BORSOD-ABAÚJ-ZEMPLÉN MEGYEI KÖZPONTI KÓRHÁZ ÉS EGYETEMI OKTATÓKÓRHÁZ
3526 Miskolc, Szentpéteri kapu 72-76.

Főigazgatói Szabályzat

ADATVÉDELMI SZABÁLYZAT

Készítette:	**Rivnyák József** **Intézeti Adatvédelmi Felelős**	2019.08.12. **Dátum**
Minőségügyi szempontból ellenőrizte:	**Dr. Tóth László** **Igazgatói Szaktanácsadó**	B.A.Z. Megyei Központi Kórház és Egyetemi Oktatókórház *dr. Tóth László* *igazgatói szaktanácsadó* 2019. 08. 12. **Dátum**
Jóváhagyta és érvénybe léptette:	**Dr. Révész János** **Főigazgató**	2019 AUG. 12 **Dátum**

A dokumentum kódja:	**FISZ – 006** - 2
Kiadás száma:	**2**
Érvénybelépés időpontja:	**2019. augusztus 15.**

A példány sorszáma: ☐☐/ **A példány tulajdonosa:**

Nyilvántartott példány: ☐ **Munkapéldány:** ☐

Az egyes példányok tulajdonosait az Elosztási lista tartalmazza sorszám szerint.

MÓDOSÍTÁSOK JEGYZÉKE

Sorszám	Módosította Aláírás/dátum	Az oldal változat-száma	Módosított oldalszám	Jóváhagyta Aláírás/dátum	Minőségügyi szempontból ellenőrizte Aláírás/dátum	Módosítás időpontja
	Új kiadás: 2019. 08. 15.					
1.	**Rivnyák József s.k. 2020.01.06.**	**2/39**		**Dr. Révész János s.k. 2020.01.10.**	**Dr. Tóth László s.k. 2020.01.07.**	**2020. 01. 15.**
		2	**4/39, 39/39 A03a adatlap A03b adatlap**			
		A módosított részeket vékony folytonos vonal jelöli: ——————				
2.	**Rivnyák József s.k. 2020.03.10.**	**2/39**		**Dr. Révész János s.k. 2020.03.12.**	**Dr. Tóth László s.k. 2020.03.11.**	**2020. 03. 15.**
		3	**4/39, 39/39**			
		2	**M01 melléklet A03a adatlap A03b adatlap**			
		1	**A09 adatlap**			
		A módosított részeket vastag folytonos vonal jelöli: ——————				

TARTALOMJEGYZÉK Oldal

FISZ-006-2/**M01**	Az egészségügyi dokumentáció megismerésének, illetve kiadásának folyamata
FISZ-006-2/**A01**	Beleegyező nyilatkozat fénykép, videó- és hangfelvétel készítésébe (E-MK 2002-74/19)
FISZ-006-2/**A02**	Meghatalmazás (E-MK 2001-112/19)
FISZ-006-2/**A03a**	Egészségügyi dokumentáció kikérő lap – Magyar nyelvű (E-MK 2017-139/19)
FISZ-006-2/**A03b**	Egészségügyi dokumentáció kikérő lap – Angol nyelvű (E-MK 2017-139/19)
FISZ-006-2/**A04**	Egészségügyi dokumentáció kérése további gyógykezelés céljából (E-MK 2003-35/19)
FISZ-006-2/**A05**	Nyilatkozat képalkotó diagnosztikus eljárás során készült felvétel kiadásához (E-MK 2001-110/19)
FISZ-006-2/**A06**	Látlelet kérő lap (E-MK 2002-59/19)
FISZ-006-2/**A07**	Képalkotó diagnosztikai eljárással készült egészségügyi dokumentáció másolat kérése (E-MK 2016-23/19)
FISZ-006-2/**A08**	Képalkotó diagnosztikai eljárással készült egészségügyi dokumentáció másolat kérése további gyógykezelés céljából (E-MK 2016-24/19)
FISZ-006-2/**A09**	Megbízólevél osztályos adatvédelmi megbízott részére

1. A SZABÁLYZAT CÉLJA, HATÁLYA, ALAPELVEK, ALAPFOGALMAK

1.1. Bevezető rendelkezések

1. A Borsod-Abaúj Zemplén Megyei Központi Kórház és Egyetemi Oktatókórház (a továbbiakban: Kórház) jelen szabályzatban (a továbbiakban: Szabályzat) határozza meg a természetes személyek személyes adatainak kezelésével és védelmével kapcsolatos irányelveket, valamint az adatvédelmi tevékenység ellátásában résztvevő szervezeti egységek feladatait és együttműködésük kereteit. A Kórház általános adatkezelési tájékoztatóját e Szabályzat melléklete tartalmazza.

2. A Szabályzat hatálya alá tartozó személyek kötelesek a tevékenységük során a Kórház kezelésében lévő személyes adatokat a mindenkori jogszabályi rendelkezéseknek megfelelően, így különösen a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679/EU európai parlamenti és tanácsi rendelet (a továbbiakban: GDPR), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) alkalmazandó rendelkezései, az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény rendelkezései valamint a Kórházra irányadó egyéb jogszabályok rendelkezései szerint kezelni. A Kórház a személyes adatok kezelésével járó tevékenysége során érvényre juttatja a GDPR alapelveit, így különösen:
   a/ jogszerűség, tisztességes eljárás és átláthatóság elve: a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni;
   b/ célhoz kötöttség elve: a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történik, és azokat a Kórház nem kezeli ezekkel a célokkal össze nem egyeztethető módon;
   c/ adattakarékosság elve: a kezelt személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk;
   d/ pontosság elve: a kezelt személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;
   e/ korlátozott tárolhatóság elve: a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé;

f/ integritás és bizalmas jelleg: a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve;

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

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

3. A Szabályzat hatálya alá tartozó személyek kötelesek az olyan tevékenységük során, amely szükségszerűen együtt jár személyes adatok kezelésével, az adott tevékenységre vonatkozó – a Szabályzat I.(. címében felsorolt – speciális szabályzatokban foglalt rendelkezések mellett a jelen szabályzat rendelkezései szerint eljárni azzal, hogy amennyiben a speciális szabályzat a jelen szabályzattal ellentétes rendelkezést tartalmaz, úgy jelen szabályzat alkalmazandó.

1.2. A Szabályzat célja

4. Jelen Szabályzat célja, hogy biztosítsa a Kórház tevékenysége során a személyes adatok védelméhez fűződő jog érvényesülését, továbbá, hogy a Kórház által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes és különleges adatok kezelése során irányadó adatvédelmi és adatbiztonsági szabályokat.

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

6. A Szabályzat további célja, hogy meghatározza a Kórház szervezeti egységeinél vezetett, személyes adatokat tartalmazó nyilvántartások vezetésének és működtetésének jogszerű rendjét, valamint biztosítsa a személyes adatok védelme elveinek és az adatbiztonság követelményeinek érvényesülését.

1.3. A szabályzat személyi hatálya

7. Jelen Szabályzat személyi hatálya kiterjed a Kórház közalkalmazottaira, munkavállalóira, egyéb munkavégzésre irányuló jogviszonyban állókra, továbbá mindazon szerződéses partnerekre, akiknek jogait vagy jogos érdekeit az adatkezelés érinti (a továbbiakba együttesen: dolgozók), továbbá azon természetes személyekre (a továbbiakban: érintett), akik személyes adatait a jelen Szabályzat hatálya alá tartozó adatkezelések tartalmazzák, továbbá azon érintettekre, akik jogait vagy jogos érdekeit az adatkezelés érinti. A Kórház megbízásából személyes adatok kezelését vagy feldolgozását végzők esetén az erre a jogviszonyra a Kórház által kötött szerződésben a GDPR 28. cikkének megfelelően rendelkezni kell arról, hogy a Kórház által megbízott adatfeldolgozó a feladata ellátása során hogyan juttatja érvényre jelen Szabályzat rendelkezéseit.

1.4. A szabályzat tárgyi hatálya

8. A Szabályzat tárgyi hatálya a Kórház mindazon adatkezeléseire kiterjed – függetlenül attól, hogy az adatkezelés elektronikusan vagy papíralapon történik –, amelyek
   a/ az egészségügyi ellátás nyújtásához kapcsolódó adatkezelést valósítanak meg a Szabályzat 3. fejezetében felsorolt jogszabályok és belső szabályzatok szerint;
   b/ az egészségügyi ellátáson kívüli ügyfélkapcsolati jellegű adatkezelést valósítanak meg (a Kórházzal kapcsolatba lépni szándékozó, kapcsolatban álló vagy kapcsolatban állt személyek, beleértve ezek meghatalmazottait, képviselőit is);
   c/ foglalkoztatási jogviszonyhoz kapcsolódó adatkezelést valósítanak meg [a Kórházzal közalkalmazotti jogviszonyban, munkaviszonyban vagy egyéb foglalkoztatási jogviszonyban (együtt: foglalkoztatási jogviszony) álló, állt, vagy foglalkoztatási jogviszonyba lépni szándékozó személyek);
   d/ a Kórházzal szerződéses kapcsolatban álló társaságok képviselőinek, kapcsolattartóinak az adataira vonatkoznak.

1.5. Dokumentálási kötelezettség

9. A Kórház felelős a személyes adatok kezelésére vonatkozó alapelvek [GDPR 5. cikk (1) bek.] betartásáért. A Kórháznak képesnek kell lennie a személyes adatok kezelésére vonatkozó alapelvek betartásának igazolására [GDPR 5. cikk (2) bek.]. A megfelelőség igazolása különösen az adatkezeléshez kapcsolódó döntéseket megalapozó körülmények és a döntések (pl. az adatkezelés feltételeit meghatározó döntéselőkészítő iratok), az érintetteknek szóló adatkezelési tájékoztatók, az érintettől származó nyilatkozatok (pl. hozzájáruló nyilatkozatok, az adatkezelési tájékoztató megismerését igazoló dokumentumok), továbbá a személyes adatokat tartalmazó (elektronikus vagy papír alapú) dokumentumok szervezeten belüli vagy azon kívüli mozgásának megfelelő dokumentálásával történik. A Kórház – a GDPR 30. cikkének megfelelően – nyilvántartást vezet az általa végzett adatkezelésekről.

2. Alapfogalmak

10. Jelen Szabályzat alkalmazása során a GDPR 4. cikkében és az Infotv. 3. § 3., 4., 6., 11., 12., 13., 16., 17., 21., 23-24. pontjában meghatározott fogalmakon kívül az alábbi fogalmakat kell alkalmazni:
    a/ hatókörére, körülményeire és céljaira, ideértve különösen az új technológiák alkalmazásának esetét – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, és amelynek célja annak megállapítása, hogy a tervezett adatkezelés a személyes adatok védelmét hogyan érinti. Az adatvédelmi hatásvizsgálat egy olyan eljárás, amelynek során az adatkezelő a tervezett adatkezelési műveletet vagy műveleteket áttekinti, megvizsgálja az adatkezelés érintettekre gyakorolt esetleges hatását, felméri annak kockázatait, a kockázatok kezelésének módját, és mindezt megfelelően dokumentálja,
    b/ adatvédelmi tisztviselő: a Kórház szervezetében működő, a GDPR 39. cikkében meghatározott feladatokat a Kórház jelen szabályzatában foglaltak szerint ellátó, a Kórházzal foglalkoztatási jogviszonyban álló természetes személy,
    c/ álnevesítés (pszeudonimizálás) a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni,
    d/ deperszonalizálás (anonimizálás): a nyilvántartási rendszerben tárolt személyes adatok közül a személyazonosításra alkalmas adatok eltávolítása olyan, visszafordíthatatlan módon, hogy a nyilvántartási rendszerben megmaradó adatok a továbbiakban semmilyen körülmények között nem teszik lehetővé egy természetes személy azonosítását,

e/ dolgozói személyes adat: a Kórházzal foglalkoztatási jogviszonyban álló személyek adata,

f/ érdekmérlegelési teszt: jogos érdeken alapuló adatkezelés tervezett bevezetése esetén annak írásbeli dokumentálása, hogy az adatkezelő számba vette az adatkezelést megalapozó érdekeket, érveket, valamint az érintettek személyes adatok védelméhez fűződő – a tervezett adatkezelés ellen ható – jogait és érdekeit, és ezen érdekek és érvek összevetésével megalapozza az adatkezelés bevezetését vagy a bevezetés elutasítását,

g/ titkosítás: az adatok olyan átalakítása, melynek során az adat értelmezhetetlenné válik a megfelelő kulcs ismerete nélkül,

h/ törlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása a továbbiakban már nem lehetséges. A törlés célja megvalósítható deperszonalizálással (anonimizálással) [d/ pont] is.

i/ ügyvitel: a Kórház tevékenységére vonatkozó jogszabályokban a Kórház részére meghatározott közfeladatok ellátásával összefüggő eljárás.

3. A SZABÁLYZATHOZ KAPCSOLÓDÓ JOGSZABÁLYOK, BELSŐ SZABÁLYZATOK

GDPR	Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [az Infotv-nek a GDPR hatálya alá eső adatkezelésekre alkalmazandó szabályai – lsd. Infotv. 2. § (2) és (4) bekezdése]
Eüak.	1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről, és a végrehajtására kiadott jogszabályok
Eütv.	1997. évi CLIV. törvény az egészségügyről, és a kapcsolódó jogszabályok
Ebtv.	1997. évi LXXXIII. törvény kötelező egészségbiztosítás ellátásairól, és a végrehajtására kiadott jogszabályok
Kjt.	1992. évi XXXIII. törvény a közalkalmazottak jogállásáról, és annak az egészségügyi ágazatban történő végrehajtására vonatkozó jogszabályok
Mt.	2012. évi I. törvény a Munka Törvénykönyvéről
	A KÖZÉRDEKŰ ÉS A KÖZÉRDEKBŐL NYILVÁNOS ADATOK KEZELÉSÉNEK RENDJE
	a Kórház Informatikai Biztonsági Szabályzata
	a Kórház Iratkezelési Szabályzata
	a Kórház Szervezeti és Működési Szabályzata
	a Kórház szervezeti egységei által kezelt nyilvántartási rendszereket szabályozó utasítások
	a Kórház [kollektív szerződése és közalkalmazotti szabályzata], az egyes munkavállalói juttatásokat szabályozó külön utasítások.

4. AZ ADATVÉDELMI TEVÉKENYSÉG SZERVEZETE ÉS IRÁNYÍTÁSA A KÓRHÁZNÁL

4.1. Az adatvédelmi tevékenység ellátásában résztvevők

11. Az adatvédelmi tevékenység irányításában és ellátásában a Kórház szervezeti egységei – a Kórház Szervezeti és Működési Szabályzatában meghatározott feladatkörükön belül – az alábbiak szerint vesznek részt.

12. A főigazgató
    a/ kinevezi a Kórház adatvédelmi tisztviselőjét, és az adatvédelmi tisztviselő nevét és elérhetőségét bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak;
    b/ munkajogi értelemben vett közvetlen felettese az adatvédelmi tisztviselőnek, amennyiben munkaviszonyban, vagy közalkalmazotti jogviszonyban áll az intézménnyel.

13. A Kórház szervezeti egységeinek vezetői az irányításuk alá tartozó szervezeti egység tekintetében:
    a/ betartják és betartatják az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírásokat,
    b/ kijelölik az irányításuk alá tartozó szervezeti egység adatkezelési felelősét,
    c/ gondoskodnak arról, hogy az irányításuk alá tartozó szervezeti egységek felelősségi körébe tartozó nyilvántartási rendszerek naprakészek, megbízhatóak legyenek,
    d/ gondoskodnak arról, hogy az irányításuk alatt álló személyek az adatkezelés meghatározott feltételeinek megfelelően járjanak el [GDPR 32. cikk (4) bek.],
    e/ az adatkezelési felelős előterjesztésére – a Kórház döntéselőkészítésre vonatkozó szabályainak megfelelően – döntenek a jelen utasításban, illetve az adatkezeléssel járó folyamatot szabályozó egyéb belső szabályzatokban a feladat- és hatáskörébe utalt kérdésekben.

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

15. A panaszügyek kezeléséért, kivizsgálásáért felelős személy/szervezeti egység:
    a/ az adatvédelmi tisztviselő szükség szerinti közreműködésével ellátja az érintetti jogok gyakorlásával kapcsolatos beadványok megválaszolását (72. pont) a személyes adatok kezelését, illetve a GDPR szerinti jogaik gyakorlását érintő panaszok (72. pont 72.j/j/ alpont72.j/) kivételével.

16. Az Informatikai és Logisztikai Igazgatóság:
    a/ ellátja az informatikai biztonsági biztonsággal kapcsolatos feladatokat a folyamatos üzemeltetési feladatok kivételével, különösen a Kórház mindenkor hatályos információbiztonsági szabályzatában meghatározott feladatokat;
    b/ ellátja az IT fejlesztéseknél és beszerzéseknél a beépített adatvédelem kontrolljai meglétének biztosításával, az adatminőség biztosításával, az informatikai biztonság kockázatarányos szintjét biztosító jogosultsági és naplózási rendszer kialakításának megfelelőségével, a biztonságos szoftverfejlesztés alapelveinek érvényesítésével kapcsolatos feladatokat,
    c/ az IT üzemeltetés területén ellátja a személyes adatok kezelésével kapcsolatos technikai védelem megvalósítását, ellátja – a Kórház mindenkor hatályos információbiztonsági szabályzatában meghatározott – hatáskörébe tartozó információbiztonsági feladatokat, valamint rendelkezésre állási kontrollok biztosítását, a tárolt és továbbított személyes adatok bizalmasságának védelmét, az incidensfelderítési és -kezelési tevékenység támogatását.

17. A Jogi Osztály:
    a/ szorosan együttműködik a Kórház adatvédelmi tisztviselőjével feladatainak ellátásában,
    b/ szakmai támogatást nyújt az adatkezeléssel összefüggő, nem adatvédelmi jogszabályok értelmezésében,
    c/ segíti a Kórház peres képviseletét ellátó közalkalmazottat vagy meghatalmazottat az érintett által a Kórház ellen az érintett adatvédelmi jogainak megsértése miatt indított, illetve a Kórház által a Nemzeti Adatvédelmi és Információszabadság Hatóság határozatainak felülvizsgálata iránt indított perekben.

18. Az adatkezelési felelős az őt foglalkoztató szervezeti egység feladatkörén belül jelen szabályzat és egyéb belső szabályzatok szerint:
    a/ előkészíti az adatkezeléssel kapcsolatos, az adatkezelőt terhelő döntéseket, illetve abban közreműködik;
    b/ gondoskodik az adatkezeléshez kapcsolódó adminisztratív teendők ellátásáról (az adatkezeléssel összefüggő döntések dokumentálása, érdekmérlegelési teszt elvégzése, hatásvizsgálat lefolytatása, az adatkezeléssel összefüggő szerződések előkészítése, az adatkezelések nyilvántartásának naprakészen tartása stb.), illetve abban közreműködik;
    c/ együttműködik az ugyanazon adatkezelésben érintett más adatkezelési felelősökkel;
    d/ közreműködik az érintettek jogai gyakorlásának biztosításában;
    e/ közreműködik az adatvédelmi incidensek következményeinek elhárításában;
    f/ közreműködik az adatvédelmi tisztviselő vizsgálataiban;
    g/ közreműködik az adatvagyon-felmérés elkészítésében,
    h/ közreműködik a Kórház kezelésében lévő az adatok biztonsági osztályba sorolásában.

19. Adatkezelési felelőst valamennyi szervezeti egységnél ki kell jelölni. Adatkezelési felelősnek olyan személyt kell kijelölni, aki az adott szakterületet illetve – az információbiztonsági szakterületen – a szakterületek tevékenységét támogató IT rendszereket illetően kellő ismeretekkel bír.

4.2. Az adatvédelmi tisztviselő

20. Az adatvédelmi tisztviselőt a főigazgató nevezi ki az olyan, a Kórházzal foglalkoztatási jogviszonyban álló természetes személyek közül, aki ismeri a Kórház működését, feladatait, munkafolyamatait és rendelkezik:
    a/ jogi szakvizsgával vagy informatikai egyetemi végzettséggel;
    b/ az európai és hazai adatvédelemmel kapcsolatos főbb szabályozók, hatósági és bírósági határozatok, iránymutatások ismeretével;
    c/ alapvető adatvédelmi és IT folyamatok ismeretével;
    d/ legalább 1 év adatvédelmi területen szerzett gyakorlattal.

21. Az adatvédelmi tisztviselő kinevezése mellett a Kórház adatvédelmi tanácsadási feladattal egyéb, jogi vagy természetes személy szakértőt is megbízhat.

22. Az adatvédelmi tisztviselő független, függetlensége biztosítása érdekében szakmai feladatai ellátása során utasítást nem fogadhat el, szakmai feladatai ellátásával összefüggésben nem bocsájtható el. Jelen szabályzatban foglalt tevékenysége ellátása során autonóm, szakmai ügyekben kizárólag a főigazgatónak tartozik felelősséggel.

23. A Kórház elősegíti az adatvédelmi tisztviselő megfelelő szakmai feladatellátását, ennek érdekében a Kórház biztosítja különösen az adatvédelmi tisztviselő feladatai végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáférést, valamint a szakértői szintű ismereteinek fenntartásaihoz szükséges forrás biztosítását, elegendő idő biztosítását feladatai ellátásához, valamint az informatikai és a biztonsági szakterület együttműködése révén az adatvédelmi tisztviselő bevonását:
    a/ a megfelelő technikai-eljárási intézkedésekhez szükséges források meghatározása (költségvetési tervezés) során annak érdekében, hogy teljesüljenek az adatvédelem alapelvei a technikai vívmányok alkalmazása (beépített adatvédelem) és az adatvédelem-barát megoldások (alapértelmezett adatvédelem) révén;
    b/ a felügyeleti hatósággal történő együttműködés során, mellyel az adatvédelmi tisztviselő – az adatvédelmi csoport, a Jogi Osztály és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – tartja a kapcsolatot.

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

25. Az adatvédelmi tisztviselőt tisztsége fennállása alatt és annak megszűnését követően titoktartási kötelezettség terheli a tevékenysége során tudomására jutott, közérdekű vagy közérdekből nem nyilvános adatnak nem minősülő információk kapcsán.

26. A Kórházban nem lehet adatvédelmi tisztviselő az a természetes személy, aki a Kórházban az adatkezelési tevékenység céljainak, kereteinek, eszközeinek meghatározásáról dönt, különösen a főigazgató, adatkezelésért felelős szervezeti egység vezetője (**Hiba! A hivatkozási forrás nem található.** pont) és a belső ellenőr.

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

28. Az adatvédelmi tisztviselő nevét és elérhetőségeit a Kórház honlapján, székhelyén, telephelyén a nyilvánosság részére mindenkor elérhetővé kell tenni. A Kórház továbbá közli az adatvédelmi tisztviselő nevét és elérhetőségét a Nemzeti Adatvédelmi és Információszabadság Hatósággal.

29. Az adatvédelmi tisztviselő feladatai:
    a/ közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
    b/ ellenőrzi a GDPR, az Infotv. és az adatkezelésre vonatkozó más jogszabályok, valamint a jelen szabályzat, továbbá a Kórház egyéb belső szabályzatai rendelkezéseinek a megtartását, belső adatvédelmi ellenőrzési eljárást folytat le;
    c/ kivizsgálja – az érintett szakterületek, az adatvédelmi csoport és a Jogi Osztály bevonásával – a neki címzett panaszokat, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
    d/ az adatvédelmi csoporttal, a Jogi Osztállyal és az Informatikai és Logisztikai Igazgatósággal együttműködve elkészíti az adatvédelmi és adatbiztonsági szabályzatot;
    e/ az adatvédelmi csoporttal, a Jogi Osztállyal együttműködve gondoskodik az adatvédelmi ismeretek oktatásáról [elsősorban az intraneten közzétett segédanyagok útján];
    f/ az adatvédelmi csoporttal, a Jogi Osztállyal együttműködve személyes adatok kezelésére vonatkozó előírásokról tájékoztatást nyújt, tanácsot ad;
    g/ személyes adatot is kezelő új informatikai rendszer belső fejlesztéssel történő bevezetése során közreműködik az adatvédelmi hatásvizsgálat lefolytatásában;
    h/ az adatvédelmi incidenskezeléssel kapcsolatban ellátja a jelen szabályzat szerinti feladatokat;
    i/ éves összefoglaló jelentést készít a főigazgatónak;
    j/ kapcsolatot tart és – az adatvédelmi csoport, a Jogi Osztály és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – együttműködik a Hatósággal.

4.3. Az Adatvédelmi Csoport

30. Az Adatvédelmi tisztviselő feladatainak segítése keretében az adatvédelmi csoport (a továbbiakban: csoport) felügyeli az adatkezelési nyilvántartás vezetését.

A csoport:
(a) együttműködik az Adatvédelmi tisztviselővel az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
(b) segítséget nyújt az Adatvédelmi tisztviselővel az Intézmény egyéb belső szabályzatai rendelkezéseinek a megtartásában, valamint a belső adatvédelmi ellenőrzési eljárás lefolytatásában;
(c) részt vesz az Adatvédelmi tisztviselőhöz érkezett bejelentések kivizsgálásában, illetve jogosulatlan adatkezelés észlelése esetén adatkezelő vagy az adatfeldolgozó felhívásában annak megszüntetésére;
(d) az Adatvédelmi tisztviselővel valamint a Jogi Osztállyal együttműködve elkészíti az adatvédelmi és adatbiztonsági szabályzatot;
(e) gondoskodik az adatvédelmi ismeretek oktatásáról elsősorban az intraneten közzétett segédanyagok útján;
(f) koordinálja a személyes adatok kezelésére vonatkozó előírásokról szóló tájékoztatásnyújtást, tanácsadást;
(g) az Adatvédelmi tisztviselővel együttműködik az adatvédelmi hatásvizsgálat lefolytatásában;
(h) az Adatvédelmi Csoport tagjaként az incidenskezeléssel kapcsolatban ellátja a jelen szabályzat szerinti feladatokat.

31. Adatvédelmi incidens (papíralapú és nem papíralapú adatokra vonatkozóan egyaránt) felmerülése esetén az Intézmény csoportja haladéktalanul – szükség esetén olyan napon is, amikor az Intézménynél a munka szünetel – ülést tart annak érdekében, hogy megvizsgálja és kategorizálja a bekövetkezett incidenst, valamint meghatározza az esetleges elhárítás érdekében szükséges további intézkedéseket.

32. A csoport állandó tagja az Adatvédelmi tisztviselő, a szakterületi vezetők által delegált, adatkezelésben, adatvédelemben jártas további tagjai, akik a korábbi adatvédelmi felelősök voltak az Intézményben, valamint egy fő adminisztratív alkalmazott, akinek nincs szavazati joga, kizárólag a dokumentációk elkészítésében vesz részt. Az egyes adatvédelmi felelősök nem mind kerülnek a csoport tagjai közé automatikusan, azonban az egyes szakterületet érintően a csoport eseti jelleggel bevonhatja őket azon feladatok elvégzése során, ahol a saját szakterületük érintett.

33. Az 5 állandó tagból álló csoport vezetője az Adatvédelmi tisztviselő. A csoport vezetője hívja össze a csoportot, a csoport munkájáról kivonatos jegyzőkönyv készül. A csoport szótöbbséggel dönt. A csoport állandó tagjaként az adatvédelmi tisztviselőn kívül egy jogi végzettségű és az adatvédelem területén jártas személy, egy az informatikai adatvédelemhez értő személy, valamint az orvosi és ápolási szakma 1-1 képviselője tevékenykedik.

34. A csoport kinevezése mellett az Intézmény adatvédelmi tanácsadási feladattal egyéb, jogi vagy természetes személy szakértőt is megbízhat.

35. A csoport havonta egyszer ülésezik, incidens felmerülése esetén a csoport vezetője rendkívüli ülést hív össze.

36. Az adatvédelmi csoport összehangolja a Központi Kórház és a tagkórházak adatkezelési felelőseinek munkáját, szükség esetén az adatvédelmi csoport üléseire meghívja az ülésen tárgyalt témakörben érintett részlegek adatkezelési felelőseit.

5. ADATKEZELÉS BEVEZETÉSÉVEL, MÓDOSÍTÁSÁVAL ÉS MEGSZÜNTETÉSÉVEL KAPCSOLATOS FELADATOK

5.1. Adatkezelés bevezetésével kapcsolatos feladatok

37. Jogszabályban elrendelt vagy jogszabály rendelkezése miatt szükséges, vagy a Kórház döntése alapján létrehozandó nyilvántartási rendszer (a továbbiakban együtt: adatkezelés) bevezetése esetén, amennyiben az természetes személyek adatainak kezelésével (beleértve meglévő nyilvántartási rendszer adatainak új célú felhasználásával, új célú adatkezelés bevezetésével, nyilvántartási rendszerbe adatok felvételével, adatok tárolásával, harmadik személynek továbbításával stb.) jár, az adatkezelés bevezetése során e fejezet rendelkezéseit figyelembe véve kell alkalmazni.

38. Adatkezelés bevezetése főigazgatói utasítással történik. A főigazgatói utasítás tartalmazza
    a/ az adatkezelésért felelős szervezeti egységnek és egyéb szervezeti egységeknek az adatkezeléssel kapcsolatos feladatait, így különösen:
        aa/ az adatok felvételének, módosításának, törlésének rendje,
        ab/ adatszolgáltatási kötelezettségek meghatározása az adatok naprakészen tartása érdekében,
        ac/ a nyilvántartási rendszerből történő adattovábbítás, az ahhoz való hozzáférés rendje
    b/ mellékletként
        ba/ a GDPR-nak, az Infotv-nek és egyéb alkalmazandó jogszabálynak megfelelő adatkezelési tájékoztatót,
        bb/ hozzájáruláson alapuló adatkezelés esetén a hozzájáruló nyilatkozat mintáját.

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

40. Amennyiben az új adatkezelés bevezetése több szakterületet/szervezeti egységet érint, az adatkezelésért felelős valamennyi érintett szervezeti egység adatkezelési felelősét be kell vonni az adatkezelés feltételeinek kidolgozása folyamatába. Az Informatikai és Logisztikai Igazgatóság adatkezelési felelősét minden esetben be kell vonni a folyamatba. A fejlesztési igényt megfogalmazó szervezeti egység vezetője az egyéb területek adatkezelési felelősei bevonásának szükségességéről az érintett adatkezelési felelősöket és az adatvédelmi tisztviselőt értesíti.

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

42. Az adatkezelés bevezetésével, az adatkezelés feltételeinek meghatározásával kapcsolatban

a/ a leendő adatkezelésért annak tárgya szerint felelős szakterület/szervezeti egység adatkezelési felelőse (több érintett adatkezelési felelős egymással együttműködve):

aa/ meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, és ilyen tartalmú javaslatot készít a döntésre jogosultnak (GDPR 4. cikk 7. és 16. pont);

ab/ az aa/ alpontban meghatározott feladat részeként előterjesztést tesz a döntésre jogosultnak arról, hogy az eltérő célú adatkezelés összeegyeztethető-e az eredeti céllal, és így szolgálhat-e a tervezett adatkezelés új jogalapjául [GDPR 6. cikk (4) bek.];

ac/ az aa/ pontban meghatározott feladat részeként, amennyiben az adatkezelés jogalapja a jogos érdek lehet, elkészíti az érdekmérlegelési teszt dokumentumának tervezetét [GDPR 6. cikk (1) bek. f) pont];

ad/ az aa/ pontban meghatározott feladat részeként az adatvédelmi tisztviselő véleményének kikérése után javaslatot tesz a döntésre jogosultnak adatvédelmi hatásvizsgálat elvégzésére [60-71. pont]; a döntésre jogosult erre vonatkozó pozitív döntése esetén – az informatikai fejlesztéseket, az informatikai architektúra tervezést, illetve az IT üzemeltetést végző szervezeti egységnél működő adatkezelési felelős közreműködésével – elvégzi a hatásvizsgálatot, elkészíti ennek dokumentumát, és kikéri róla az adatvédelmi tisztviselő, valamint – ha alkalmazható – az érintettek vagy képviselőik véleményét [GDPR 35. cikk (1)-(2) és (9) bek.];

ae/ az aa/ pontban meghatározott feladat részeként előterjesztést tesz a döntésre jogosultnak arról, hogy az adatkezelést közös adatkezelésként indokolt-e ellátni, illetve indokolt-e adatfeldolgozót bevonni;

af/ az aa/ pontban meghatározott feladat részeként javaslatot tesz automatizált döntéshozatali módszer, illetve profilalkotási módszer alkalmazására [GDPR 22. cikk (1) bek.];

ag/ az aa/ pontban meghatározott feladat részeként megszövegezi a hozzájáruló nyilatkozatot [GDPR 7. cikk (2) bek.], illetve a megfelelő szerződéses rendelkezéseket;

ah/ megfogalmazza az adatkezelésről szóló tájékoztatást (GDPR 13-14. cikk);

ai/ az Informatikai és Logisztikai Igazgatóság közreműködésével gondoskodik az adatkezelésről szóló tájékoztatás könnyen hozzáférhető módon való közzétételéről [GDPR 12. cikk (1) bek.];

aj/ az adatkezelés bevezetéséről való döntést követően az Adatkezelési Nyilvántartásában rögzíti az új adatkezelést, illetve a nyilvántartott adatokban bekövetkezett valamennyi változást [GDPR 30. cikk (1) bek.]

ak/ amennyiben ennek szükségessége felmerül, egyedi esetben előterjesztést tesz a döntésre jogosultnak az érintett vagy harmadik személy létfontosságú érdeke fennállásáról [GDPR 6. cikk (1) bek. d) pont, 9. cikk (2) bek. d) pont] mint az adatkezelés lehetséges jogcíméről;

al/ amennyiben ennek szükségessége felmerül, egyedi esetben előterjesztést tesz a döntésre jogosultnak arról, hogy személyes adatok harmadik országba továbbíthatók-e egyedi ügyekben [GDPR 49. cikk (1) bek.];

b/ az informatikai fejlesztéseket, az informatikai architektúra tervezést, illetve az IT üzemeltetést végző szervezeti egységeknél működő adatkezelési felelősök – szervezeti egységük feladatkörében – a személyes adatot kezelő rendszer fejlesztése és beszerzése során közreműködnek

ba/ a célhoz kötött adatkezelés és az adattakarékosság elvének megfelelően gyűjtött adatokra vonatkozóan a beépített és alapértelmezett adatvédelem elveinek dokumentált érvényesüléséről;

bb/ annak biztosításában, hogy az adathordozhatóság, adattörlés és adattisztítás célú módosítások szabályozott és visszakereshető módon valósuljanak meg;

bc/ annak biztosításában, hogy az adatvédelmi tájékoztatók és nyilatkozatok könnyen elérhetők legyenek az ügyfelek számára,

bd/ annak biztosításában, hogy az adatkezeléssel kapcsolatos ügyfélrendelkezéseket visszakereshető formában tárolják;

be/ az adatok sértetlenségével, bizalmasságuk megőrzésével és üzletmenet-folytonossággal kapcsolatos kontrollok (pl. változáskezelés, magas rendelkezésre állás, jogosultságkezelés, adatrejtő eljárások, incidenskezelés támogatása) tervezéskori érvényesítésében, illetve dokumentált meglétében;

bf/ az aa/, ad/, ae/, af/, ah/ és al/ alpont szerinti döntések előkészítésében.

43. A 42. pont alkalmazása során döntésre jogosultnak minősül az személy, aki – a Kórház Szervezeti és Működési Szabályzata szerint – az érintett adatkezelés alapjául szolgáló tevékenységgel kapcsolatban döntésre jogosult, illetve – amennyiben a döntés testületi hatáskörbe tartozik – a testületi döntés előkészítéséért felelős.

44. A 42. pontban meghatározott döntések, javaslatok véglegesítése előtt ki kell kérni az adatvédelmi tisztviselő véleményét, úgy, hogy az adatvédelmi tisztviselőnek legalább 8 munkanapja legyen a vélemény adására.

45. Az adatvédelmi tisztviselő véleményének kikéréséhez olyan dokumentumot/leírást kell benyújtani, amely kellő részletességgel meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, illetve a 42. pontban meghatározott egyéb döntési javaslatokat.

46. Az adatvédelmi tisztviselő adatvédelmi jogi támogatást nyújt az adatkezelési felelős által előkészített, megszövegezett, adatkezeléshez kapcsolódó dokumentumok elkészítésében és közreműködik azok véglegesítésében.

    Az adatvédelmi tisztviselő
    a/ beszerzi az alábbi szervezeti egységek véleményét is:
        aa/ az adatvédelmi csoport és a Jogi Osztály véleményét a 42. pont aa/, ae/, af/, ag/, ah/ és al/ alpont tekintetében;
        ab/ az Informatikai és Logisztikai Igazgatóság véleményét a 42. pont aa/, ad/, ae/, af/, ah/ és al/ alpont tekintetében;
    b/ megvizsgálja a véleményezésre megküldött dokumentumot/leírást
        ba/ adatvédelmi jogi szempontból,
        bb/ abból a szempontból, hogy azok milyen módon illeszthetők be a Kórház informatikai rendszereibe, illetve nincs-e a tervezett adatkezeléssel azonos vagy hasonló adatkezelés.

47. A végleges dokumentumok szakmai megfelelőségéért a dokumentum létrehozását kezdeményező adatkezelési felelős, az adatvédelmi megfelelőségéért az adatvédelmi tisztviselő, az IT biztonsági megfelelőségért pedig az Informatikai és Logisztikai Igazgatóság a felelős. Abban az esetben, ha bármely terület eltér a megfogalmazott szakmai, adatvédelmi vagy információbiztonsági állásfoglalásoktól, az eltérésért, illetve a végleges dokumentumért az adatvédelmi tisztviselő vagy az információbiztonsági szakterület semmilyen felelősséggel nem tartozik.

48. A 46. pontban említett szervezeti egységek a véleményüket az adatvédelmi tisztviselőnek küldik meg az adatvédelmi tisztviselő által meghatározott határidőben, amely nem lehet kevesebb 5 munkanapnál. A véleményeket az adatvédelmi tisztviselő összesíti és véglegesíti, szükség esetén az adatkezelési felelősökkel és a véleményezőkkel való konzultáció után.

49. Amennyiben az adatkezelés feltételei kidolgozásában részt vevő adatkezelési felelősök között véleményeltérés van, illetve az adatvédelmi csoport, a Jogi Osztály vagy az Informatikai és Logisztikai Igazgatóság kifogást fogalmaz meg, az adatvédelmi tisztviselő – szükség esetén az adatkezelési felelősökkel és a véleményezőkkel való konzultáció után – javaslatot tesz a lehetséges megoldásra.

50. Az adatvédelmi tisztviselő véleményét az adatkezelés bevezetéséről való döntést kezdeményező előterjesztésben ismertetni kell. Az adatvédelmi tisztviselő véleményétől való eltérést az előterjesztésben részletesen meg kell indokolni.

5.2. Az adatkezelési felelős feladatai az adatkezelés során

51. Az adatkezelés során az adatkezelésért felelős szervezeti egység adatkezelési felelőse az adatkezelésért felelős szervezeti egység feladatkörébe tartozó kérdésekben:
    a/ képviseli az adatkezelőt az adatfeldolgozó felé vagy – közös adatkezelés esetén – a többi adatkezelő felé (amennyiben releváns);
    b/ figyelemmel kíséri az adatkezelés feltételeinek folyamatos fennállását (beleértve az adatkezelés jogszerűségéhez szükséges tájékoztatások megadását, nyilatkozatok beszerzését stb.) és szükség esetén megteszi vagy kezdeményezi a szükséges intézkedéseket az adatkezelés feltételeinek módosítása iránt;
    c/ amennyiben az adatkezelés hozzájáruláson alapul, megfelelő szabályozás kialakítása útján gondoskodik arról, hogy mindenkor igazolható legyen, hogy az érintett a hozzájárulását megadta [GDPR 7. cikk (1) bek.];
    d/ gondoskodik arról, hogy legalább az érintettel való első kapcsolatfelvételkor felhívják a figyelmét a tiltakozási jogra, és hogy az erről szóló tájékoztatást egyértelműen és más információtól elkülönítve jelenítsék meg [GDPR 21. cikk (4) bek.];
    e/ rendszeres időközönként, de legalább évente áttekinti a hatásvizsgálatban azonosított kockázatok alakulását, jelzi az adatvédelmi tisztviselőnek az adatkezeléssel járó kockázatok változását, közreműködik az adatvédelmi hatásvizsgálatok utóellenőrzésben [GDPR 35. cikk (11) bek.].

52. Az adatkezelés során (személyes adatok kezelési életciklusának üzemeltetési szakaszában) az Informatikai és Logisztikai Igazgatóságnál működő adatkezelési felelősök – a feladatkörükbe tartozó kérdésekben – gondoskodnak arról, hogy az adatkezelés általános adatbiztonsági kontrolljainak működtetése az erre vonatkozó eljárásrendeknek és az információbiztonsági szakterület által meghatározott elvárásoknak megfelelően történjék, ezen belül gondoskodva különösen
    a/ a fizikai és logikai hozzáférés-védelem kontrolljairól,
    b/ a rendkívüli esemény-kezelési eljárásokról (adatvédelmi incidensek feladatkörükbe tartozó kezelése, kedvezőtlen külső vagy belső behatásokkal szembeni ellenállási képesség biztosítása),

c/ jogosultságkezelésről és
d/ az adatminőséggel, illetve adatrejtéssel kapcsolatos intézkedések végrehajtásáról.

53. A 51. bekezdés b/ pont alá eső esetekben
a/ megfelelően alkalmazni kell a 38-50. pont rendelkezéseit,
b/ az adatkezelés megváltozott adatait – a változást elrendelő döntés után – át kell
c/ vezetni az Adatkezelési Nyilvántartásban.

5.3. Adatkezelés megszüntetésével kapcsolatos feladatok

54. Amennyiben a kezelt adatokra a továbbiakban nincs szükség (az adatkezelési cél megvalósult), vagy jogszabályi változások miatt, vagy az adatvédelmi felügyeleti hatóság vagy bíróság döntése értelmében az adatok kezelését meg kell szüntetni, az adatkezelési felelős – az adatvédelmi tisztviselő és rajta keresztül a [jogi ügyekért felelős szervezeti egység] és az Informatikai és Logisztikai Igazgatóság véleményének kikérése után – javaslatot tesz a döntésre jogosultnak:

a/ az adatkezelés egészének vagy egyes adatfajták nyilvántartásának megszüntetésére (az adatok archiválására az adattörlési idő leteltéig),
b/ nyilvántartási rendszer egészének vagy egyes adatfajták, illetve adatok törlésére.

55. A 54. pontban meghatározott esetben

a/ megfelelően alkalmazni kell a 38-50. pont rendelkezéseit,
b/ az Adatkezelési Nyilvántartásból az adatkezelést vagy az egyes adatfajtákat törölni kell,
c/ az adatokat – a 54. pont a/ és b/ pontjában tett megkülönböztetés szerint –
ca/ az informatikai rendszerekben archiválni kell, illetve
cb/ az informatikai rendszerekből törölni kell, a papír alapú nyilvántartásban kezelt adatokat pedig – a Kórház iratkezelési szabályzatáról szóló főigazgatói utasítás szerint – selejtezni kell.

5.4. Az érdekmérlegelési teszt elvégzésének módszertana

56. Amennyiben a Kórház valamely adatkezelésének a Kórház vagy harmadik személy jogos érdeke a jogalapja [GDPR 6. cikk (1) bekezdés f) pont], érdekmérlegelési tesztet kell elvégezni és azt dokumentálni. Jogos érdek az a törvényes, kellően pontosan megfogalmazott, valós és fennálló, illetve elérhető előny, amelyet az adatkezelő származtat – vagy a harmadik személy származtathat – az adatkezelésből.

57. Az érdekmérlegelési tesztet a tervezett adatkezelésért felelős szervezeti egység adatkezelési felelőse végzi el. Az érdekmérlegelési tesztet írásban kell elvégezni. Az elkészült dokumentumot – a 44-46. pont szerint – az adatvédelmi tisztviselőnek kell megküldeni, aki azt szakmai szempontból véleményezi. A jogos érdeken alapuló adatkezelés kizárólag az érdekmérlegelési teszt elvégzését és az adatvédelmi tisztviselő véleményének beszerzését követően kezdhető meg. A 50. pont rendelkezéseit jelen esetben is alkalmazni kell.

58. Az érdekmérlegelési teszt módszertanát, a megválaszolandó kérdéseket minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani, az alábbi kérdések köre csak orientáló, a tervezett adatkezelés szempontjából releváns egyéb kérdésekkel bővíthető. Abból kell kiindulni, hogy bármilyen adatkezelés beavatkozás az érintett magánszférájába és e beavatkozás jogosságát, szükségességét és arányosságát kell bizonyítani.

59. Az érdekmérlegelési teszt részei:

a/ a tervezett adatkezelés leírása és az annak keretében kezelni tervezett személyes adatok meghatározása.
b/ Az adatkezelő vagy azon harmadik fél jogos érdekének azonosítása, akinek az adatkezelés érdekében áll (Miért szükséges az adatkezelés?)
c/ Az érintett érdekeinek, jogainak azonosítása (Arányban van-e az adatkezelés az érintett magánszférájának korlátozásával?)
d/ az adatkezelő (vagy harmadik fél) és az érintettek érdekeinek összevetése:
e/ Biztosítékok leírása:
f/ Az érdekmérlegelési teszt eredménye

5.5. Az adatvédelmi hatásvizsgálat elvégzésének módszertana

60. Ha az adatkezelés valamely, különösen új technológiákat alkalmazó típusa valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve az adatkezelést megelőzően hatásvizsgálatot kell végezni. Olyan egymással hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló kockázatokat jelentenek, egyetlen adatvédelmi hatásvizsgálat (továbbiakban hatásvizsgálat) keretei között is értékelhetők.

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

62. A hatásvizsgálat elvégzését a tervezett adatkezelésért felelős szervezeti egység adatkezelési felelőse koordinálja a 42. pont ad/ alpontja szerinti módon. A hatásvizsgálat megállapításait írásban kell rögzíteni. Az elkészült hatásvizsgálati dokumentációt az adatvédelmi tisztviselőnek kell megküldeni, amely azt 8 munkanapon belül szakmai szempontból véleményezi és beszerzi az információbiztonsági szakterület véleményét is. Ha az adatkezelési felelős úgy ítéli meg, hogy az adatkezelés nem jár magas kockázattal, úgy meg kell indokolnia és dokumentumokkal igazolnia a mellőzés okait. A 50. pont rendelkezéseit jelen esetben is alkalmazni kell. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

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

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

65. A hatásvizsgálat módszertanát minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani. Egy lehetséges módszertant alkalmazó szoftver található a Nemzeti Adatvédelmi és Információszabadság Hatóság honlapján (**https://naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html**).

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

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

67. A hatásvizsgálat második részében ki kell fejteni és meg kell indokolni

    a/ az adatkezelés szükségességének és arányosságának garanciáit,
    b/ az érintett jogait biztosító garanciák érvényesülését.

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

69. A hatásvizsgálat negyedik része tartalmazza a tervezett adatkezelés értékelését:

a/ a 66-68. pontban meghatározott szempontok értékelését a tekintetben, hogy azok egyenként megfelelőek, további intézkedésekkel megfelelőek lehetnek, illetve nem megfelelőek;
b/ a tervezett kiegészítő intézkedések végrehajtásának ütemtervét;
c/ annak egyértelmű rögzítését, hogy a tervezett adatkezelés valószínűsíthetően magas kockázattal jár-e a természetes személyek jogaira nézve, és ennek alapján az adatkezelés megkezdhető-e, illetve szükség van-e az adatvédelmi felügyeleti hatósággal (NAIH) való konzultációra.

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

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

6. AZ ÉRINTETTŐL SZÁRMAZÓ KÉRELMEK, PANASZOK MEGVÁLASZOLÁSÁNAK RENDJE

6.1. Az adatvédelmi bejelentések típusai

72. Az érintettől a következő, személyes adatai [intézmény] általi kezelését érintő beadványok érkezhetnek:

a/ bejelentheti a Kórház által nyilvántartott adatok megváltozását;
b/ tájékoztatást kérhet személyes adatai [milyen személyes adato(ka)t milyen célból, milyen jogalapon, milyen forrásból szerezve meddig kezeli a Kórház, alkalmaz-e automatizált döntéshozatalt és/vagy profilalkotást az adatkezelés során, és a személyes adatokat kinek, milyen jogalapon továbbítja)] – hozzáféréshez való jog (GDPR 15. cikk);
c/ kérheti pontatlanul nyilvántartott személyes adatai helyesbítését, illetve vitathatja a nyilvántartott személyes adatok pontosságát – helyesbítéshez való jog (GDPR 16. cikk);
d/ kérheti nyilvántartott személyes adatai törlését – törléshez való jog (GDPR 17. cikk);

e/ kérheti személyes adatai kezelésének korlátozását (a pontatlan adat helyesbítéséig terjedő időre; a jogellenesen kezelt személyes adatok törlése helyett; jogszerűen kezelt, de szükségtelenné vált adatok törlése helyett az érintett kérésére az érintett jogi igényének előterjesztéséhez, érvényesítéséhez vagy védelméhez; jogos érdeken alapuló adatkezelés elleni tiltakozás elbírálásáig) – az adatkezelés korlátozásához való jog (GDPR 18. cikk);

f/ kérheti, hogy a rá vonatkozó, általa a Kórház rendelkezésére bocsátott és elektronikus adatbázisban kezelt adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja – adathordozhatósághoz való jog (GDPR 20. cikk);

g/ tiltakozhat személyes adatai kezelése ellen, ha az adatkezelés jogalapja az adatkezelő vagy harmadik személy jogos érdeke, illetve közérdekű feladat vagy közfeladat ellátása, beleértve mindkét esetben a profilalkotást is – tiltakozási jog gyakorlása (GDPR 21. cikk);

h/ automatizált döntéshozatal alkalmazása esetén az adatkezelő részéről emberi beavatkozást kérhet, közölheti álláspontját [GDPR 22. cikk (3) bek.];

i/ kifogást nyújthat be az automatizált döntéshozatal alkalmazásával meghozott döntéssel szemben [GDPR 22. cikk (3) bek.];

j/ panaszt nyújthat be a személyes adatok kezelését, illetve a GDPR szerinti jogaik gyakorlását érintően [GDPR 77. cikk, 38. cikk (4) bek.];

k/ az elhunyt érintett életében tett meghatalmazottjaként vagy közeli hozzátartozójaként gyakorolni kívánja az érintett egyes jogait [Infotv. 25. §].

6.2. Az adatvédelmi beadványok elintézése

73. Az egyes belső szabályzatoknak az érintettek adatainak felvételére, módosítására vagy helyesbítésére, illetve törlésére vonatkozó rendelkezései alkalmazását jelen szabályzat nem érinti, az adatvédelmi tisztviselő azonban bármely esetben – az érintett beadványának kivizsgálása, illetve saját ellenőrzése eredményeként, továbbá az adatvédelmi felügyeleti hatóság vagy bíróság döntése végrehajtásaként – az említett szabályzatokban meghatározott hatásköri és eljárási rendtől függetlenül kezdeményezheti személyes adat helyesbítését, törlését vagy az adatkezelés korlátozását (zárolást).

74. A Kórházhoz érkező, a 72. pontban meghatározott beadványokat a Kórház Panaszkezelési Szabályzatában foglaltaknak megfelelően kell – a GDPR 12. cikkében írt határidők figyelembevételével – elintézni, az alábbi kiegészítésekkel és eltérésekkel:

a/ a 72. pont j/ alpontban meghatározott panasz kivizsgálását az adatvédelmi tisztviselő végzi. A panasz kivizsgálása során az érintett szervezeti egységek kötelesek az adatvédelmi tisztviselővel együttműködni. A személyes adatok kezelését, illetve a GDPR szerinti jogok gyakorlását érintő panasz megalapozottsága esetén az adatvédelmi tisztviselő az adatkezelésért felelős szervezeti egység(ek)nél intézkedést kezdeményez a panasz kiváltó okainak orvoslására, az érintett folyamatok felülvizsgálatára, valamint – szükség esetén – a személyi felelősség megállapítására,

b/ az adatvédelmi tisztviselő dönt abban a kérdésben, hogy a 72. pontban meghatározott tárgyú beadvány egyértelműen megalapozatlan vagy túlzó-e,

c/ az érintettnek saját adatairól szóbeli tájékoztatás csak egyértelmű azonosítás után lehetséges, ellenkező esetben az ügyfelet írásbeli kérelem benyújtására kell megkérni,

d/ az ügyfélszolgálati tevékenységet ellátó szervezeti egység bármely beadvány esetén kérheti az adatvédelmi tisztviselő véleményét a tekintetben, hogy a beadvány a 72. pontban meghatározott tárgyú-e, illetve, hogy az érintett kérte-e az adatkezelés korlátozását [zárolás, GDPR 18. cikk – lsd. 72. pont e/ alpont], és kérés esetén az adatvédelmi tisztviselő intézkedik annak az informatikai rendszerekben történő megvalósításáról. Az adatkezelés korlátozásának (zárolásának) feloldásáról az adatvédelmi tisztviselő külön tájékoztatja az érintett informatikai rendszer(eke)t üzemeltető szervezet egység(ek)et,

e/ a Kórház szervezeti egységei a 72. pontban meghatározott tárgyú ügyekben készített válaszlevél-tervezetét jóváhagyás végett bemutatják az adatvédelmi tisztviselőnek.

75. Az egészségügyi dokumentációban a hibás egészségügyi adatot, az adatfelvételt követően úgy kell kijavítani vagy törölni, hogy az eredetileg felvett adat megállapítható legyen, a javítás ténye személyhez köthető legyen.

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

77. Adatot megsemmisíteni csak akkor lehet, ha:

a/ Jogszabályok által előírt kötelező tárolási idő letelt, és egyéb rendelkezés nem szól az adatok tárolásáról.

b/ Amennyiben párhuzamos adatnyilvántartás történt, és az adatok nyilvántartása egy helyen valósult meg, ebben az esetben a duplikáció elkerülése miatt törölhető az adat.

c/ A programban személyes adat csak addig törölhető, ameddig ahhoz betegellátás nem került rögzítésre. Egy beteghez rögzített- ténylegesen megtörtént ellátás nem törölhető.

78. Az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. tv. értelmében a beteg (érintett) jogosult az egészségügyi dokumentációba betekinteni, és arról - saját költségére - másolatot kérni. A beteg (érintett) halála esetén – törvényes képviselője, közeli hozzátartozója, valamint örököse jogosult a halál okával összefüggő vagy összefüggésbe hozható, továbbá a halál bekövetkezését megelőző gyógykezeléssel kapcsolatos egészségügyi adatokat – írásos kérelmére - megismerni, az egészségügyi dokumentációba betekinteni, valamint azokról – saját költségére – másolatot kapni.

A Kórházban a hivatalos szervek megkeresése esetén a dokumentáció kiadását a Jogi Osztály, Főigazgató, vagy Orvosigazgató előkészítése után az Orvosigazgató engedélyezi. A kórházban az állampolgárok által kért egészségügyi dokumentumok másolatának kiadását a Központi Iktató és Irattár előadói készítik elő, a kiadást az Orvosigazgató engedélyezi. A képalkotó diagnosztikai eljárás során készült felvételek esetén a Képalkotó Diagnosztikai Centrum kijelölt munkatársai végzik a képalkotó eljárás során készült felvétel másolatának kiadását. Mivel az egészségügyi dokumentáció részeként meg kell őrizni a beteg testéből kivett szövetmintákat, ezért a Kórház az érintett kezdeményezésére szövettani vizsgálati mintát csak indokolt esetben adhat ki. A kérés beérkezése után a szövettani anyag az archívumból kikeresés után a feladattal megbízott szakorvoshoz kerül szakmai véleményezés céljából.

79. Külső oktatási, kutatási, felsőoktatási intézményekkel kötött megállapodás alapján – szakdolgozat írása és egyéb kutatási célból – hallgatók, kutatók jogosultak a HIS rendszerhez történő hozzáféréshez, illetve – korlátozott módon – az ott található egészségügyi adatok megismeréséhez. Az Oktatási Csoport személyi azonosításra alkalmas kutatói jegyzéket állít össze a hallgatók (kutatók) részére, az általuk korábban megadott paraméterek alapján. A hallgatók (kutatók) a HIS rendszerben (MedWork's) névre szóló fiókot kap. A hallgatók (kutatók) HIS hozzáférése automatikusan határozott ideig, azaz kutató munkájának végéig tart.

7. AZ ADATBIZTONSÁGI INTÉZKEDÉSEK (TECHNIKAI ÉS SZERVEZÉSI INTÉZKEDÉSEK) MEGHATÁROZÁSA ÉS VÉGREHAJTÁSA

80. A Kórház működése során betartandó adatbiztonsági szabályokat (GDPR 32. cikk) külön szabályzatok tartalmazzák, így különösen a mindenkor hatályos
   a/ [információbiztonsági szabályzat],
   b/ [katasztrófa elhárítási és informatikai üzletmenet folytonossági szabályzat].

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

82. Az adatbiztonsági intézkedéseket érintően az adatkezelésért felelős szervezeti egység adatkezelési felelőse:
   a/ informatikai elemek védelmi osztályokba sorolásában;
   b/ a szakterületére vonatkozó információk szolgáltatásával közreműködik az adatkezelés biztonságát fenyegető kockázatok felmérésében és meghatározásában;
   c/ az informatikai rendszert üzemeltető szervezeti egységgel együttműködve közreműködik azon információbiztonságot érintő feladatok végrehajtásában, amelyek az adatbiztonsági követelmények megvalósulásához szükségesek;

d/ figyelemmel kíséri a belső adatvédelmi szabályok érvényre juttatását a szakterületen belül, felhívja a szakterületen dolgozók figyelmét a szabályok betartására, jelzi a szabályok megsértését az érintett munkavállaló felettesének, közreműködik a szakterületen dolgozók adatvédelmi tudatosságának növelésében.

83. Az adatbiztonság elveinek egy adatkezelés (lsd. 37. pont) bevezetésének vagy személyes adatkezelést és/vagy -feldolgozást eredményező módosításának előkészítése során történő érvényesítése az Informatikai és Logisztikai Igazgatóság adatkezelési felelőseinek feladata, akiket az adatkezelési tevékenységet támogató nyilvántartási rendszerek kifejlesztésének, módosításának folyamatába kötelezően be kell vonni (lsd. 40. pont).

84. Az adatbiztonsági intézkedések mindennapi működésben történő betartására a Kórház minden alkalmazottja, valamint a Kórház informatikai rendszereihez hozzáférő személy köteles.

8. A KÖZÖS ADATKEZELŐI ÉS AZ ADATFELDOLGOZÓI SZERZŐDÉSEK MEGKÖTÉSÉNEK ÉS VÉGREHAJTÁSA ELLENŐRZÉSÉNEK SZABÁLYAI

8.1. Közös adatkezelés

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

86. A közös adatkezelésről szóló megállapodásban meg kell határozni különösen
a/ az adatkezelés célját, a kezelendő adatok körét, az adatkezelés időtartamát, az alkalmazandó adatbiztonsági intézkedéseket, az adatkezelés egyéb feltételeit,
b/ azt, hogy a közös adatkezelésben érintett egyes adatkezelők
ba/ mely adatkezelési műveleteket (pl. hozzájáruló nyilatkozatok felvétele, adatok tárolása, adatok felhasználása stb.) végzik,
bb/ az érintett tájékoztatását hogyan végzik (pl. melyik adatkezelő készíti el az adatkezelési tájékoztatót és bocsátja az érintettek rendelkezésére stb.),
bc/ az érintett jogai gyakorlását hogyan biztosítják (pl. egyesített vagy elkülönített ügyfélszolgálat stb.),
bd/ az esetleges jogellenes adatkezelés következményeit milyen arányban viselik;
c/ az adatvédelmi incidens észlelése esetén követendő eljárást, különösen azt, hogy
ca/ az adatvédelmi incidens tudomásra jutása esetén a másik adatkezelő adatvédelmi tisztviselőjét (adatvédelmi tisztviselő hiányában a kijelölt kapcsolattartót) haladéktalanul kötelesek értesíteni az adatvédelmi rendellenességről vagy incidensről,
cb/ egymással kötelesek együttműködni az adatvédelmi rendellenesség vagy incidens okának kiderítésében és következményeinek felszámolásában,

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

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

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

87. A közös adatkezelés szükségességét az adatkezelési felelős az adatkezelés bevezetéséről való döntés előkészítése részeként [42. pont af/ alpont] vizsgálja meg.

88. Amennyiben döntés születik a közös adatkezelés bevezetéséről, az illetékes adatkezelési felelős(ök), az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő és egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a Jogi Osztály közreműködésével, továbbá az Informatikai és Logisztikai Igazgatóság véleményének kikérésével előkészíti a közös adatkezelésről szóló megállapodás tervezetét (benne a közös adatkezelőknek az érintettek számára kijelölendő kapcsolattartójának kijelölésével kapcsolatos döntést, valamint a közös adatkezelésre vonatkozó megállapodásnak az érintettek rendelkezésére bocsátható lényegi elemeit) és azt felterjeszti a szerződés megkötésére jogosult személynek.

89. A 88. pont alkalmazásában a szerződés megkötésére jogosult személy az, aki – a Kórház Szervezeti és Működési Szabályzata szerint – az érintett adatkezelés alapjául szolgáló tevékenységgel kapcsolatban döntésre jogosult, illetve – amennyiben a döntés testületi hatáskörbe tartozik – a testületi döntés előkészítéséért felelős. E szabály nem érinti az együttes aláírásra vonatkozó szabályokat.

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

8.2. Adatfeldolgozói szerződések

91. Adatfeldolgozó igénybevétele esetén az adatfeldolgozóval kötendő szerződésnek tartalmaznia kell a GDPR 28. cikk (1)-(4) bekezdésében foglalt tartalmi elemeket a 92. pontban foglalt kiegészítések és pontosítások szerint.

92. Az adatfeldolgozóval kötendő szerződésben

a/ a kellő részletességgel (pl. szabályzatra vagy szabványokra utalással) meg kell határozni az adatfeldolgozó, vagy az adatfeldolgozó által igénybe veendő további adatfeldolgozó (al-adatfeldolgozó) által betartandó adatbiztonsági szabályokat, amelyek nem lehetnek kevésbé szigorúak, mint a Kórház által alkalmazott adatbiztonsági intézkedések, és az adatfeldolgozónak az adatbiztonsági intézkedések végrehajtásával kapcsolatos feladatait;

b/ rögzíteni kell az adatfeldolgozónak az érintettől származó kérelmek, panaszok megválaszolásában való közreműködésének eljárásrendjét;
c/ rögzíteni kell az adatfeldolgozó kötelezettségeit adatvédelmi incidens észlelése esetén, így különösen
  ca/ az adatvédelmi incidens tudomásra jutása esetén a Kórház adatvédelmi tisztviselőjét haladéktalanul köteles értesíteni az adatvédelmi incidensről,
  cb/ köteles együttműködni a Kórház adatvédelmi tisztviselőjével és más közreműködő szervezeti egységgel az adatvédelmi incidens okának feltárásban és következményeinek felszámolásában,
  cc/ az adatvédelmi incidens bejelentésének teljesítésében,
d/ rögzíteni kell az adatfeldolgozó kötelezettségét az adatvédelmi hatásvizsgálat elvégzésében, illetve a hatásvizsgálatban azonosított kockázatok alakulásának figyelemmel kísérésében, az adatkezeléssel járó kockázatok változásának jelzésében, illetve az adatvédelmi hatásvizsgálatok utóellenőrzésben.

93. Az adatfeldolgozó igénybevételének szükségességét az adatkezelési felelős az adatkezelés bevezetéséről való döntés előkészítése részeként [42. pont af/ pont] vizsgálja meg. Ezt a szabályt kell alkalmazni akkor is, ha az adatfeldolgozó igénybevételéről az adatkezelés folyamán születik döntés.

94. Az adatbiztonsági intézkedések megfelelőségének megítélése az Informatikai és Logisztikai Igazgatóság hatáskörébe tartozik, beleértve azt is, hogy az adatfeldolgozó által egy magatartási kódexhez vagy tanúsítási mechanizmushoz való csatlakozás elegendő garanciát jelent-e az adatbiztonsági szabályok megfelelőségére.

95. Amennyiben döntés születik az adatfeldolgozó igénybevételéről, az adatkezelési felelős az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő és egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a Jogi Osztály közreműködésével, továbbá Informatikai és Logisztikai Igazgatóság véleményének kikérésével előkészíti az adatfeldolgozóval kötendő szerződés tervezetét és azt felterjeszti a szerződés megkötésére a 89. pont szerint jogosult személynek.

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

97. A 91.-96. pont rendelkezéseit al-adatfeldolgozó igénybevétele esetén is megfelelően alkalmazni kell azzal, hogy az al-adatfeldolgozó igénybevételére vonatkozó hozzájáruló nyilatkozatnak az adatfeldolgozói szerződés megkötésre jogosult személy általi kiadása előtt az adatkezelési felelős kikéri az adatvédelmi tisztviselő és rajta keresztül a Jogi Osztály, továbbá Informatikai és Logisztikai Igazgatóság véleményét is.

9. AZ ADATKEZELÉSI NYILVÁNTARTÁS

98. Az adatvédelmi tisztviselő feladatainak segítése keretében az adatvédelmi csoport vezeti az adatkezelési nyilvántartást (Adatkezelési Nyilvántartás).

Az adatkezelési nyilvántartás valamennyi, a Kórház általi adatkezelés esetén tartalmazza:

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

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

100. A Kórház adatvédelmi csoportja az Adatkezelési Nyilvántartásba való betekintést – a Hatóság képviselőin kívül – a Kórház érintett szakterületei részére biztosítja.

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

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

103. Az Adatkezelési Nyilvántartással összefüggésben az adatvédelmi tisztviselő:
   a/ ellenőrzi az adatkezelések, illetve adatfeldolgozás adatainak az Adatkezelési Nyilvántartásba történő rögzítését és jelzi az adatkezelésért felelős szervezeti egység vezetőjének a hiányos, hibás vagy valószínűleg megváltozott adatokat, információkat;
   b/ az adatvédelmi csoporttal, a Jogi Osztállyal együttműködve figyelemmel kíséri az adatkezelést érintő jogszabályok változását és a szükséges módosításokra felhívja az adatkezelési felelősök figyelmét;
   c/ az adatvédelmi felügyeleti hatóság megkeresésére adatot szolgáltat az Adatkezelési Nyilvántartásból.

10. AZ ADATVÉDELMI INCIDENSEK KEZELÉSE

10.1. Az adatvédelmi incidens

104. Adatvédelmi incidens csak akkor következik be, ha az adatbiztonsági intézkedések [7. fejezet] – akár vétlen, akár szándékos – megsértésének következtében bekövetkezik a személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés:
   a/ súlyos incidens: olyan incidens (pl. adatvesztés, adatsérülés), mely valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve (pl.: a jogosulatlan hozzáféréssel érintett adatok esete; az olyan adatsérülés, adatvesztés, amelynél az adatok naplózott állományból nem állíthatók helyre);
   b/ enyhe incidens: minden incidens, amely nem tartozik az a) pont alá (pl. átmeneti szolgáltatásleállás, -kiesés a Kórház munkavállalói által használt olyan belső rendszerekben, amely nem jár adatsérüléssel vagy adatvesztéssel).

105. Az adatvédelmi incidensre vonatkozó szabályokat kell alkalmazni a Kórház tulajdonát képező adathordozón, mobiltelefonon, laptopon, egyéb számítástechnikai eszközön tárolt adatokra, továbbá a Kórház alkalmazottainak olyan saját tulajdonú eszközein (adathordozó, mobiltelefon, laptop, egyéb számítástechnikai eszköz) tárolt adatokra, amely eszközöket munkavégzéshez, munkaköri feladatok ellátásához, hivatalos célból használhat. Az adatvédelmi incidensre vonatkozó szabályokat a Kórház birtokában lévő papíralapú adathordozón lévő adatokra is alkalmazni kell.

106. Az információbiztonsági incidens adatvédelmi incidensnek is minősül, amennyiben személyes adatokra nézve következik be.

10.2. Az adatvédelmi esemény bejelentése

107. Az a munkavállaló, aki a Kórház által kezelt vagy feldolgozott személyes adatokkal kapcsolatban, vagy a Kórház szerződéses partnere által kezelt vagy feldolgozott személyes adataival kapcsolatban adatvédelmi incidenst észlel, köteles azt haladéktalanul bejelenteni a **gdpr@bazmkorhaz.hu** e-mail címen. Az előbbieken túli egyéb bejelentő a Kórház elektronikus elérhetőségén jelentheti be az adatvédelmi incidenst.

108. Az adatvédelmi incidensről szóló bejelentésben ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát, továbbá bejelentő nevét és elérhetőségét.

109. A közös adatkezelésről szóló szerződésben [GDPR 26. cikk], illetve az adatfeldolgozóval kötendő szerződésben [GDPR 28. cikk] egyértelműen rendelkezni kell a másik adatkezelő, illetve az adatfeldolgozó azon kötelezettségéről, hogy az adatvédelmi incidensről a Kórház adatvédelmi tisztviselőjét köteles haladéktalanul, de legkésőbb az észlelést követő 24 órán belül értesíteni.

10.3. Incidensprotokoll általában

110. Az informatikai biztonságban résztvevők és szükség szerint az informatikai vagy szakmai rendszergazdák bevonásával a riasztásokban szereplő sérülékenység elhárításakor a következők szerint kell eljárniuk:
   a/ figyelembe kell venni a különböző informatikai biztonsági szabályozásokban a sérülékenységek elhárítására vonatkozó rendelkezéseket;
   b/ amennyiben a Kórház rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt azzal az eszközzel azonnal el kell kezdeni;
   c/ ha a Kórház – a mindenkor hatályos [információbiztonsági szabályzatában], továbbá a [katasztrófaelhárítási és informatikai üzletmenet folytonossági szabályzatában] foglaltakkal összhangban – nem rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt manuális módon kell azonnal elkezdeni;
   d/ amennyiben a sérülékenység elhárítása belső erőforrásból nem kivitelezhető, akkor külsős szakértőket kell bevonni az elhárítás folyamatába.

111. A nem papíralapon kezelt adattal kapcsolatos incidensek kezelésére a Kórház mindenkor hatályos információbiztonsági szabályzatában foglaltak is irányadók. A papíralapon kezelt iratokkal kapcsolatban a jelen Szabályzat hatálya alá tartozók kötelesek a személyes adatokat tartalmazó iratokat a munkavégzés befejezését követően, ahol ennek feltételei biztosítottak, zárható szekrényben, zárral ellátott fiókban tárolni. Ahol a tárolás előbb nevesített feltételei nem adottak, az irodahelyiség ajtajának kulcsra zárásával kell a személyes adatok védelmét biztosítani abban az esetben, ha az irodahelyiségben senki sem tartózkodik. A szabályzat hatálya alá tartozók kötelesek a Kórház egyéb belső szabályzatai, így különösen az iratkezelés rendjéről szóló mindenkor hatályos belső szabályzatnak megfelelően eljárni.

10.4. Az adatvédelmi incidens kivizsgálása

112. Adatvédelmi incidens (papíralapú és nem papíralapú adatokra vonatkozóak egyaránt) felmerülése esetén a Kórház adatvédelmi tisztviselője a Jogi Osztály és az Informatikai és Logisztikai Igazgatóság kijelölt munkatársának (a továbbiakban együtt: incidensvizsgáló bizottság) közreműködésével megvizsgálja, és a 104. pont szerint kategorizálja a bekövetkezett incidenst és meghatározza az esetleges elhárítás érdekében szükséges további intézkedéseket. Az említett személyeknek szükség esetén munkaidőn kívül is rendelkezésre kell állniuk.

113. Az adatvédelmi incidensről – szükség esetén – az adatvédelmi csoport értesíti a kórház főigazgatóját és a kórház adatvédelmi tisztviselőjét.

114. A bejelentés előzetes megvizsgálása során az alábbi szempontokat kell figyelembe venni:
   a/ a bejelentés személyes adatot érint-e,
   b/ amennyiben a bejelentés személyes adatot érint, megállapítható-e a személyes adatok köre,
   c/ megállapítható-e az incidensben érintett személyek köre,
   d/ a hatályos jogszabályok és belső szabályok alapján megállapítható-e, hogy személyes adat jogellenes kezelése vagy feldolgozása történt,
   e/ az incidens valószínűsíthetően magas kockázattal jár-e az érintettek jogaira és szabadságaira nézve,
   f/ melyek az adatvédelmi incidensből eredő, valószínűsíthető következmények,
   g/ a Kórház által alkalmazott technikai és szervezési védelmi intézkedések az incidensben érintett személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik-e az adatokat.

115. Az incidensvizsgáló bizottság legkésőbb az incidens bejelentés vagy az incidensről való tudomásszerzés közül a korábbi időpontot követő 1 napon belül tájékoztatja a következő személyeket az előzetes vizsgálat eredményéről, a GDPR 33. cikkében írt hatósági bejelentés szükségességéről, valamint arról, hogy szükséges-e az incidens részletes vizsgálata:

a/ a Kórház főigazgatóját;
b/ Jogi Osztály vezetőjét;
c/ informatikai rendszert is érintő incidens esetén az [informatikai biztonság ellátásáért felelős szervezeti egység] vezetőjét;
d/ a szakmailag illetékes szervezeti egység vezetőjét;
e/ az Adatvédelmi Csoport vezetőjét.

116. Az incidensvizsgáló bizottság javaslata alapján a főigazgató legkésőbb a bizottság javaslatának kézhezvételét követő 1 napon belül dönt a GDPR 33. cikkében írt hatósági bejelentés szükségességéről. A főigazgató döntéséről az adatvédelmi tisztviselő értesíti az illetékes vezetőt.

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

118. A vizsgálat során elsősorban az alábbi módszerek alkalmazhatóak:

a/ személyes megbeszélés az adatvédelmi incidensben érintett személyekkel, valamint az érintett szervezeti egységek munkatársaival és vezetőivel,
b/ írásbeli tájékoztatás kérése az érintett szervezeti egységektől,
c/ dokumentumok vizsgálata,
d/ informatikai rendszerek vizsgálata.

119. Amennyiben az incidensvizsgáló bizottság a részletes vizsgálat során úgy ítéli meg, hogy azonnali intézkedések szükségesek annak biztosítására, hogy az incidenssel azonos problémaforrásból eredő incidens a jövőben ne valósuljon meg, úgy a szükséges intézkedések megtétele érdekében haladéktalanul tájékoztatja az [érintett szervezeti egységek vezetőit].

120. Az incidensvizsgáló bizottság legkésőbb a vizsgálat megkezdését követő 15 munkanapon belül vizsgálati jelentést készít. A vizsgálati jelentés tartalmazza az adatvédelmi incidens elhárításához és további incidens megelőzéséhez szükséges intézkedésekre vonatkozó, az illetékes vezető részére tett javaslatot.

121. A jelentés alapján a vizsgálatban érintett szervezeti egységek vezetői 15 napon belül intézkedési tervet készítenek és megküldik az adatvédelmi tisztviselőnek.

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

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

10.5. Az érintett tájékoztatása a súlyos adatvédelmi incidensről

124. Súlyos adatvédelmi incidens esetén, amennyiben az valószínűsíthetően magas kockázattal jár, a Kórház indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

125. Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az alábbi információkat és intézkedéseket:
   a/ közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
   b/ ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
   c/ ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

126. Az érintettet nem kell tájékoztatni, amennyiben az incidens nem jár magas kockázattal, és a következő feltételek bármelyike teljesül:
   a/ a Kórház megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
   b/ a Kórház az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
   c/ a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

127. A Kórház főigazgatójának döntése alapján a Kórház az érintetteket a Kórház honlapján vagy országos lefedettségű sajtótermékben közzétett hirdetmény útján is értesítheti.

10.6. Az incidens bejelentése a Hatóságnak

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

129. A bejelentés összeállításának és beadásának felelőse az adatvédelmi tisztviselő.

130. Az adatvédelmi incidensről szóló bejelentésben legalább:
   a/ ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
   b/ közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
   c/ ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
   d/ ismertetni kell a Kórház által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

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

10.7. Az adatvédelmi incidensek nyilvántartása

132. Az adatvédelmi incidensekről az adatvédelmi csoport az adatvédelmi tisztviselő közreműködésével elektronikus nyilvántartást vezet.

133. A nyilvántartásban rögzíteni kell:
   a/ az incidensben érintett személyes adatok körét és számát,
   b/ az adatvédelmi incidenssel érintettek körét és számát,
   c/ az adatvédelmi incidens időpontját,
   d/ az adatvédelmi incidens körülményeit, hatásait,
   e/ az adatvédelmi incidens elhárítására megtett intézkedéseket,
   f/ az adatvédelmi incidenssel kapcsolatban adott tájékoztatások adatait.

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

11. HARMADIK ORSZÁGBA IRÁNYULÓ ADATTOVÁBBÍTÁS KÜLÖNÖS SZABÁLYAI

135. Amennyiben személyes adatnak harmadik országba történő továbbításának szükségessége merül fel, az érintett szervezeti egység köteles az adatvédelmi tisztviselő véleményét kérni az adattovábbítás megengedhetőségéről, illetve az adattovábbítás lehetséges módjáról.

136. Az adatvédelmi tisztviselő – szükség esetén a Jogi Osztály és az Informatikai és Logisztikai Igazgatóság véleményének kikérése után – javaslatot tesz az adattovábbítás módjára, az adatátadás során alkalmazandó biztosítékok körére.

12. BELSŐ ADATVÉDELMI ELLENŐRZÉSI ELJÁRÁS

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

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

139. Az éves ellenőrzési tervet a Kórház főigazgatója hagyja jóvá.

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

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

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

143. Az adatvédelmi tisztviselő a lefolytatott ellenőrzésről vizsgálati jelentést készít, melynek mellékletét képezi az ellenőrzésről készült jegyzőkönyv. A vizsgálati jelentés tartalmazza az adott szervezeti egységnél vizsgált körülményeket, adatokat, megállapításokat. A vizsgálati jelentés tervezetére a szervezeti egység vezetője 10 napon belül észrevételt tehet. Az észrevételezés elmaradása a szervezeti egység vezetőjének egyetértését jelenti.

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

145. Az adatvédelmi tisztviselő rendkívüli ellenőrzést is lefolytathat, ha adatvédelmi szempontból az indokolt, különösen, ha a személyes adatkezeléssel érintettek száma jelentős. Rendkívüli ellenőrzésnek minősül az éves ellenőrzési tervben nem szereplő ellenőrzés. A rendkívüli ellenőrzést a Kórház főigazgatója előzetesen engedélyezi.

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

13. ZÁRÓ RENDELKEZÉSEK

147. Jelen szabályzat az aláírást követő napon lép hatályba. Ezzel egyidejűleg hatályát veszti az e tárgyban 2017. 12.15-én kiadott szabályzat.

14. MELLÉKLETEK, ADATLAPOK JEGYZÉKE

Minőségügyi kód	Cím	Az oldal változatszáma
Melléklet		
FISZ-006-2/M01	Az egészségügyi dokumentáció megismerésének, illetve kiadásának folyamata	**1**
Adatlap		
FISZ-006-2/A01	Beleegyező nyilatkozat fénykép, videó- és hangfelvétel készítésébe (MedWork's azonosító: E-MK 2002-74/19)	**1**
FISZ-006-2/A02	Meghatalmazás (E-MK 2001-112/19)	**1**
FISZ-006-2/A03a	Egészségügyi dokumentáció kikérő lap –Magyar Nyelvű (E-MK 2017-139/19)	**1**
FISZ-006-2/A03b	Egészségügyi dokumentáció kikérő lap –Angol Nyelvű (E-MK 2017-139/19)	**1**
FISZ-006-2/A04	Egészségügyi dokumentáció kérése további gyógykezelés céljából (E-MK 2003-35/19)	**1**
FISZ-006-2/A05	Nyilatkozat képalkotó diagnosztikus eljárás során készült felvétel kiadásához (E-MK 2001-110/19)	**1**
FISZ-006-2/A06	Látlelet kérő lap (MedWork's azonosító: E-MK 2002-59/19)	**1**
FISZ-006-2/A07	Képalkotó diagnosztikai eljárással készült egészségügyi dokumentáció másolatának kérése (E-MK 2016-23/19)	**1**
FISZ-006-2/A08	Képalkotó diagnosztikai eljárással készült egészségügyi dokumentáció másolatának kérése további gyógykezelés céljából (E-MK 2016-24/19)	**1**
FISZ-006-2/A09	Megbízólevél osztályos adatvédelmi megbízott részére	**1**