzett panasz benyújtásának joga;
- a személyes adatok forrása, illetve hogy az adatok nyilvánosan hozzáférhető forrásból származnak-e;
- automatizált döntéshozatal ténye (ideértve a profilalkotást is), logikája, és hogy ennek milyen következményei lehetnek az érintettre vonatkozóan.

AzVI.2. pont szerinti tájékoztatástól annyiban el lehet tekinteni, amennyiben:

- a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne. Ezekben az esetekben is azonban az

Adatkezelőnek megfelelő intézkedéseket kell hoznia – az információk nyilvánosan elérhetővé tételét is ideértve – az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében;

- az adatkezelést uniós vagy tagállami jogszabály írja elő, és rendelkezik a megfelelő garanciákról;
- uniós vagy tagállami jogszabályban előírt szakmai titoktartási kötelezettség alapján bizalmasnak kell maradnia.

VII. Az érintettek jogai

VII.1. Az érintett hozzáférési / tájékoztatáshoz való joga

Az érintett jogosult arra, hogy az Adatkezelőtől tájékoztatást kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha igen, jogosult arra, hogy a személyes adataihoz és a következő információkhoz hozzáférést kapjon:

- az adatkezelés célja;
- az érintett személyes adatok kategóriái;
- 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. Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan;
- a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- 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;
- a Felügyeleti hatósághoz címzett panasz benyújtásának joga;
- ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
- az 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.

Az Adatkezelőnek az adatkezelés tárgyát képező személyes adatok másolatát az érintett kérésére ingyenesen rendelkezésére kell bocsátania. A tájékoztatás megadása azonban nem érintheti hátrányosan mások jogait és szabadságaitazaz az érintett rendelkezésére kizárólag a róla kezelt adatok bocsáthatók. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett ezt másként kéri.

VII.2. Törléshez („elfeledtetéshez”) való jog

Az érintett kérésére az Adatkezelőnek indokolatlan késedelem nélkül törölnie kell a rá vonatkozó személyes adatokat.

Ezen túlmenően is az Adatkezelő köteles az érintettre vonatkozó személyes adatok indokolatlan késedelem nélkül törlésére, ha:

- a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
- az érintett hozzájárulását visszavonta, feltéve, hogy nincs más jogalap;
- az érintett tiltakozik az adatkezelés ellen, és az Adatkezelőnek nincs elsőbbséget élvező jogszerű oka az adatkezelésre. Ha az érintett a közvetlen üzletszerzés céljából gyűjtött adatai kezelése ellen tiltakozik, az adatokat törölni kell;
- a személyes adatokat jogellenesen kezelték;
- uniós vagy tagállami jogban előírt jogi kötelezettség írja elő a törlést;
- a személyes adatok gyűjtésére közvetlenül a gyermekeknek kínált, információs társadalommal összefüggő szolgáltatásokkal kapcsolatosan – a szülői felügyeletet gyakorló személy hozzájárulásának hiányában - került sor.

Ha az Adatkezelő nyilvánosságra hozta a személyes adatot, és azt a fentiek értelmében törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével minden ésszerűen elvárható lépést meg kell tennie – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő többi Adatkezelőt arról, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

Nem lehet az adatokat törölni, ha az adatkezelés:

- a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából szükséges;
- a személyes adatok kezelését előíró, uniós vagy tagállami jog szerinti kötelezettség teljesítése érdekében szükséges;
- közérdekű archiválás, tudományos és történelmi kutatási vagy statisztikai célból szükséges és a törlés lehetetlenné tenné vagy komolyan veszélyeztetné az adatkezelést;
- jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges (pl. az adatokra bírósági eljárásban, bizonyítékként való felhasználás céljából van szükség).

Amennyiben az érintett olyan személyes adatokat bocsát az Adatkezelő rendelkezésére, amelyek az adott adatkezelési cél eléréséhez nem szükségesek, az Adatkezelő a célszerűség elvével össze nem egyeztető adatokat – amennyiben az aránytalan terhet és költséget nem jelent - indokolással ellátva visszaküldi az érintettnek, vagy abban az esetben, amikor az adatok visszaküldése nem lehetséges (pl. fénymásolat, elektronikai rendszerben tárolt adatok, stb.) törli vagy megsemmisíti. Az adatok visszaküldését, törlését vagy megsemmisítését, valamint az adatkezelési célhoz viszonyított szükségszerűtlenség indokát adott eljárásban rögzíteni kell.

VII.3. Helyesbítéshez való jog

Az érintett kérésére az Adatkezelőnek indokolatlan késedelem nélkül helyesbítenie kell a rá vonatkozó pontatlan személyes adatokat. Az adatkezelés céljának figyelembe vételével az érintett kérheti a hiányos személyes adatok kiegészítését is.

VII.4. Korlátozáshoz való jog

Az Adatkezelő az érintett kérésére korlátozza az adatkezelést, az alábbi feltételek valamelyikének teljesülése esetén:

- az érintett vitatja a személyes adatok pontosságát. Ez esetben a korlátozás addig tart, ameddig az Adatkezelő ezt ellenőrizni tudja;
- az adatkezelés jogellenes, az érintett ellenzi az adatok törlését, és törlés helyett az adatok felhasználásának korlátozását kéri;
- az Adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;
- az érintett tiltakozik 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 a fentiek alapján korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az alábbi célokból, illetve jogalapok alapján lehet kezelni:

- az érintett hozzájárulásával,
- jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében,
- az Unió, illetve valamely tagállam fontos közérdekéből.

Az Adatkezelő az adatkezelés korlátozásának feloldása esetén köteles erről azt az érintettet előzetesen tájékoztatni, akinek a kérésére korlátozták az adatkezelést.

VII.5. Tiltakozáshoz való jog

Az érintett a saját helyzetével kapcsolatos okból bármikor tiltakozhat személyes adatainak jogos érdeken alapuló kezelése ellen, ideértve a profilalkotást is. Ebben az esetben a személyes adatok nem kezelhetők tovább, kivéve, ha az Adatkezelő bizonyítja, hogy az adatkezelést olyan az ő oldalán fellépő jogos érdek indokolja, amely elsőbbséget élvez 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 bármikor tiltakozhat a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik.Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatai a továbbiakban e célból nem kezelhetők.

A fentiekben említett tiltakozási jogra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni az érintett figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

Fontos, hogy nem illeti meg az érintettet a tiltakozás joga:

- hozzájáruláson
- szerződés teljesítésén
- jogi kötelezettség teljesítésén
- létfontosságú érdek védelmén

alapuló adatkezelések esetén.

VII.6. Adathordozhatósághoz való jog

Az érintett jogosult arra, hogy

- a rá vonatkozó, általa egy Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy
- ezeket az adatokat az érintett egy másik Adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az Adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha:

- az adatkezelés hozzájáruláson, vagy szerződésen alapul és
- az adatkezelés automatizált módon történik.

- kérje a személyes adatok Adatkezelők közötti közvetlen továbbítását, amennyiben ez technikailag megvalósítható.

VII.7. Automatizált adatkezeléssel hozott döntés alóli mentesülés

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené. Ez tehát az érintettet megillető alanyi jog, nem függ attól, hogy ezt kérelmezi vagy sem.

Kizárólag automatizált adatkezelés tehát akkor alkalmazható, ha

- az érintett és az Adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges;
- az Adatkezelőre vonatkozó uniós vagy tagállami jog lehetővé teszi; vagy
- az érintett kifejezett hozzájárulásán alapul.

Az első és a harmadik esetben az Adatkezelő köteles megfelelő intézkedéseket tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek legalább azt a jogát, hogy

- az Adatkezelő részéről emberi beavatkozást kérjen,
- álláspontját kifejezze, és
- a döntéssel szemben kifogást nyújtson be.

Az alkalmazhatóság fenti eseteiben a döntések nem alapulhatnak a személyes adatoknak a különleges kategóriáin, kivéve a kifejezett hozzájárulást, amennyiben az érintett jogainak és jogos érdekeinek védelme érdekében megfelelő intézkedések megtételére került sor.

Jelenleg nem alkalmaz automatizált döntéshozatallal együttjáró eljárásokat aIntézmény.

VII.8. Jogorvoslathoz való jog

Az érintett jogosult a rá vonatkozó személyes adatok kezelésének megsértése esetén arra, hogy panaszt tegyen a Felügyeleti hatóságnál.

Ezen túlmenően az érintettet megilleti a bírósághoz fordulás joga is az alábbi esetekben:

- a Felügyeleti hatóság rá vonatkozó jogilag kötelező erejű döntésével szemben;
- ha a Felügyeleti hatóság nem foglalkozik a panasszal;

- ha a Felügyeleti hatóság 3 hónapon belül nem tájékoztatja a panaszával kapcsolatos eljárás fejleményeiről vagy annak eredményéről;
- ha megítélése szerint az Adatkezelő vagy az Adatfeldolgozó a GDPR rendelkezéseinek nem megfelelő adatkezelés következtében megsértette a Rendelet szerinti jogait

A jogorvoslat lehetőségéről az érintettet a VI. pontban meghatározott módon kell tájékoztatni.

VII.9. Az Adatkezelő értesítési kötelezettsége

Az Adatkezelőnek minden olyan címzettet tájékoztatni kell az adatok helyesbítéséről, törléséről, korlátozásáról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha lehetetlen vagy aránytalanul nagy erőfeszítést igényel.

Az érintettet is tájékoztatni kell:

- kérelmére a címzettekről
- automatikusan: az érintetti jogok gyakorlása körében benyújtott kérelme nyomán megtett intézkedésekről. Ezekről az intézkedésekről az Adatkezelőnek a kérelem beérkezésétől számított egy hónapon belül kell tájékoztatnia az érintettet, amely határidő szükség esetén – a kérelem összetettségére és a kérelmek számára tekintettel - további két hónappal meghosszabbítható. A határidő meghosszabbításáról a kérelem beérkezésétől számított egy hónapon belül kell tájékoztatni az érintettet a késedelem okainak megjelölésével. Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást is elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri.

Ha az Adatkezelő nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával. Az érintett jogaival kapcsolatos és az adatvédelmi incidensről szóló tájékoztatást és intézkedést díjmentesen kell biztosítani. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, az Adatkezelő, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre, megtagadhatja a kérelem alapján történő intézkedést.

A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása az Adatkezelőt terheli.

VIII. Az új adatkezelések meghatározása

A beépített és alapértelmezett adatvédelem elvének megfelelően biztosítani kell az adatvédelmi tisztviselő számára, hogy a személyes adatok védelmével kapcsolatos összes ügybe megfelelő időben (még az új adatkezelés megkezdése előtt) és módon bekapcsolódhasson. Új adatkezelés megkezdése az adatvédelmi tisztviselő véleményének kikérése nélkül nem kezdhető meg.

Ennek értelmében a tervezett új adatkezelések (ideértve a korábban kezelt adatok új célra történő felhasználásának tervét is) előkészítése során ki kell kérni az adatvédelmi tisztviselő véleményét az adatkezelés körülményeinek meghatározásával és szükség esetén az érdekmérlegelési teszt részére történő egyidejű adatvedelem@mfkh.hu e-mail címre történő megküldésével.

Az adatvédelmi tisztviselő a tervezett új adatkezelést 5 munkanapon belül véleményezi az adatvédelemre vonatkozó jogszabályoknak való megfelelés szempontjából. Ha a véleményezés során kiegészítő információk bekérésére van szükség, az 5 munkanapot azok adatvédelmi tisztviselőhöz való beérkezésétől kell számítani.

IX. Az Adatkezelőre, adatfeldolgozóra vonatkozó szabályok

IX.1. Adatkezelő – Adatfeldolgozó elhatárolása

- Adatkezelő: Heves Vármegyei Markhot Ferenc Oktatókórház és Rendelőintézet
- Adatfeldolgozó: az Adatkezelőtől elkülönült személy
- Az Adatkezelő határozza meg (önállóan vagy másokkal együtt) a személyes adatok kezelésének céljait és eszközeit. Az Adatfeldolgozó ezeket nem határozhatja meg.
- Az Adatkezelő mindig a saját nevében jár el, az Adatfeldolgozó az Adatkezelő nevében jár el.
- Az Adatkezelő a saját döntései szerint jár el, az Adatfeldolgozó az Adatkezelő utasításai szerint jár el (kivéve, ha az adatfeldolgozóra vonatkozó uniós vagy tagállami jog az adatfeldolgozóra is adatkezelést ír elő);
- Az Adatkezelőnek nem kerül feltétlenül birtokába az adat, az Adatfeldolgozónak mindig birtokába kerül az adat.

IX.2. Az Adatkezelő feladatai

Az Adatkezelőnek 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 kell végrehajtania annak biztosítása és bizonyítása céljából (az elszámoltathatóság elvére tekintettel), hogy a személyes adatok kezelése a GDPR rendelkezéseivel összhangban történjen.

Ilyen intézkedések:

- belső adatvédelmi szabályok alkalmazása (amely tágabb kategória, mint belső adatvédelmi szabályzat megalkotása);
- nyilvántartások vezetése;
- hatásvizsgálat elkészítése a valószínűsíthetően magas kockázattal járó új adatkezelések megkezdése előtt;
- alapértelmezett és beépített adatvédelem elvének következetes érvényesítése;
- megfelelő adatvédelmi incidenskezelés;

Ezeket az intézkedéseket a belső szabályzatok rendszeres felülvizsgálata során át kell tekinteni és a szükséges módosításokat el kell végezni, ezáltal biztosítva az intézkedések naprakészségét.

IX.3. Adatfeldolgozó igénybevétele

Ha az Adatkezelő az adatkezeléshez Adatfeldolgozót vesz igénybe, az csak olyan személy, szervezet lehet, aki vagy amely

- megfelelő garanciákat nyújt az adatkezelés GDPR követelményeinek való megfelelése érdekében;
- az érintettek jogainak védelmét biztosító megfelelő technikai és szervezési intézkedések végrehajtására képes, és ezek megvalósítására megfelelő garanciákat is nyújt.

Az Adatfeldolgozó további adatfeldolgozót igénybe vehet, ennek azonban feltétele az Adatkezelő előzetes, írásban tett, eseti vagy általános felhatalmazása. Általános írásbeli felhatalmazás esetén az Adatfeldolgozónak tájékoztatnia kell az Adatkezelőt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva az Adatkezelőnek azt, hogy ezekkel a változtatásokkal szemben kifogást emeljen.

Az Adatfeldolgozó tevékenységéért az Adatkezelő tartozik felelősséggel. A további Adatfeldolgozó tevékenységéért az őt megbízó Adatfeldolgozó teljes felelősséggel tartozik. A további Adatfeldolgozó kötelezettségei ugyanazok, mint az Adatkezelővel szerződött Adatfeldolgozóé.

IX.4. Az adatfeldolgozói szerződés tartalmi elemei

Az Adatfeldolgozó által végzett adatkezelésre irányuló szerződésnek vagy más jogi aktusnak legalább az alábbiakat kell tartalmaznia:

Az adatkezelés

- tárgyát,
- időtartamát,
- jellegét és célját,
- a személyes adatok típusát,
- az érintettek kategóriáit,

- az Adatkezelő valamint az Adatfeldolgozó kötelezettségeit és jogait (konkrét feladatait és felelősségét). E körben szükséges azt is rögzíteni, hogy az Adatfeldolgozó milyen esetekben és részletességgel köteles az Adatkezelőt a tevékenységéről és a feladat állásáról tájékoztatni,
- azt, hogy a személyes adatokat kizárólag az Adatkezelő írásbeli utasításai szerint lehet kezelni, az Adatfeldolgozó ettől semmilyen esetben nem térhet el. Indokolt rögzíteni, hogy az Adatkezelő vélelmezett célszerűtlen, szakszerűtlen utasítása esetén az Adatfeldolgozó köteles erre az Adatkezelő figyelmét felhívni, és azt is, hogy mi az eljárás ilyen esetben (az Adatkezelő kockázatára végrehajtja az utasítást, illetve milyen esetekben tagadhatja meg az utasítás végrehajtását), tovább milyen jogok illetik meg az Adatfeldolgozót, ha az Adatkezelő a figyelemfelhívás ellenére is fenntartja az utasítását (végrehajtás megtagadása, felmondás, elállás).
- a megfelelő adatbiztonság vállalását (érdemes előre tisztázni – és a szerződésben rögzíteni -, hogy az adatbiztonsági intézkedések min alapulnak: saját dokumentált rendelkezéseken, magatartási kódexhez való csatlakozáson vagy tanúsításon). Az adatbiztonság megfelelősségét dokumentálni kell,
- azt, hogy további Adatfeldolgozó igénybevétele csak az Adatkezelő ilyen irányú rendelkezése alapján lehetséges,
- érintetti jogok teljesítéséhez az Adatkezelővel való együttműködés vállalása (indokolt eleve meghatározni, hogy az együttműködés során milyen tájékoztatási kötelezettségeket kell teljesíteni az Adatfeldolgozónak, és milyen konkrét technológiai feladatokat kell végrehajtania),
- Adatbiztonság biztosításában való együttműködés vállalása (indokolt eleve rögzíteni az Adatfeldolgozó által teendő technikai, szervezési intézkedéseket, eljárásokat, határidőket, felelősöket),
- Incidensek kezelésében való együttműködés vállalása (indokolt eleve rögzíteni az Adatfeldolgozó által teendő technikai, szervezési intézkedéseket, eljárásokat, határidőket, felelősöket),
- Adatvédelmi hatásvizsgálatban és előzetes konzultációban való együttműködés vállalása (indokolt eleve rögzíteni az Adatfeldolgozó által teendő technikai, szervezési intézkedéseket, eljárásokat, határidőket, felelősöket),

- Adatok törlésének vagy visszajuttatásának kötelezettsége (célszerű eleve rögzíteni azt, hogy a szerződés megszűnésekor az Adatfeldolgozó miként köteles eleget tenni az adatok visszajuttatási kötelezettségének, illetve a törlés vagy visszajuttatás miként kerüljön dokumentálásra – elszámoltathatóság elve),
- Adatfeldolgozói kötelezettségek igazolásához szükséges információk rendelkezésre bocsátásának vállalása,
- Ellenőrzési jog biztosítása, információk megadása és helyszíni vizsgálatok (indokolt eleve rögzíteni az Adatkezelő - vagy az Adatkezelő által megbízott ellenőr - által végzett auditok, helyszíni vizsgálatok kezdeményezésének, lefolytatásának szabályait),
- Tájékoztatási kötelezettségvállalás, ha az Adatkezelő utasítása adatvédelmi jogot sért
- Az Adatkezelő, illetve az Adatfeldolgozó kapcsolattartóit, elérhetőségeiket

IX.5. Adatfeldolgozói tevékenységadatvédelmi ellenőrzése

Az Adatkezelőnek ellenőrizni kell az alábbiakat az adatfeldolgozást végzőnél:

a) Szerződéskötés előtt
   - o a szabályozottság megfelelőségét (nem csak Adatvédelmi Szabályzat, hanem folyamatszabályozások megfelelősége);
   - o a technikai, szervezési intézkedések, garanciák meglétét, megfelelőségét;
   - o az adatbiztonsági követelmények megfelelőségét;
   - o esetleges tanúsítások meglétét;
   - o az adatvédelmi tudatosságot biztosító protokollok meglétét

b) Szerződés fennállása alatt
   - o távolról történő ellenőrzés (jelentések, nyilatkozatok, kérdőívek formájában);
   - o helyszíni ellenőrzés;
   - o lejáratkor: adattörlés, adatok visszajuttatása (dokumentálás)

c) A már megkötött adatfeldolgozói szerződéseket folyamatosan kell a fenti szempontok szerint felülvizsgálat alá vonni.

IX.6. Adatfeldolgozói nyilvántartás

Amennyiben azIntézmény adatfeldolgozói feladatokat (is) ellát, és mint ilyen Adatfeldolgozónak (is) minősül, az Adatkezelő nevében végzett adatkezelési

tevékenységekről írásban (ideértve az elektronikus formátumot is) nyilvántartást kell vezetnie. A Nyilvántartás vezetéséről a főigazgató gondoskodik.

A nyilvántartást a Felügyeleti hatóság részére – erre irányuló megkeresésre – rendelkezésre kell bocsátani

A nyilvántartásnak a következő információkat kell tartalmaznia:

- az Adatfeldolgozó neve és elérhetősége,
- az Adatfeldolgozó képviselőjének neve és elérhetősége,
- az Adatfeldolgozó adatvédelmi tisztviselőjének neve és elérhetősége,(amennyiben van ilyen)
- az Adatkezelő neve és elérhetősége, akinek a nevében eljár,
- az Adatkezelő képviselőjének neve és elérhetősége,
- azadatvédelmi tisztviselő elérhetőségei,
- ha igénybe vett további Adatfeldolgozót, akkor annak, valamint képviselőjének, és - ha van – adatvédelmi tisztviselőjének neve és elérhetősége,(amennyiben van ilyen)
- az egyes Adatkezelők nevében végzett adatkezelési tevékenységek kategóriái,
- harmadik országba vagy nemzetközi szervezet részére történő továbbítás esetén az ország vagy a nemzetközi szervezet azonosító adatai, és a továbbítás garanciáinak leírása,
- a technikai és szervezési intézkedések általános leírása.

X. Adattovábbítás harmadik országba vagy nemzetközi szervezetek részére

AzIntézmény részéről személyes adatok harmadik országba vagy nemzetközi szervezetek részére történő továbbításra (akár Adatkezelői, akár adatfeldolgozó minőségben jár el), csak a IX.1-IX.4. pontban meghatározott esetekben kerülhet sor. Az adattovábbításról az Adatkezelőnek/Adatfeldolgozónak Adattovábbítási Nyilvántartást kell vezetnie. A Nyilvántartást azIntézményfőigazgatója által kijelölt személy vezeti.

X.1. Megfelelőségi határozat alapján

Személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására alapértelmezetten akkor kerülhet sor, ha a Bizottság határozatban megállapította, 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. Az ilyen adattovábbításhoz nem szükséges külön engedély.

A Bizottság az olyan harmadik országok, harmadik országon belüli területek és meghatározott ágazatok, valamint nemzetközi szervezetek jegyzékét, amelyek esetében úgy ítélte meg, hogy biztosítják, vagy többé nem biztosítják a megfelelő védelmi szintet az Európai Unió Hivatalos Lapjában és annak honlapján teszi közzé.

X.2. Megfelelő garanciák alapján

Megfelelőségi határozat hiányában az Adatkezelő vagy az Adatfeldolgozó csak abban az esetben továbbíthat személyes adatokat harmadik országba vagy nemzetközi szervezet részére, ha az Adatkezelő vagy az Adatfeldolgozó megfelelő garanciákat nyújtott, és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek rendelkezésre állnak. A Felügyeleti hatóság külön engedélye nélkül ilyen garanciák lehetnek különösen:

- a Bizottság által - a Bizottság munkáját segítő vizsgálóbizottság eljárásával összhangban - elfogadott általános adatvédelmi kikötések;
- a felügyeleti hatóság által elfogadott és a Bizottság által jóváhagyott általános adatvédelmi kikötések;
- a GDPR 40. cikke szerinti, jóváhagyott magatartási kódex a harmadik országbeli Adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető

kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő garanciákat, ideértve az érintettek jogait illetően is;

- a GDPR 42. cikke szerinti, jóváhagyott tanúsítási mechanizmus a harmadik országbeli Adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő garanciákat, ideértve az érintettek jogait illetően is;
- a felügyeleti hatóság engedélyével az Adatkezelő vagy Adatfeldolgozó és a harmadik országbeli vagy a nemzetközi szervezeten belüli Adatkezelő, adatfeldolgozó vagy a személyes adatok címzettje között létrejött szerződéses rendelkezések.

X.3. Megfelelőségi határozat és megfelelő garanciák hiányában (egyedi esetekre vonatkozó eltérések)

A IX.1. pont szerinti megfelelőségi határozat és a IX.2. pont szerinti megfelelő garanciák hiányában személyes adatok harmadik ország vagy nemzetközi szervezet részére történő továbbítására csak az alábbi feltételek legalább egyikének teljesülése esetén kerülhet sor:

- az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról;
- az adattovábbítás az érintett és az Adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges;
- az adattovábbítás az Adatkezelő és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;
- az adattovábbítás fontos közérdekből szükséges;
- az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;
- az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására;
- a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja, és amely vagy

általában a nyilvánosság, vagy az ezzel kapcsolatos jogos érdekét igazoló bármely személy számára betekintés céljából hozzáférhető.

X.4. Eljárás egyéb esetben

Ha az adattovábbítás nem alapulhat

- a X.1. pont szerinti megfelelőségi határozaton és
- a X.2. pont szerinti megfelelő garanciákon sem, valamint
- a X.3. pontban említett egyedi esetekre vonatkozó eltérések egyike sem alkalmazandó,

akkor a harmadik országok és nemzetközi szervezetek részére történő adattovábbítás csak abban az esetben történhet, ha

- az adattovábbítás nem ismétlődő,
- korlátozott számú érintettre vonatkozik,
- az Adatkezelő olyan kényszerítő erejű jogos érdekében szükséges, amely érdekhez képest nem élveznek elsőbbséget az érintett érdekei, jogai és szabadságai,
- az Adatkezelő az adattovábbítás minden körülményét megvizsgálta, és
- e vizsgálat alapján megfelelő garanciákat nyújtott a személyes adatok védelme tekintetében.

Az Adatkezelőnek ebben az esetben tájékoztatnia kell a felügyeleti hatóságot az adattovábbításról. Az Adatkezelőnek – VI.2 és VI.3. pontban említett információk nyújtásán kívül az érintettet is tájékoztatnia kell az adattovábbításról, valamint az Adatkezelő kényszerítő erejű jogos érdekéről.

XI. Adatbiztonság

XI.1. Az adatkezelés biztonsága

Az Adatkezelőnek megfelelő technikai és szervezési intézkedésekkel a kockázat mértékének megfelelő szintű adatbiztonságot kell garantálnia. Az adatbiztonság megfelelő szintjét az alábbi körülmények figyelembevételével kell meghatározni:

- a tudomány és technológia állása;
- a megvalósítás költségei;
- az adatkezelés jellege, hatóköre, körülményei és céljai;
- a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatok.

A biztonság megfelelő szintjének meghatározásához az alábbi kockázatokat kell értékelni különösen: a kezelt személyes adatok

- véletlen vagy jogellenes megsemmisítéséből,
- elvesztéséből;
- megváltoztatásából;
- jogosulatlan nyilvánosságra hozatalából vagy
- az azokhoz való jogosulatlan hozzáférésből

eredő kockázatokat.

Ezen kockázatok minimalizálása érdekében az Adatkezelőnek az alábbi technikai és szervezési intézkedéseket kell tennie:

- a személyes adatok álnevesítése és titkosítása;
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének, integritásának, rendelkezésre állásának és ellenálló képességének biztosítása;
- fizikai vagy műszaki incidens esetén az arra való képesség biztosítása, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- a kockázatokhoz igazított elvárt adatbiztonsági szint meghatározása;
- kockázatok folyamatos értékelése, elemzése;

- a biztonsági intézkedések hatékonyságának rendszeres tesztelése, visszamérése, erre eljárás kidolgozása;
- adatbiztonsági intézkedések nyilvántartása;
- megfelelő adatbiztonság igazolása (magatartási kódex, tanúsítás útján is megtehető)
- beépített és alapértelmezett adatvédelme biztosítása;
- védelmet biztosító és a megfelelőséget igazoló intézkedések megtétele (megfelelő adatvédelmi szabályok kialakítása)

XI.2. Adatvédelmi incidens

Adatvédelmi incidensnek minősül a GDPR szerint a biztonság olyan sérülése, amely a kezelt személyes adatok

- véletlen vagy jogellenes megsemmisítését;
- véletlen vagy jogellenes elvesztését;
- véletlen vagy jogellenes megváltoztatását;
- jogosulatlan közlését;
- az azokhoz való jogosulatlan hozzáférést eredményezi.

Adatvédelmi incidens észlelése esetén az a munkatárs, aki az incidenst észleli, haladéktalanul köteles azt azIntézményfőigazgatója és az adatvédelmi tisztviselő részére jelenteni az adatvedelem@mfkh.hu e-mail címen.

Az adatvédelmi tisztviselő a hozzá beérkezett információk alapján az adatvédelmi incidenst megvizsgálja, és a döntést hoz főigazgató részére javaslatot tesz, amely szerint:

a) az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, ezért nem kell bejelenteni a Felügyeleti hatóságnak; vagy

b) az adatvédelmi incidens valószínűsíthetően olyan fokú kockázattal jár, amely alapján az incidenst be kell jelenteni a Felügyeleti hatóságnak.

c) Az adatvédelmi incidens valószínűsíthetően olyan magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, amely a Felügyeleti hatóságnak történő bejelentés mellett – igényli az érintettek késedelem nélküli tájékoztatását is.

Bejelentésre irányuló főigazgatói döntés esetén a bejelentést indokolatlan késedelem nélkül, de legkésőbb a tudomásra jutástól számított 72 órán belül kell megtenni. A

„tudomásra jutás” megállapításához egy „ésszerű fokú bizonyosság” szükségeltetik: meg kell tudni állapítani, hogy a bekövetkezett incidens valószínűsíthetően jelent-e veszélyt, kockázatot a személyes adatokra nézve. Ennek megfelelően az ennek megállapításához szükséges rövid idejű kivizsgálás időtartama nem számít bele a 72 órába!!

A tudomásszerzés több forrásból történhet, pl.

- magától az érintettől
- esetleg a médiából
- az Adatkezelő saját maga is rájöhet (pl. logelemzés)
- Adatfeldolgozó igénybevétele esetén magától az Adatfeldolgozótól. Az Adatfeldolgozónak indokolatlan késedelem nélkül kell bejelentést tenni az Adatkezelő felé. Ennek tényét, az eljárás menetét az adatkezelési szerződésben rögzíteni kell.

A bejelentésnek az alábbiakat kell tartalmaznia:

- ismertetni kell az adatvédelmi incidens jellegét;
- az érintettek kategóriáit és hozzávetőleges számát;
- az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket;
- a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit.

Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

Részinformációk is közölhetők, amennyiben a 72 órás határidőn belül nem áll minden információ rendelkezésre, de ez nem mentesít a későbbi információ-szolgáltatási kötelezettség alól, amelyet az információk beszerzését követően szintén haladéktalanul kell teljesíteni.

Az érintettek késedelem nélküli tájékoztatásának módjáról is a hatósági bejelentés kérdésében döntésre jogosult Intézményfőigazgatója határoz az adatvédelmi tisztviselő javaslatának figyelembevételével.

Az Adatkezelőnek az adatvédelmi incidensekről nyilvántartást kell vezetnie.

A bejelentés, illetve a nyilvántartás céljából jelentett adatok valóságáért, helyességéért és hiánytalanságáért az adatszolgáltatást teljesítő munkatárs tartozik felelősséggel.

XII. Adatvédelmi hatásvizsgálat

XII.1. Adatvédelmi hatásvizsgálat

Az Adatkezelőnek az adatkezelést megelőzően adatvédelmi hatásvizsgálatot kell végeznie arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik, 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.

Főszabály szerint adatkezelési műveletenként kell elvégezni, de egymáshoz hasonló típusú adatkezelési műveletek - amelyek egymáshoz hasonló magas kockázatokat jelentenek) -, egyetlen hatásvizsgálat keretei között is értékelhetők. Hasonló típusú az adatkezelési művelet, ha:

- ugyanazon célból,
- ugyanazon típusú adatkezelés történik,
- hasonló technológia mellett.

Ha az Adatkezelő adatfeldolgozót is igénybe vesz, akkor a hatásvizsgálatot együtt kell elvégezni.

Az adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

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

AzEurópai Adatvédelmi Testület (jogelődje: 29. cikk szerinti Munkacsoport WP 29.) kilenc mérlegelendő szempontot határoz meg annak eldöntéséhez, hogy mely esetekben kell kötelezően elvégezni a hatásvizsgálatot:

- Értékelés vagy pontozás, ideértve a profilalkotást is, amikor az adatkezelés célja, hogy az érintettek személyes jellemzőinek szisztematikus értékelése alapján megfelelő döntést lehessen hozni.

- Joghatással vagy más hasonló jelentős hatással járó automatikus döntéshozatal, amikor az adatkezelés pl. egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti;
- Módszeres megfigyelés, amikor az érintettek megfigyelése, nyomon követése vagy ellenőrzése céljából történik az adatkezelés;
- Személyes adatok különleges kategóriáinak kezelése;
- Nagy számban kezelt adatok: a GDPR nem határozza meg, hogy mi értendő nagy szám alatt, de azEurópai Adatvédelmi Testület is csak általános szempontokat ad (Pl. az érintettek száma konkrét számadatként vagy a lakosság számának arányában; a kezelt adatok mennyisége, vagy adatfajták köre; az adatkezelési tevékenység időtartama vagy állandó jellege, földrajzi kitettsége). Ezek alapján ez valamennyi körülmény figyelembe vételével történő egyéni mérlegelés kérdése;
- Különböző célokból, illetve eltérő Adatkezelők által kezelt adatok, adatkészletek egymásnak való megfeleltetése, összevonása;
- Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok kezelése (pl. gyermekek, munkavállalók, lakosság különleges védelmet igénylő, kiszolgáltatott helyzetben lévő rétegei – pl. fogyatékos személyek -; minden olyan eset, amikor az Adatkezelő és az érintett között egyenlőtlen kapcsolat van);
- Új technológiai vagy szervezési megoldások használata: mindazon esetek, amikor a technológia elismert állásának megfelelő új technológia alkalmazására kerül sor;
- Mindazok az esetek, amikor az adatkezelés önmagában véve megakadályozza, hogy az érintettek a jogaikat gyakorolják, szolgáltatásokat vegyenek igénybe, vagy szerződésből eredő igényeiket érvényesítsék
- Bizonyos esetekben már egy vagy két szempontnak megfelelő adatkezelés esetében is szükség lehet hatásvizsgálatra. Minél több szempontban felel meg az adatkezelés, annál nagyobb a valószínűsége annak, hogy magas kockázattal jár az érintettek jogaira és szabadságaira nézve.

Az olyan adatkezelési műveletek típusainak a jegyzékét - amelyekre vonatkozóan adatvédelmi hatásvizsgálatot kell végezni - a Felügyeleti hatóság állítja össze és hozza nyilvánosságra. A felügyeleti hatóság összeállíthatja és nyilvánosságra hozhatja az olyan adatkezelési műveletek típusainak a jegyzékét is, amelyekre vonatkozóan nem kell

adatvédelmi hatásvizsgálatot végezni. Az adatvédelmi hatásvizsgálatot a NAIH iránymutatásai alapján a következő esetekben kötelező elvégezni:

- Ha egy természetes személy biometrikus adatainak kezelése módszeres megfigyelésre irányul.
- Ha kiszolgáltatott helyzetben lévő érintettekkel – különös tekintettel a gyermekekre, munkavállalókra, idős, mentális betegségben szenvedőkre – kapcsolatos biometrikus adat kezelése történik.
- Ha az adatkezelés egy természetes személy genetikai adatainak egyéb különleges adatokhoz vagy fokozottan személyes jellegű adatokhoz történő hozzákapcsolásával jár.
- Ha egy természetes személy genetikai adatai kezelésének célja a természetes személy értékelése vagy pontozása.
- Pontozás. Az adatkezelés célja, hogy az érintett bizonyos tulajdonságait felmérje, és annak eredménye kihatással van az érintett részére nyújtott, illetve nyújtandó szolgáltatás létrejöttére vagy minőségére.
- Hitelképesség értékelése. Az adatkezelés célja, hogy az érintett hitelképességét felmérje a személyes adatok nagy számú, illetve módszeres értékelése útján.
- Fizetőképesség értékelése. Az adatkezelés célja, hogy az érintett fizetőképességét felmérje a személyes adatok nagy számú, illetve módszeres értékelése útján.
- Harmadik személytől gyűjtött adatok további felhasználása. Az adatkezelés célja, hogy a harmadik személytől begyűjtött személyes adatokat felhasználják az érintettre vonatkozó szolgáltatás visszautasítására vagy megszüntetésére vonatkozó döntés meghozatalánál.
- Diákok, hallgatók személyes adatainak értékelésre való felhasználása. Az adatkezelés célja a diákok, hallgatók felkészültségének, teljesítményének, alkalmasságának, illetve mentális állapotának rögzítése, valamint vizsgálata és az adatkezelés nem jogszabályon alapul, függetlenül attól, hogy az oktatás alap-, közép- vagy felsőfokú.
- Profilozás. Az adatkezelés célja személyes adatok nagy számú, illetve módszeres értékelése révén végzett profilozás, különösen ha az az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körére, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők alapján történik.

- Csalás elleni fellépés. Az adatkezelés célja hitelreferencia-, pénzmosás és a terrorizmus finanszírozása elleni vagy csalásellenes adatbázis felhasználása ügyfelek szűrésére.
- Okosmérők. Az adatkezelés célja közműszolgáltatók által telepített „okosmérők" alkalmazása (fogyasztási szokások nyomon követése).
- Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal. Az adatkezelés célja a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések meghozatala, amely adatkezelés adott esetben egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti.
- Módszeres megfigyelés. Érintettek nagyszámú és módszeres megfigyelése jellemzően közterületeken vagy nyilvános helyeken történő kamerarendszerek, drónok felhasználásával, illetve bármely más új technológia használatával (Wi-Fi tracking, Bluetooth tracking, testkamera).
- Helymeghatározási adatok kezelése, ha az módszeres megfigyelésre vagy profilalkotásra utal.
- Munkavállaló munkájának megfigyelése. Munkavállalók munkájának megfigyelése. Az adatkezelés célja a munkavállaló munkájának megfigyelése során a munkavállaló személyes adatainak nagy számú és módszeres feldolgozása, illetve értékelése. Például GPS megfigyelő autóban történő elhelyezése, kamerás megfigyelés lopás vagy csalás elleni fellépés céljából.
- Különleges adatok nagy számban való kezelése. A GDPR (91) preambulumbekezdése alapján a személyes adatok kezelése nem tekinthető nagymértékűnek, ha az adatkezelés egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adataira vonatkozik.
- Nagyszámú személyes adatok kezelése bűnüldözési célból
- Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos, nagy számban kezelt adatok eredeti céltól eltérő kezelése: pl. gyermekek, idősek, mentális betegségben szenvedők esetében.
- Gyermekek személyes adatainak kezelése profilozás, automatikus döntéshozatal, vagy marketing céljából, vagy közvetlenül részükre kínált, információs társadalommal összefüggő szolgáltatások ajánlása vonatkozásában.

- Új technológiai megoldások használata az adatkezelés során. Ideértve az érzékelővel ellátott eszközök által előállított adatok interneten vagy más csatornán keresztül történő nagyszámú kezelése (pl.: okos televízió, okos háztartási eszközök, okos játékok stb.), és amelyek adatokat szolgáltatnak a természetes személy fizetőképességére, egészségére, személyes érdeklődési körére, megbízhatóságára vagy viselkedésére, tartózkodási helyére és amelyek alapján profilalkotás történik.
- Egészségügyi adatokra vonatkozó adatkezelések. Nagy számban kezelt adatok tekintetében a kórházak, egészségügyi ellátó intézmények, magán-egészségügyi szolgáltatók vagy nagyszámú páciensi körrel rendelkező természetgyógyászok által kezelt különleges adatok vonatkozásában. Ideértve a nagyobb sportlétesítmények, edzőtermek által a tagoktól felvett egészségügyi adatok kezelése.
- Amikor több adatkezelő egy egész ágazat által közösen használt alkalmazást, rendszert, eszközt, illetve platformot tervez létrehozni, amelyben különleges adatokat is kezelnek.
- Az adatkezelés célja a különböző forrásokból származó adatok összevonása, egymással való megfeleltetése vagy összehasonlítása.

A hatásvizsgálatnak legalább az alábbiakra kell kiterjednie:

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

Az adatvédelmi hatásvizsgálat akkor van összhangban a GDPR rendelkezéseivel, ha

- módszeres leírás készült az adatfeldolgozásról;
- értékelésre került a szükségesség és az arányosság;

- az érintett jogait és szabadságait érintő kockázatok felmérésre kerültek, és ezen kockázatok orvoslására intézkedési terv született;
- az érdekeltek bevonásra kerültek

Az elfogadható adatvédelmi hatásvizsgálat szempontjaira és módszertanára nézve azEurópai Adatvédelmi Testület WP248 számú Iránymutatása az irányadó.

Az Adatkezelőnek adott esetben – a kereskedelmi érdekek vagy a közérdek védelmének vagy az adatkezelési műveletek biztonságának sérelme nélkül – ki kell kérni az érintettek vagy képviselőik véleményét a tervezett adatkezelésről.

Folyamatban lévő adatkezelések esetén, ha az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges adatkezelés jogalapját uniós vagy az Adatkezelőre alkalmazandó tagállami jog írja elő, és e jog a szóban forgó konkrét adatkezelési műveletet vagy műveleteket is szabályozza, valamint e jogalap elfogadása során egy általános hatásvizsgálat részeként már végeztek adatvédelmi hatásvizsgálatot, akkor a hatásvizsgálatot nem kell ismételten elvégezni, kivéve, ha a tagállamok az adatkezelési tevékenységet megelőzően ilyen hatásvizsgálat elvégzését szükségesnek tartják.

Az Adatkezelőnek szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést kell lefolytatnia annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

XII.2. Előzetes konzultáció a Felügyeleti hatósággal

Ha a hatásvizsgálat azt állapítja meg, hogy az adatkezelés az Adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az Adatkezelő köteles konzultálni a Felügyeleti hatósággal.

Ha a Felügyeleti hatóság véleménye szerint a tervezett adatkezelés megsértené a GDPR előírásait – így különösen, ha az Adatkezelő a kockázatot nem elégséges módon azonosította vagy csökkentette –, a Felügyeleti hatóság az Adatkezelőnek és adott esetben az adatfeldolgozónak legkésőbb a konzultáció iránti megkeresés kézhezvételétől számított nyolc héten belül

- írásban tanácsot ad, továbbá
- gyakorolhatja a GDPR 58. cikkében említett hatásköreit.

Ez a határidő – a tervezett adatkezelés összetettségétől függően – hat héttel meghosszabbítható. A Felügyeleti hatóság a megkeresés kézhezvételétől számított egy hónapon belül tájékoztatja az Adatkezelőt vagy adott esetben az adatfeldolgozót a meghosszabbításról és a késedelem okairól. Az említett időtartamok felfüggeszthetők arra az időtartamra, amíg a Felügyeleti hatóság nem jut hozzá azokhoz az információkhoz, amelyeket adott esetben a konzultáció céljából kért.

Az Adatkezelő a Felügyeleti hatósággal folytatott konzultáció során a Felügyeleti hatóságot tájékoztatja:

- az adatkezelésben részt vevő Adatkezelő, közös adatkezelők és Adatfeldolgozók feladatköreiről;
- a tervezett adatkezelés céljairól és módjairól;
- az érintetteknek a GDPR értelmében fennálló jogainak és szabadságainak védelmében hozott intézkedésekről és garanciákról;
- azadatvédelmi tisztviselő elérhetőségeiről; (amennyiben van ilyen)
- a lefolytatott adatvédelmi hatásvizsgálatról;
- a felügyeleti hatóság által kért minden egyéb információról.

XIII. Az adatvédelem szervezete

XIII.1. AzIntézmény jogai és kötelezettségei, felelőssége azIntézményt érintő adatvédelemben

AzIntézmény köteles az Adatvédelmi Szabályzat rendelkezéseit betartani. AzIntézményfőigazgatója az adatvédelmi tisztviselő bevonásávalellátja az adatvédelmi tárgyú jogszabályokból és a jelen Szabályzatból eredő, adatvédelmi feladatokat.

XIII.2. AzIntézményfőigazgatója

AzIntézményfőigazgatójaaz alábbi feladatok ellátásáról gondoskodik:

- gondoskodik az adatvédelmi tevékenység irányításában és ellátásában résztvevő szervezeti egységek kijelöléséről, feladataik, az adatvédelmi tárgyú ügyekkel kapcsolatos döntési jogkörök meghatározásáról, az egyes adatkezelési döntési szintek kialakításáról;
- kijelöli és megbízza az adatvédelmi tisztviselőt (DPO), akit a Felügyeleti Hatóság nyilvántartásában regisztrál;
- kijelöli és megbízza a belső adatvédelmi felelőst (BAF);
- kijelöli a szervezeti egység szintű adatvédelmi felelősöket (AF);
- munkajogi értelemben vett közvetlen felettese az adatvédelmi tisztviselőnek (DPO) és a belső adatvédelmi felelősnek(BAF);
- ellenőrzi az adatvédelmi tisztviselő (DPO) és a belső adatvédelmi felelős (BAF) tevékenységét;
- felelős az Adatvédelmi Szabályzat kiadásáért és betartatásáért;
- biztosítja az adatvédelmi tevékenység irányításához és ellátásához, valamint az érintett jogai gyakorlásához szükséges személyi és tárgyi feltételeket;
- gondoskodik az adatkezelés során esetleg előforduló, feltárt hiányosságok megszűntetéséről, szükség szerint a felelősségre vonásról;
- az Országos Kórházi Főigazgatóság számára adatszolgáltatást teljesít;

XIII.3. Az Adatvédelmi tisztviselő (DPO) jogállása, felelőssége, elhelyezkedése a szervezetben

AzIntézmény az adatvédelmi tevékenységének magas szintű szakmai támogatása érdekében, valamint a GDPR 37. cikk (1) bekezdésében meghatározott kötelezettségteljesítése céljából DPO-t alkalmaz. A DPO alkalmazása kapcsán nincs előírás a végzettség kapcsán, így ennek meghatározása minden szervezet saját döntése. A GDPR alapján a DPO-t a szakmai rátermettség, az adatvédelmi jog és gyakorlat szakértői szintű ismerete, és a feladatai ellátására való alkalmasság alapján kell kijelölni, így a kiválasztási szempontoknál javasolt az elsődleges hangsúlyt a szakmai tapasztalatra és szakértelemre helyezni.

Releváns készségnek és szakértelemnek minősül pl.:

- szakértelem a nemzeti és európai adatvédelmi jogszabályok és gyakorlatok terén, ideértve a GDPR-t és az Európai Adatvédelmi Testület ajánlásait, iránymutatásait is;
- az elvégzett adatkezelési műveletek ismerete;
- az információs technológiák és adatbiztonság ismerete;
- az üzletág és a szervezet felépítésének és folyamatainak ismerete;
- a szervezeten belül az adatvédelmi kultúra előmozdításának képessége

A DPO-t az Intézmény főigazgatója nevezi ki, és közvetlen irányítása alatt áll.

Adatvédelmi tisztviselő jogállása, felelősége:

- Az adatvédelmi tisztviselő a megbízatása során szorosan együttműködik az Intézmény belső adatvédelmi felelősével és az egység szintű adatvédelmi felelősökkel.
- Az adatvédelmi tisztviselő független, függetlensége biztosítása érdekében szakmai feladatai ellátása során utasítást nem fogadhat el, szakmai feladatai ellátásával összefüggésben nem bocsátható el. Jelen Szabályzatban foglalt tevékenysége ellátása során autonóm, szakmai ügyekben kizárólag a főigazgatónak tartozik felelősséggel.
- Az Intézmény elősegíti az adatvédelmi tisztviselő megfelelő szakmai feladatellátását, ennek érdekében az Intézmény biztosítja különösen az adatvédelmi tisztviselő feladatai végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáférést.

- Az Intézmény kiemelt figyelmet fordít a megfelelő technikai-, eljárási intézkedésekhez szükséges források meghatározása (költségvetési tervezés) során arra vonatkozóan, hogy teljesüljenek az adatvédelem alapelvei a technikai vívmányok alkalmazása (beépített adatvédelem) és az adatvédelmet szolgáló megoldások (alapértelmezett adatvédelem) révén.
- A felügyeleti hatósággal történő együttműködés során az adatvédelmi tisztviselő – igény szerint a Jogi Iroda és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – tartja a kapcsolatot.
- Az adatvédelmi tisztviselő véleményét– a jelen szabályzat rendelkezései szerint – ki kell kérni a személyes adatok kezelést érintő döntések, szerződések és belső szabályzatok előkészítése, módosítása esetén.
- Az adatvédelmi tisztviselőt tisztsége fennállása alatt és annak megszűnését követően titoktartási kötelezettség terheli a tevékenysége során tudomására jutott minden olyan információ tekintetében, amely nem minősül közérdekű vagy közérdekből nyilvános adatnak.
- Az adatvédelmi tisztviselő nevét és elérhetőségeit az Intézmény honlapján, székhelyén, telephelyén a nyilvánosság részére mindenkor elérhetővé kell tenni. Az Intézmény továbbá az adatvédelmi tisztviselő adatainak felvételét kéri a Felügyeleti Hatóság által vezetett Adatvédelmi Tisztviselők Nyilvántartásába.

Az adatvédelmi tisztviselő feladatai:

- ellenőrzi a GDPR, az Infotv., az egészségügyi ágazati jogszabályok és a jelen Szabályzat, illetve az Intézmény egyéb adatvédelmi tárgyú belső szabályzatainak alkalmazását és végrehajtását,
- szakmailag támogatja és ellenőrzi a szervezeti egység szintű adatvédelmi rendszer felépítését, működését,
- tájékoztat, szakmai tanácsot ad és ellenőrzi az adatvédelemmel kapcsolatos jogszabálynak való megfelelést, különös tekintettel az egészségügyi adatok kezelésére vonatkozó szabályokra,
- közreműködik az Adatvédelmi Szabályzat elkészítésében,
- az adatvédelmi felelősök (AF) szakmai felügyelete és oktatása, oktatási anyagok és tematika biztosítása
- kivizsgálja –igény esetén a Jogi Iroda és az érintett szakterületek bevonásával – a neki címzett panaszokat, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót,

- tanácsot ad az adatvédelmi hatásvizsgálatra és az érdekmérlegelési tesztekre vonatkozóan, valamint aktívan közreműködik ezek elvégzése során,
- kapcsolattartó pontként működik azon érintettek számára, akik személyes adataik kezelésével és jogaik gyakorlásával kapcsolatban keresik meg,
- együttműködik és kapcsolattartó pontként működik a Felügyeleti Hatóság felé az adatkezeléssel kapcsolatos ügyekben,
- adatvédelmi incidens esetén - amennyiben ez indokolt -, a tudomására jutástól számítva haladéktalanul, maximum 72 órán belül a főigazgató jóváhagyását követően bejelentést tesz a Felügyeleti Hatóság (NAIH) felé,
- javaslatot tesz az adatvédelem területén a kifejlesztett új technológiák és eszközök alkalmazása előtt,
- az adatvédelmi tevékenységgel kapcsolatos oktatásokat megszervezi és az oktatási anyagot évente legalább egy alkalommal minden szervezeti egységben frissíti az adatvédelmi felelősök (AF) számára,
- az Intézmény adatvédelmi helyzetéről éves összefoglaló jelentést készít a főigazgatónak,
- a DATINF rendszerben nyomon követi az Országos Kórházi Főigazgatóság által kiadott állásfoglalásokat, iránymutatásokat és más mintadokumentumokat,
- kapcsolatot tart, illetve konzultációt kezdeményez a személyes adatok védelmét érintő ügyekben az Országos Kórházi Főigazgatóság Adatvédelmi Tudásközpont munkatársaival a DATINF rendszeren keresztül (szükség esetén megoldási javaslat, elemzés stb.).

XIII.4. Belső adatvédelmi felelős (BAF)

Segíti az adatvédelmi tisztviselő munkáját, kapcsolatot tart az osztályos adatvédelmi felelősökkel, végrehajtja az adatvédelmi szabályzatban foglalt feladatokat.

A belső adatvédelmi felelőst a főigazgató nevezi ki az Intézmény felsővezetői közül. Az Intézményben azáltalános főigazgató-helyettes látja el a belső adatvédelmi felelős (BAF)feladatait, az alábbiak szerint.

A belső adatvédelmi felelős feladatai:

- hatályos jogszabályok, szakmai anyagok ismerete, folyamatos követése, szakmai önképzés, a megszerzett információk alapján döntés előkészítés segítése,
- az adatvédelmi tisztviselő munkájának támogatása,
- a szervezeti egység szintű adatvédelmi felelősök munkájának támogatása és felügyelete,
- aktív részvétel adatvédelmi incidensek azonosításában és kezelésében,
- felméri az adatkezeléssel kapcsolatos igényeket, és előkészíti azokat az adatvédelmi tisztviselő számára,
- megszervezi és felügyeli az adatvédelmi felelősök tevékenységét, oktatását,

- az adatvédelmi felelősökkel együtt elvégzi az előzetes adatvédelmi hatásvizsgálatokat az adatvédelmi tisztviselő szakmai irányítása mellett,
- az adatvédelmi felelősökkel együtt elkészíti az adatkezelésekhez esetlegesen szükséges érdekmérlegelési teszteket az adatvédelmi tisztviselő szakmai irányítása mellett,
- rendszeres időközönként, de legalább évente áttekinti az adatvédelmi hatásvizsgálatban azonosított kockázatok alakulását, szükség esetén dokumentálja, illetve jelzi az adatvédelmi tisztviselőnek az adatkezeléssel járó kockázatok változását és az azok csökkentését célzó intézkedéseket, elvégzi, illetve közreműködik az adatvédelmi hatásvizsgálatok utóellenőrzésében és annak dokumentálásában,
- adatvédelmi nyilvántartások felügyelete a DATINF rendszerben.

XIII.5. Szervezeti egység szintű adatvédelmi felelős (AF)

A főigazgató minden szervezeti egységében adatvédelmi felelőst jelöl ki. Adatvédelmi felelősnek olyan személyt kell kijelölni, aki az adott szakterületet, üzleti/adminisztratív folyamato(ka)t, illetve – az informatikai szakterületen – a szakterületek tevékenységét támogató informatikai rendszereket illetően kellő ismeretekkel bír, a feladatai közé az alábbiak tartoznak.

Adatvédelmi felelős feladatai:

- figyelemmel kíséri a jogszerű adatkezelés feltételeinek folyamatos fennállását (beleértve az adatkezelési tájékoztatások megadását, nyilatkozatok beszerzését stb.) és szükség esetén egyeztet az adatvédelmi tisztviselővel és a belső adatvédelmi felelőssel,
- amennyiben az adatkezelés hozzájáruláson alapul, ellenőrzi, hogy az érintett a hozzájárulását szabályosan szerezték-e be,
- gondoskodik arról, hogy legalább az érintettel való első kapcsolatfelvételkor felhívják a figyelmét az adatkezelő vagy harmadik személy jogos érdeke, illetve közérdekű feladat vagy közfeladat ellátása jogalapon (ideértve az említett jogalapokon alapuló profilalkotást is) történő adatkezeléssel szembeni tiltakozási jogra, és hogy az erről szóló tájékoztatást egyértelműen és más információtól elkülönítve jelenítsék meg,
- az új dolgozók adatkezelési tájékoztatása,
- adatvédelmi incidens gyanújának rögzítése és haladéktalan továbbítása az adatvédelmi tisztviselő (DPO) és a belső adatvédelmi felelős (BAF) számára,
- az érintettek megkereséseinek rögzítése és haladéktalan továbbítása az adatvédelmi tisztviselő (DPO) és a belső adatvédelmi felelős (BAF) számára,

- a partnerek megkereséseinek rögzítése és haladéktalan továbbítása az adatvédelmi tisztviselő (DPO) és a belső adatvédelmi felelős (BAF) számára,
- a közérdekű adatok megismerése iránti igények rögzítése és haladéktalan továbbítása az adatvédelmi tisztviselő (DPO) és a belső adatvédelmi felelős (BAF) számára,
- a tudományos, történeti kutatások, statisztikai és edukációs adatok kezelésével kapcsolatos igények rögzítése és haladéktalan továbbítása az adatvédelmi tisztviselő (DPO) és a belső adatvédelmi felelős (BAF) számára,
- a belső szabályozókban előírtaknak történő megfelelés ellenőrzése a napi munkavégzés során,
- az Intézmény dolgozóinak rendszeres, a belépő dolgozók kötelező adatvédelmi oktatását a szervezeti egység szintjén,
- rendszeres időközönként, de legalább évente áttekinti az adatvédelmi hatásvizsgálatban azonosított kockázatok alakulását, szükség esetén dokumentálja, illetve jelzi az adatvédelmi tisztviselőnek az adatkezeléssel járó kockázatok változását és az azok csökkentését célzó intézkedéseket, elvégzi, illetve közreműködik az adatvédelmi hatásvizsgálatok utóellenőrzésében és annak dokumentálásában,
- előkészíti az adatkezeléssel kapcsolatos döntéseket,
- gondoskodik az adatkezeléshez kapcsolódó adminisztratív teendők ellátásáról,
- együttműködik az ugyanazon adatkezelésben érintett más adatvédelmi felelősökkel,
- közreműködik az érintettek jogai gyakorlásának biztosításában,
- közreműködik az adatvédelmi incidensek észlelésében és a következményeinek elhárításában,
- közreműködik az adatvédelmi tisztviselő (DPO) és a belső adatvédelmi felelős (BAF) vizsgálataiban,
- közreműködik az adatvagyon-felmérés elkészítésében.

XIII.6. AzIntézménydolgozói

AzIntézménydolgozói a mindennapi munkájuk során az adatvédelemmel kapcsolatosan kötelesek:

- a tudomására jutott személyes adatok védelmét biztosítani,
- szabályokat megismerni és betartani,
- a vonatkozó oktatási anyagokat megismerni,
- tájékoztatást nyújtani az érintettek számára,
- a hozzájuk érkezőérintetti megkereséseket, jogérvényesítési igényekethaladéktalanul továbbítani azadatvédelmi felelősnek,

- adatvédelmi incidens estén az incidens észlelését követően azonnal jelezni azt és annak körülményeit azadatvédelmi felelősnek és az adatvédelmi tisztviselőnek, és közreműködni az incidens elhárításában, kárenyhítésben, részletes felderítésben.

XIII.7. AzIntézményadatvédelmi tisztviselőjének és belső adatvédelmi felelősének adatai

Az Intézmény adatvédelmi tisztviselőinek (DPO) elérhetőségei:

név	Dr. Berta Lilla
telefonszám	+36 30 528 4995
e-mail cím	adatvedelem@mfkh.hu
név	Nagy József
telefonszám	+36 30 616 0305
e-mail cím	adatvedelem@mfkh.hu

Az Intézmény belső adatvédelmi felelősének (BAF) elérhetőségei:

név	Dr. Orosz Krisztina
telefonszám	+36 20 3297537
e-mail cím	adatvedelem@mfkh.hu

XIV. Az adatvédelmi ellenőrzés rendszere

A DPO jogosult és egyben köteles azIntézmény szervezetén belül feladatkörébe tartozó ellenőrzéseket végezni, amely eredményességének biztosítása érdekében a vizsgált szervezeti egység köteles teljes körűen és a vizsgálat akadályozása nélkül adatot szolgáltatni. A DPO ellenőrzési tevékenysége része azIntézményen belüli komplex ellenőrzési mechanizmusnak.

A belső adatvédelmi ellenőrzés célja, hogy a DPO meggyőződjön arról, hogy az egyes szervezeti egységek az adatvédelemmel kapcsolatos jogszabályoknak és belső szabályzatoknak megfelelően kezelik-e az adatokat.

A DPO az adatvédelmi tevékenység átfogó ellenőrzésének (pl. valamely szervezeti egység adatkezelési gyakorlatának ellenőrzése, HR terület adatkezelési gyakorlatának ellenőrzése stb.), illetve célvizsgálatának lefolytatásáról az érintett szervezeti egység vezetőjét az ellenőrzés kezdete előtt 15 nappal e-mailben tájékoztatja, melyben az eljárás kezdő időpontjára is javaslatot tesz. A szervezeti egység vezetője köteles gondoskodni arról, hogy a DPO a javasolt időpontban megkezdhesse ellenőrzését, illetve szükség esetén – legfeljebb három munkanapon belüli – új időpontra tesz javaslatot.

Az ellenőrzés során a DPO a szervezeti egység irodahelységeibe beléphet, az irataiba betekinthet, a szervezeti egység munkatársaitól tájékoztatást kérhet adott üggyel vagy bármely adatkezelési tárgykörrel kapcsolatos adatkezelésről. A megkeresésnek az érintett szervezeti egység a megjelölt határidőben – annak hiányában 5 munkanapon belül - köteles eleget tenni.

Egyes célvizsgálatok esetében a DPO előzetes bejelentés nélkül is végezhet vizsgálatot (pl. adatkezelési tájékoztatók kihelyezése).

A vizsgálatokról a DPO vizsgálati jelentést készít. A vizsgálati jelentés tartalmazza az ellenőrzött szervezeti egység, valamint annak vezetője nevét, az ellenőrzés lefolytatásának tényét, annak időpontját és időtartamát, a vizsgálat körülményeit, adatokat, megállapításokat. A vizsgálati jelentésre az érintett szervezeti egység vezetője észrevételeket tehet. A véglegesített vizsgálati jelentést a DPO a főigazgató, a belső adatvédelmi felelős, valamint az érintett szervezeti egység vezetője részére is e-mail útján megküldi. Amennyiben a DPO jogosulatlan adatkezelést észlel, a jelentésnek tartalmaznia kell a jogosulatlan adatkezelés ismertetését, és annak megszüntetésének szükségességét, valamint a megszüntetésre vonatkozóan annak adatvédelmi jogi szempontjait.

A megszűntetéssel kapcsolatban megtett és esetlegesen tervezett intézkedésekről a szervezeti egység vezetője a vizsgálati jelentés kézhezvételétől számított 30 napon belül tájékoztatást nyújt a főigazgató, a belső adatvédelmi felelős és a DPO részére. Ennek megvalósulásáról a DPO-nak a jelen Adatvédelmi Szabályzatban előírt rendszeres beszámolójában ki kell térnie.

A DPO jogsértés megállapítása hiányában is jogosult a szervezeten belüli és kívüli általa legjobb gyakorlatnak ítélt eljárásokról az éves vagy eseti vizsgálati jelentésében vagy akár egyedi formában tájékoztatást adni és javasolni egy adott eljárás módosítását, vagy új eljárás bevezetését.

XV. Kötelező adatkezelések felülvizsgálata

Az Infotv. 5. § (5) bekezdése a kötelező adatkezelések tekintetében előírja, hogy az Adatkezelő az adatkezelés megkezdésétől számított legalább háromévente felülvizsgálja azt, hogy az általa vagy a megbízásából eljáró adatfeldolgozó által kezelt személyes adatok kezelése az adatkezelés céljának eléréséhez szükséges-e. A vizsgálat eredményét a törvény előírásai szerint dokumentálni kell és azt 10 évig meg kell őrizni, valamint azt a NAIH kérése esetén a hatóság rendelkezésére kell bocsátani.

Az adatvédelmi tisztviselő köteles a szervezeti egységek bevonásával a vizsgálatot elvégezni és az elkészült jegyzőkönyvet benyújtani a főigazgató és a belső adatvédelmi felelős számára jóváhagyás céljából.

XVI. Felügyeleti hatóság

A természetes személyek alapvető jogainak és szabadságainak a személyes adataik kezelése tekintetében történő védelme, valamint a személyes adatok Unión belüli szabad áramlásának megkönnyítése érdekében minden tagállam köteles létrehozni, illetve kijelölni egy vagy több független közhatalmi szervet (Felügyeleti hatóság), amely a GDPR alkalmazásának ellenőrzéséért felel. A Felügyeleti hatóságnak a szerepét Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) tölti be. A Felügyeleti hatóság elősegíti a GDPR-nak az Unió egész területén történő egységes alkalmazását. A nemzeti felügyeleti hatóságok e célból együttműködnek egymással.

Minden Felügyeleti hatóság a saját tagállamának területén illetékes, azonban minden felügyeleti hatóság jogosult a hozzá benyújtott panaszok kezelésére, illetve jogosult a GDPR rendelkezéseinek megsértése esetén eljárni, ha

- az ügy tárgya kizárólag egy, a hatóság tagállamában található tevékenységi helyet érint, vagy
- ha kizárólag a tagállamában érint jelentős mértékben érintetteket.

A Felügyeleti hatóság által kiszabható bírság mértéke több rendelkezés megsértése esetén sem haladhatja meg a legsúlyosabb jogsértés esetén meghatározott összeget. A kiszabható bírság felső határa 20 millió EUR, vállalkozások esetén az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4%-át kitevő összeg; a kettő közül a magasabb.

XVII. Oktatás, képzés

AzIntézmény, mint adatkezelő köteles gondoskodni arról, hogy valamennyi vezető állású személye, alkalmazottja az adatvédelmi jogszabályi rendelkezéseket, valamint a jelen Szabályzatban foglaltakat megismerje és betartsa, az adatvédelmi kötelezettségekkel, illetve az adatkezelési célokkal tisztában legyen és szükség esetén a GDPR-ban, az Infotv-ben valamint a jelen Szabályzatban rögzítetteknek megfelelően járjon el (kötelező oktatás). AzIntézményfőigazgatója és belső adatvédelmi felelőseaz adatvédelmi tisztviselő bevonásávalgondoskodik az oktatás megszervezéséről és lebonyolításáról, valamint az oktatási anyag elkészítéséről.

XVIII. Egészségügyi adatok kezelésének általános adatbiztonsági szabályai az Eüakr. alapján

AzIntézménybenüzemelőklinikaiprogramokkalcsakazarrajogosultszemélydolgozhat. Mivel a betegszemélyiésápolásiadataikiemeltvédelmetélveznek, ezértbiztosítanikellnemcsak a programokkaldolgozószemélyekazonosítását, de a számukramegengedettműveletekszabályozhatóságát is.Újdolgozófelvételekor a Munkahelyivezetőírásbanközliazinformatikaiosztálymegbízottmunkatársával (Intézményirendszergazda) a dolgozónevét, beosztását, (orvosesetében - titulusát, orvosipecsétszámát), munkakörétés a munkavégzéshelyét.A fentiadatokalapjánazIntézményirendszergazdaelőállítja a felhasználóibelépésijogosultságokatéshozzáférésilistát a megadottmunkahelyekhez.

A medikairendszerbentároltadatokvédelméértaz Adatvédelmitisztviselőfelelős. Betegdokumentációrólkértmásolatoknyilvántartásaazerrekijelöltszemélyfeladata.A medikairendszerbevalóbelépéscsaksajátfelhasználónévvelésjelszóvallehetséges, melytevékenységmindenesetbenvisszaellenőrizhetőésnyomonkövethető. A medikairendszerbenvalójogosultságokszintjétazegyesfoglalkoztatottiköröktekintetébenazInformatikaiBiztonságiSzabályzatrészleteselőírásaitartalmazzák.Az adatokpontosságáértazadatokatszármaztatóésrögzítőmunkatárs a felelős. Az adatokbevitelekorazegészségügyidokumentációvezetésérevonatkozószakmaielőírásokésprotokollokrendelkezéseitmaradéktalanul be kelltartani.

Az adatkezelésirendszerműködésimegbízhatóságatekintetébenbiztosítaniszükséges, hogyazabbaadatotrögzítőkmegfelelőismeretekkelésmunkafegyelemmelrendelkezzenek, valamint a rendszermegfelelősségefolyamatosanellenőrizvelegyen.

A számítástechnikairendszertfolyamatosanellenőrizniésszükségszerintbővítenikell. Az archívtároláshelyigényét, a rendezetttárolásfeltételeit, a tűz – ésfizikaimegsemmisüléselleniévédelemműszakifeltételeitbiztosítaniéskarbantartanikell. Jogszabályváltozás, vagyegyéb ok miattszükségesséválómódosításeseténazadatvédelmiésadatkezelésiszabályzatmódosítását, korszerűsítését, továbbá a karbantartástaz Adatvédelmitisztviselővégzi.

Azegészségügyidokumentációosztályonvalótárolásaazilletéktelenekszámárahozzáférhetetlen, az Adatkezelő, illetve a betegellátószámárapedighozzáférhetőmódonkell, hogytörténjen.

Archiválásesetén az adatkezelés folyamatának meg kell felelnie az Iratkezelési szabályzat előírásainak.

Minden munkatárs feladata az eltulajdonítás ellen az alábbi alapelvek betartása, illetve ezek elősegítése, továbbá az érintett munkatársak megfelelő tájékoztatása a jogszabályi háttérről és a jelen szabályzatról:

- Az ellátás alatti, illetve azzal kapcsolatos dokumentációt az ellátást követően olyan helyen kell tartani, ahol azzárható és ily enesetben be is zárt.
- A betegszállítása, más telephelyen vagy rendelőben történő vizsgálata során a dokumentumot személyszerint a vizsgálatért, vagy beavatkozásért felelős, vagy azátvételt intéző egészségügyi dolgozónak kell átadni, borítékban vagy dossziéban.
- A beteggel kapcsolatos dokumentációk, adatok eltulajdonításának gyanúja esetén az Adatvédelmi tisztviselőt kell értesíteni.
- Tényleges adateltulajdonítás akor jegyzőkönyvet kell felvenni és az Adatvédelmi tisztviselőt tájékoztatni kell az eseményről, a jegyzőkönyv egy példányának eljuttatása mellett.

Az Intézmény adatvédelmi rendszerének felépítését a Szervezeti és Működési Szabályzat, valamint jelen szabályzat rögzíti.

Az egyes szervezeti egységekben a szervezeti egységen belül az adatkezelésre jogosultak körét, az adatkezelés módját, adatok továbbítását és nyilvántartását. Az Intézmény által kezelt adatok és dokumentumok kezelésének, megőrzésének és tárolásának rendjét az Intézmény hatályos Iratkezelési Szabályzata határozza meg, függetlenül az adatok formátumától. Az Intézményben az iratkezelés elektronizált vegyes iratkezelési rendszerben történik.

Az elektronikus iratkezelési szoftver hozzáférési jogosultságainak, az egyedi azonosítóknak, a helyettesítési jogoknak a kiosztását a rólés jogszerűségéről az igazgatás-szervezési osztályvezető kötelessége gondoskodni az informatikai osztály bevonásával.

Az egészségügyi szolgálati jogviszonnyal rendelkező munkavállalók esetében az adatok kezelésével, védelmével kapcsolatos feladat-, hatás- és jogköreit a munkaköri leírás tartalmazza. Az Intézmény fokozott biztonsági fokozatba tartozik (beteg adatok, személyes adatok és pénzügyi adatok kezelése), általános informatikai feldolgozást végez. Az

IntézményrendelkezikInformatikaiBiztonságiSzabályzattal (IBSZ), melyalapvetőcélja, hogyazinformatikairendszeralkalmazásasoránbiztosítsaazadatvédelemalkotmányoselveinek, azadatbiztonságkövetelményeinekérvényesülését, s megakadályozza a jogosulatlanhozzáférést, azadatokmegváltoztatásátésjogosulatlannyilvánosságrahozatalát. Meghatározzaazegyesfolyamatoktekintetébenazegyesszereplőkkötelezettségeit, valamintazellenőrzésrejogosultakkörét. Az Intézményrendelkezik a 2013. évi L. törvény 13. §-ábanmeghatározottfeladatokellátásáraelektronikusinformációsrendszerbiztonságáértfelelőssze méllyel (IBF).

Az egészségügyidokumentációbanazadatokatnemlehettörölni, a hibásadatokkijavítására is csakakképpkerülhetsor, hogyazeredetilegfelvettadat is megmaradjon. Az egyesbetegadatokkezelésévelkapcsolatosrészletesszabályokatjelenSzabályzattartalmazza.Az egészségügyidokumentációtirattárbatörténőátadásakor, valamint kiadás és betekintés esetén is tételesen (kórlap, lázlap, ápolási lap, dekurzus, lelet, stb.) éslapszámszerintkellátvenni, melysegítségévelazadatokmegsemmisítése, elvesztése, megváltoztatásamegakadályozható.

Az eredetiegészségügyidokumentációIntézményenkívülikiadásanemmegengedett – ettőlazügyészségikikéréseseténlehetkizárólageltérni.Hiányzóegészségügyidokumentációról – ideértveazelvesztést, megsemmisülést – a főigazgatót, azorvosigazgatót, valamint az adatvédelmitisztviselőt a hiányészlelésétkövetőenhaladéktalanulírásbantájékoztatnikell.Intézménybőltávozottbetegdok umentációját a távozásnapján, különösméltánylástérdemlő, indokoltesetbenlegkésőbb a távozástkövető 2 (két) munkanaponbelül le kellzárniazadatkezelésirendszersérüléseesetére.

Az Intézményrendelkezik a mindenkoritechnikaifejlettségnekmegfelelőműszaki, szervezeti, programozási, jogi, ügyrendiintézkedésekmegtételéhezazoneszközökkel, amelyek a védelemtárgyánakkülönbözőveszélyforrásokbólszármazókártokozóhatásokkal, szándékokkalszembenimegóvásátelősegítik, illetvebiztosítják.Az informatikaibiztonságifeladatokelvégzéseazInformatikaiOsztályfelügyeletemellettzajlanak.

A gazdaságirendszerekbencsakazarrajogosultszemélydolgozhat. A programokhozhozzáférési jog, kizárólagazadottterületvezetőjénekelőzetesengedélyéveladhatóki.Az Intézménybelsőadatállományaihoz, valamint a gépparktávmenedzseléséhezkülsőhozzáférésteсsak VPN kapcsolatonésnagyonindokoltesetben, csak a főigazgatókülöntájékoztatásautánaazInformatikaivezetőengedélyévellehetséges,

függetlenül a hozzáférésfizikaivoltától (Internet, betárcsázás, stb).A belsőhálózatvédelméttűzfalrendszerhasználatávalkellbiztosítani; valamintazInternetheztörténőhozzáféréscsakezen a kapcsolatonkeresztülvalósulhat meg a belsőhálózatothasználószámítógépekesetén; a programnakrendelkezniekell a belülről kifelé és a kívülrőlbefeléirányulóadatforgalomtípusonkéntiésfelhasználónkéntiszabályozásánaktulajdonságával, valamintszétkelltudniaválasztani a belsőéskülsőadatforgalmat.

Az Intézménymindenszámítógépénvírusellenőrző program került telepítésre, ugyanígy a szerverekés a tűzfalrendszervírusellenőrzőprogrammal van ellátva. A vírustámadásokveszélyénekminimalizálásaérdekében a vírusvédelmirendszernapitöbbszörifrissítésebiztosított.Az egyesfelhasználóksajátfelhasználónévvelésjelszóvalrendelkeznek, melybizalmaskezeléséreírásbelinyilatkozattalvállalnakfelelősséget.A jelszavakatvagy a jelszófájlokat a hálózatonnyílt, olvashatóformábantovábbítanitilos. A felhasználóijelszószerkezetiszabályaival (bonyolultság) szembentámasztottkövetelményeketmindenesetbenazhatározza meg, hogymilyen a kiszolgálóntároltadatokérzékenységibesorolásaésebbőlkövetkezően a kiszolgálóinformatikaibiztonságiosztálybasorolása.

Az Intézményhálózatáraszámítógépet, illetveegyébgyengeáramúberendezéstkizárólagazInformatikaiosztálymunkatársaicsatlakoztathatnak. A szabályzatnakmegfelelően a nemhasználtvégpontokat, illetveaktíveszközportokatinaktívállapotbakellhelyezni. Az egymástóljólelkülöníthetőfeladatokatellátógépeketkülönhálózatbakellszervezni.

A számítógépesadatállományrólnapontatörténikmentés. Az adatbázisszerverekről éjjel 1 és 3 óraközött, elosztottanautomatikusmentéstörténikkülsőadattárolóra. Az adattárolóhelyetechnikaiésfizikaivédelemalattálló, önállóhelység.A számítógépeshálózatbanmindenolyanprogramnakmegfelelőendokumentáltnakkelllennie, mellyel a védettadatfeldolgozásatörténik. A képernyősadatmegjelenítéstitokvédelemszempontjábóladattovábbítóeszköznekminősül, ezértminősítettadatfeldolgozásasorán a helységbencsak a betekintésrejogosulttartózkodhat.

Az Intézménybenbiztosítottazadatkezelésirendszerektűzvédelmiszempontbóltörténővédelme. Az adattartalmúszámítástechnikaiberendezésekIntézményből történőkiszállításacsakfőigazgatóien

gedéllyellehetséges.A különlegesvédelmetigénylőinformatikaieszközökhelységébecsakazarrajogosult, ellenőrzöttbelépésirenddelléphet be (riasztóberendezés).Az adatokvédelmét a feldolgozás, adattovábbításéstárolássoránmegfelelőenbiztosítanikell. A biztonságiokbólelőállítottmásolatiadathordozókatazeredetitőlterületilegtávolkelltartani.

A megsérült, elveszettadatokvisszaállításátésannakmértékét – a lehetőségekfelmérésével, indoklásávalésmérlegelésével – a vezetőkkelegyeztetveazadatvédelmitisztviselőrendeli el írásban. Amennyiben a visszaállítás – reálismódon – nemvalósítható meg, arrólazadatvédelmitisztviselőírásosfeljegyzéstkészít, melyetaziktatásirendszerben „Adatvédelem” iktatásijelzésseltartanaknyilván. A visszaállításról – amennyibenazméltányosésmegoldható –, a mulasztásértfelelőskötelesgondoskodni. A méltányosságés a személyesfelelősségeldöntéseazadatvédelmitisztviselőhatáskörébetartozik.

Minden foglalkoztatottkötelezettségeazIntézményáltalkiadottszabályzatokelőírásainakbetartásaésbetartatása.Betegellátássorán, valamintaztkövetőengondoskodnikell a dokumentációfolyamatosanellenőrizhetőelhelyezéséről. Amennyibenazellátottátszállításrakerülmástelephelyre, vagyintézménybe, a betegdokumentációtzártborítékbanvagydossziébankellátadni – összhangbanazIratkezelési Szabályzatelőírásaival.Amennyibenfelmerülazadatokeltulajdonításánakgyanúja, azonnal, de legkésőbb a következőmunkanaponértesítenikell a BelsőAdatvédelmiFelelőst; ténylegeseltulajdonításeténjegyzőkönyvfelvételétkövetően, annakegypéldányát el kelljuttatnihozzá.Az elektronikusmedikairendszerbenrögzítettadatokért az IntézményInformatikaivezetőjefelelős.

Az Intézményadatvédelmitisztviselője, a belsőadatvédelmifelelős,valamintazInformatikaivezető a mindenkorifőigazgatómegbízásábóljogosultellenőrizni a felhasználókat.Az adatkezelésirendszerbeminden felhasználó csakéskizárólagfelhasználónévésjelszósegítségévelléphet be, melymindenesetbenrögzíthetőésvisszakereshető.

A személyazonosítóadatokfelvétele a Betegfelvételiablakbantörténik, melyreazellátássoránazellátásbanrésztvevők – elsősorbanazadminisztrátorok, kezelőorvos – jogosultésköteles. Amennyibenazegészségügyidokumentációbanszereplőadathibás,

utólagosjavításáracsakakképpkerülhetsor, hogyazeredetilegfelvettadat is megállapíthatólegyen,

Az adatokról, s egyben a keletkezettdokumentációrólmásolatkérhető, melynekrészletesszabályaitazIntézményTérítésidíjszabályzatatartalmazza.Az egészségügyidokumentációrészeként meg kellőrizniazalábbiakat:azegyesvizsgálatokrólkészültleletek, gyógykezeléséskonzíliumsoránkeletkezettiratok, ápolásidokumentáció, képalkotódiagnosztikaieljárásokfelvételeirőlkészültleletek. A személyazonosítóadatok a medikairendszerbe a betegfelvételsoránkerülnek be, melyfolyamatalapja a hatóságiszervekalapjánkiadott, személyazonosságot, illetvejogosultságotigazolóokmányokbemutatása.A gyógykezeléssoránkeletkezettadatokazápolásiésgyógyításitevékenységbenrésztvevőkáltalrögzítetttények.

Személyesadatokcsakéskizárólaghatóságiigazolványbemutatásaalapjánkerülhetnek be a rendszerbe. A felvettadatoknakhiteleseknek, pontosaknak, teljeseknekésidőszerűeknekkelllenniük; azokfelvételeéskezelésetisztességes, törvényes, pontos, teljesésidőszerűkell, hogylegyen.A diagnózisésbeavatkozáskódoknakazellenőrzéséreazellátástvégzőorvosköteles, melyreazadatbevitellelegyidejűlegkell, hogysorkerüljön, de legkésőbbazellátottIntézményből történőtávozásáig.Az Intézményáltalhasználtmedikairendszerelektronikusalaponrögzítiazellátottról, valamint a velekapcsolatbanfelvettadatokat.
Intézményünkbenazazonosítóadatokfelvételétazadminisztrátorokésorvosírnokokvégzik, mígazellátásraésazegészségügyiadatokatazellátástvégzőorvosok.Az egyesadatokadatkezelésirendszerbetörténőbekerülése, illetveazadatkezelésirendszerbőltörténőtovábbításánakrészletesszabályaitjelenSzabályzat, dokumentációmásolatánakkikéréseesetébenpedigazIntézményTérítésidíjszabályzattartalmazza.

Az Intézménybenműködtetettszámítástechnikairendszertfolyamatosanellenőrizniésszükségszerint bővítenikell. A rendszerműködésiműszakimegbízhatóságánakalapja a működésselkapcsolatosvisszajelzésekésproblémákhatékonykezelése, melyértamindenkorifőigazgató a felelős.Az archívumszükségeshelyigényét, valamint a

keletkezettdokumentumoktűz-, víz- ésegyébfizikaimegsemmisülésellenivédelmétműszakifeltételekkel is biztosítanikell – összehangbanazIratkezelésiszabályzatelőírásaival.

JelenSzabályzategybenazIntézményadatkezelésirendszerénekszabályozása, melyösszhangban a külsőésbelsőkapcsolódószabályozásielőírásokkal, teljességébenszabályozzaazadatkezelésrendszerét.JelenSzabályzat a kiadásidőpontjábanmegvalósulóadatkezelésirendszerműködésérevonatkozószabályokattartal mazza, melynekfolyamatosfejlesztése, módosítása, javítása, valamint a változójogszabályikörnyezetnekvalómegfeleltetése abelsőadatvédelmifelelős kötelezettsége azadatvédelmitisztviselőbevonásával.

MindaddigjelenSzabályzatelőírásaitkellirányadónaktekinteni a gyakorlatitevékenységsorán, ameddigannakkihirdetettmódosításárasornemkerül.Az adatkezelőktekintetébenattólfüggően, hogymilyenadatkezelésitevékenységetvégeznek, tevékenységüketjelenSzabályzattovábbifejezeteibenmeghatározottakszerintvégzik.Amennyib en a kórlapokkódolása, adatfeldolgozás, dokumentumokarchívtárolásátmegvalósítófeladatokban a feldolgozástés a fejlesztéstvégzőfeladatkörökelválasztásrakerülnek, annakténytdokumentálniszükséges.

Az Intézménybenfolyamatosanbiztosítva van azadatkezelőkképzése, továbbképzéseéskonzultációslehetősége.JelenSzabályzathatálybalépésétkövetőenmindenévbe nlegalábbegyalkalommalsorkerüladatvédelmitovábbképzésre.

Az Intézménybiztosítjamindenszervezetiegységszintűosztályosadatvédelmifelelősszámára, hogy a belsőelektronikusrendszerébe, vagyazadatvedelem@mfkh.hue-mail címrenemmegfelelőségtapasztalásaeseténjelentéstküldjenek.A jelentésekrőlazIntézménybelsőadatvédelmifelelőseadatvédelminyilvántartástvezetazOrszágos KórháziFőigazgatóságáltalbiztosított DATINF elektronikusrendszerben.

Az Intézmény tevékenységének gyakorlása során felvett adatokat nyilván kell tartani. A nyilvántartás eszköze lehet minden olyan eszköz, vagy módszer, amely biztosítja az adatok megfelelő védelmét.Az Intézmény tevékenysége során keletkező dokumentáció, egészségügyi dokumentáció, valamint zárójelentés tárolásának, megsemmisítésének és archiválásának részletes szabályait az Iratkezelési szabályzatban határozta meg.

XIX. Záró rendelkezések

Jelen Szabályzat hatálybalépésével:

visszavonom a 182-101-7/2021 azonosítószámú (iktatószám: MFKH/1611-1/2021) Adatvédelmi Szabályzatot.