Iktató szám: ALT / 921-1 / 2021

Mátrai Gyógyintézet

Adatkezelési szabályzat

Felelős:	*Jóváhagyta:*	*Ellenjegyezte:*
adatvédelmi tisztviselő	főigazgató főorvos	gazdasági igazgató

MÁTRAI GYÓGYINTÉZET * Mátrháza * főigazgató

Dátum: 2021. május 25.

Módosítások		
Kiadása	Hatályba lépés dátuma	Formája
1.	2004. 03. 10.	Bevezetés
2.	2005. 09. 15.	Módosítás
3.	2006. 07. 01.	Névváltozás miatti aktualizálás
4.	2007. 08. 01.	Logó- és jogszabályváltozás
5.	2018. 05. 25.	Jogszabály változás
6.	2021. 05. 26.	Jogszabály változás

Tartalomjegyzék

1. A SZABÁLYZAT CÉLJA, HATÁLYA, ALAPELVEK, ALAPFOGALMAK

1.1. Bevezető rendelkezések

1. A Mátrai Gyógyintézet (a továbbiakban: Intézet) 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.

2. A Szabályzat hatálya alá tartozó személyek kötelesek a tevékenységük során az Intézet 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, valamint az Intézetre irányadó egyéb jogszabályok rendelkezései szerint kezelni. Az Intézet 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 az Intézet 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 3. fejezetében 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 az Intézet tevékenysége során a személyes adatok védelméhez fűződő jog érvényesülését, továbbá, hogy az Intézet által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes és különleges adatok kezelése során irányadó adatvédelmi szabályokat.

5. A Szabályzat célja továbbá, hogy meghatározza azokat a szervezési és technikai intézkedéseket, amelyek kialakításával az Intézet gondoskodik a személyes adatok kezelése során a személyes adatok biztonságáról. Erre tekintettel a Szabályzat az Intézet 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 az Intézet 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 az Intézet irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek (a munkavégzésre irányuló jogviszony jellegétől függetlenül), 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. Az Intézet megbízásából személyes adatok kezelését vagy feldolgozását végzők esetén az erre a jogviszonyra az Intézet által kötött szerződésben a GDPR 28. cikkének megfelelően rendelkezni kell arról, hogy az Intézet által megbízott adatfeldolgozó a feladata ellátása során hogyan juttatja érvényre jelen Szabályzat rendelkezéseit.

1.4. A szabályzat tárgyi hatálya

8. A Szabályzat tárgyi hatálya az Intézet 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 (az Intézménnyel kapcsolatba lépni szándékozó, kapcsolatban álló vagy kapcsolatban állt személyek, beleértve ezek meghatalmazottait, képviselőit is);

a/ foglalkoztatási jogviszonyhoz kapcsolódó adatkezelést valósítanak meg [az Intézménnyel közalkalmazotti jogviszonyban, munkaviszonyban vagy egyéb foglalkoztatási jogviszonyban (együtt: foglalkoztatási jogviszony) álló, állt, vagy foglalkoztatási jogviszonyba lépni szándékozó személyek);

b/ az Intézménnyel szerződéses kapcsolatban álló társaságok képviselőinek, kapcsolattartóinak az adataira vonatkoznak.

1.5. Dokumentálási kötelezettség

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

10. A megfelelőség igazolása adatvédelmi incidens esetén különösen az incidenssel érintettek körének, az incidenssel érintett személyes adatok körének, az incidens kezelése során tett intézkedéseket megalapozó körülmények és a döntések dokumentálásával történik. Az Intézet

– a GDPR 33. cikkének megfelelően – nyilvántartást vezet a bekövetkezett incidensekkel kapcsolatos tényekről és intézkedésekről.

2. ALAPFOGALMAK

11. 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/ adatbiztonság: a személyes adatok jogosulatlan kezelése, így különösen jogosulatlan megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások, valamint eljárási szabályok összessége; az adatkezelés azon állapota, amelyben az adatok sérülésének, illetéktelen felhasználásának, megsemmisülésének kockázati tényezőit – és ezáltal a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a minimálisra csökkentik,

b/ Adatkezelési Nyilvántartás: jelen utasítás 10. fejezetében meghatározott adattartalmú, folyamatosan karbantartott nyilvántartás;

c/ adatkezelésért felelős szervezeti egység: az Intézet azon szervezeti egysége, amelynek feladatkörébe tartozik az Intézet kezelésében lévő valamely nyilvántartási rendszer létrehozása, fenntartása, illetve üzemeltetése,

d/ adatvédelmi felügyeleti hatóság: a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság),

e/ adatvédelmi hatásvizsgálat: olyan vizsgálat, amelyet az adatkezelésért felelős szervezeti egység kijelölt munkavállalója (adatkezelési megbízott) köteles elvégezni, amennyiben valamely tervezett adatkezelés – figyelemmel annak jellegére, hatókörére, körülményeire és céljaira, ideértve különösen az új technológiák alkalmazásának esetét – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, 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,

f/ adatvédelmi incidens jellege: személyes adatok megsemmisülése, személyes adatok jogosulatlan megsemmisítése, személyes adatok rendelkezésre állásának sérülése, személyes adatok integritásának sérülése, személyes adatok elvesztése, személyes adatok jogosulatlan megváltoztatása, személyes adatok jogosulatlan közlése vagy jogellenes továbbítása, személyes adatokhoz történő jogosulatlan hozzáférés, személyes adatok bizalmasságának sérülése (pl. titoksértés) stb.

g/ adatkezelési megbízott: az adatkezelésért felelős szervezeti egység azon, e feladatkör ellátására kijelölt munkavállalója, aki a jelen utasításban, illetve az adatkezelést szabályozó

más belső szabályozó dokumentumokban meghatározottak szerint az adatkezelésért felelős szervezeti egység felelősségi körébe tartozó adatkezelések tekintetében, vagy adatkezeléseknek az adatkezelésért felelős szervezeti egység felelősségi körébe tartozó részében gondoskodik az adatkezelőt terhelő feladatok elvégzéséről,

h/ adatvédelmi tisztviselő: az Intézet szervezetében működő, a GDPR 39. cikkében meghatározott feladatokat az Intézet jelen szabályzatában foglaltak szerint ellátó, az Intézettel foglalkoztatási jogviszonyban álló természetes személy,

i/ 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,

j/ 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,

k/ dolgozói személyes adat: az Intézménnyel foglalkoztatási jogviszonyban álló személyek adata,

l/ 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,

m/ informatikai szakterület: az informatikai rendszerek üzemeltetéséért, az informatikai biztonság ellátásáért felelős szervezeti egység vagy egységek, ideértve az Intézet információbiztonsági felelősét is,

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

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

p/ ügyvitel: az Intézet tevékenységére vonatkozó jogszabályokban az Intézet 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 végrehajtására kiadott 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
	az Intézet Közzétételi Szabályzata
	az Intézet Informatikai Biztonsági Szabályzata
	Intézet Iratkezelési Szabályzata
	az Intézet szervezeti egységei által kezelt nyilvántartási rendszereket szabályozó utasítások
	az Intézet Betegellátási Szabályzata
	az Intézet Belső Kontrollrendszerek Szabályzata
	az Intézet Adatvédelmi és Informatikai incidens kezelési szabályzata

4. AZ ADATVÉDELMI TEVÉKENYSÉG SZERVEZETE ÉS IRÁNYÍTÁSA AZ INTÉZETNÉL

4.1. Az adatvédelmi tevékenység ellátásában résztvevők

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

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

a/ gondoskodik az adatvédelmi tevékenység irányításában és ellátásában résztvevő szervezeti egységek kijelöléséről, feladataik, az adatvédelmi tárgyú ügyekkel kapcsolatos döntési jogkörök meghatározásáról, az egyes adatkezelési döntési szintek kialakításáról;

b/ biztosítja az adatvédelmi tevékenység irányításához és ellátásához, valamint az érintett jogai gyakorlásához szükséges személyi és tárgyi feltételeket, beleértve az adatvédelmi tisztviselő feladatainak ellátásához szükséges személyi és tárgyi feltételeket;

c/ felelős az adat- és titokvédelmi, valamint biztonsági és informatikai biztonsági szabályzatok kiadásáért és betartatásáért;

d/ biztosítja, hogy az adatvédelmi tisztviselő véleményét kikérjék az Intézet adatvédelmi tárgyú vagy adatvédelmi vonatkozású belső szabályzatainak előkészítése során;

e/ gondoskodik arról, hogy az adatvédelmi tevékenység során esetleg előforduló, feltárt hiányosságok megszűntetéséről, szükség szerint a felelősségre vonásról;

f/ kinevezi az Intézet adatvédelmi tisztviselőjét, és az adatvédelmi tisztviselő nevét és elérhetőségét bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak;

g/ munkajogi értelemben vett közvetlen felettese az adatvédelmi tisztviselőnek.

14. Az Intézet szervezeti egységeinek vezetői az irányításuk alá tartozó szervezeti egység tekintetében:

a/ betartják és betartatják az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírásokat; az adatvédelmi tisztviselővel, a jogtanácsossal, valamint a Számítástechnika és Informatikai Csoporttal együttműködve gondoskodnak az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról;

b/ amennyiben indokolt, kijelölik az irányításuk alá tartozó szervezeti egység adatkezelési megbízottját;

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 megbízott előterjesztésére – az Intézet döntéselőkészítésre vonatkozó szabályainak megfelelően – döntenek a jelen utasításban, illetve az adatkezeléssel járó folyamatot szabályozó egyéb belső szabályzatokban a feladat- és hatáskörébe utalt kérdésekben.

15. A Humánpolitikai osztály vezetője

a/ adatvédelmi incidens esetén közreműködik az érintettek tájékoztatásának módjáról és a tájékoztatás tartalmáról való döntés előkészítésében,

b/ adatvédelmi incidens esetén – az adatvédelmi tisztviselő közreműködésével, az Intézet sajtónyilatkozatai kiadására vonatkozó szabályok sérelme nélkül - szükség esetén sajtóközleményt bocsát ki és kizárólagos kapcsolatot tart a sajtó képviselőivel.

16. Az Intézet Szervezeti és Működési Szabályzata szerinti hatásköri szabályok szerint a Titkárság vezetője, az Orvos igazgató és az Ápolási igazgató az érintett szervezeti egységekkel együttműködve:

a/ az adatvédelmi tisztviselő szükség szerinti közreműködésével ellátja az érintetti jogok gyakorlásával kapcsolatos beadványok megválaszolását (78. pont) a személyes adatok kezelését, illetve a GDPR szerinti jogaik gyakorlását érintő panaszok (78. pont j/ alpont) kivételével.

17. A Számítástechnika és Informatikai Csoport az Intézet szervezeti és működési szabályzatában, valamint az Intézet Informatikai biztonsági szabályzatában meghatározott feladatkörükben:

a/ ellátják az informatikai biztonsági biztonsággal kapcsolatos feladatokat a folyamatos üzemeltetési feladatok kivételével, különösen az Intézet Informatikai biztonsági szabályzatáról szóló főigazgatói utasításban meghatározott feladatokat;

b/ ellátják az informatikai fejlesztéseknél és beszerzéseknél a beépített adatvédelem kontrolljai meglétének biztosításával, az adatminőség biztosításával, az informatikai biztonság kockázatarányos szintjét biztosító jogosultsági és naplózási rendszer kialakításának megfelelőségével, a biztonságos szoftverfejlesztés alapelveinek érvényesítésével kapcsolatos feladatokat,

c/ az informatikai rendszerek üzemeltetése területén ellátják a személyes adatok kezelésével kapcsolatos technikai védelem megvalósítását, ellátják – az Intézet Informatikai biztonsági szabályzatáról szóló mindenkor hatályos főigazgatói utasításban meghatározott – hatáskörükbe tartozó információbiztonsági feladatokat, valamint rendelkezésre állási kontrollok biztosítását, a tárolt és továbbított személyes adatok bizalmasságának védelmét, az incidensfelderítési és -kezelési tevékenység támogatását,

d/ az érintett szervezeti egységek vezetőivel együttműködve gondoskodnak az információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról.

18. A jogtanácsos:

a/ szakmai támogatást nyújt az adatkezeléssel összefüggő, nem adatvédelmi jogszabályok értelmezésében,

b/ biztosítja az Intézet képviseletét az érintett által az Intézet ellen az érintett adatvédelmi jogainak megsértése miatt indított, illetve az Intézet által a Nemzeti Adatvédelmi és Információszabadság Hatóság határozatainak felülvizsgálata iránt indított perekben, illetve egyéb eljárásokban.

19. Az adatkezelési megbízott a felelősségi körébe tartozó szervezeti egység(ek) 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 Adatkezelés Nyilvántartás naprakészen tartásához szükséges információk átadása az adatvédelmi tisztviselő részére stb.), illetve abban közreműködik;

c/ együttműködik az ugyanazon adatkezelésben érintett más adatkezelési megbízottakkal;

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 az Intézet kezelésében lévő az adatok biztonsági osztályba sorolásában.

20. Adatkezelési megbízottat valamennyi igazgatóság szintű szervezeti egységnél, valamint a Számítástechnika és Informatikai Csoportnál ki kell jelölni. Adatkezelési megbízottnak olyan személyt kell kijelölni, aki az adott szakterületet, üzleti/adminisztratív folyamato(ka)t, illetve – Számítástechnika és Informatikai Csoportnál – a szakterületek tevékenységét támogató informatikai rendszereket illetően kellő ismeretekkel bír.

4.2. <u>Az adatvédelmi tisztviselő</u>

21. Az adatvédelmi tisztviselőt a főigazgató főorvos nevezi ki az olyan, az Intézménnyel foglalkoztatási jogviszonyban álló természetes személyek közül, aki ismeri az Intézet működését, feladatait, munkafolyamatait és rendelkezik:

a/ felsőfokú végzettséggel;

b/ az európai és hazai adatvédelemmel kapcsolatos főbb szabályozók, hatósági és bírósági határozatok, iránymutatások ismeretével;

c/ alapvető adatvédelmi és informatikai folyamatok ismeretével;

22. Az adatvédelmi tisztviselő kinevezése mellett az Intézet adatvédelmi tanácsadási feladattal egyéb, jogi vagy természetes személy szakértőt is megbízhat.

23. 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 főigazgató főorvosnak tartozik felelősséggel.

24. Az Intézet elősegíti az adatvédelmi tisztviselő megfelelő szakmai feladatellátását, ennek érdekében az Intézet 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, amellyel az adatvédelmi tisztviselő – a jogtanácsos és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – tartja a kapcsolatot.

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

26. 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.

27. Az Intézetben nem lehet adatvédelmi tisztviselő az a természetes személy, aki az Intézetben az adatkezelési tevékenység céljainak, kereteinek, eszközeinek meghatározásáról dönt, különösen a főigazgató főorvos, adatkezelésért felelős szervezeti egység vezetője (11.c/ pont) és a belső ellenőr.

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

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

30. 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 az Intézet egyéb belső szabályzatai rendelkezéseinek a megtartását, belső adatvédelmi ellenőrzési eljárást folytat le;

c/ kivizsgálja – az érintett szakterületek és a jogtanácsos bevonásával – a neki címzett panaszokat, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;

d/ a jogtanácsossal és a Számítástechnika és Informatikai Csoporttal együttműködve elkészíti az adatvédelmi és adatbiztonsági szabályzatot;

e/ a jogtanácsossal együttműködve gondoskodik az adatvédelmi ismeretek oktatásáról [elsősorban az intraneten közzétett segédanyagok útján];

f/ a jogtanácsossal 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 hatásvizsgálatot lefolytatásában;

h/ az adatvédelmi incidenskezeléssel kapcsolatban ellátja a jelen szabályzat szerinti feladatokat;

i/ vezeti az Adatkezelési Nyilvántartást (10. fejezet);

j/ éves összefoglaló jelentést készít a főigazgató főorvosnak;

k/ kapcsolatot tart és – jogtanácsos és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – együttműködik a Hatósággal;

l/ az Állami Egészségügyi Ellátó Központ számára adatszolgáltatást teljesít.

5. ADATKEZELÉS BEVEZETÉSÉVEL, MÓDOSÍTÁSÁVAL ÉS MEGSZÜNTETÉSÉVEL KAPCSOLATOS FELADATOK

5.1. Adatkezelés bevezetésével kapcsolatos feladatok

31. Jogszabályban elrendelt vagy jogszabály rendelkezése miatt szükséges, vagy az Intézet 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 az Intézet Szervezeti és Működési Szabályzatát, illetve az Ellenőrzési nyomvonalak szabályzatát e fejezet rendelkezéseit figyelembe véve kell alkalmazni.

32. 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:

a.a/ az adatok felvételének, módosításának, törlésének rendje,

a.b/ adatszolgáltatási kötelezettségek meghatározása az adatok naprakészen tartása érdekében,

a.c/ a nyilvántartási rendszerből történő adattovábbítás, az ahhoz való hozzáférés rendje;

b/ - az adatkezelésre vonatkozó különös adatbiztonsági intézkedések meghatározása;

c/ mellékletként

c.a/ a GDPR-nak, az Infotv-nek és egyéb alkalmazandó jogszabálynak megfelelő adatkezelési tájékoztatót,
c.b/ hozzájáruláson alapuló adatkezelés esetén a hozzájáruló nyilatkozat mintáját.

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

34. Amennyiben az új adatkezelés bevezetése több szakterületet/szervezeti egységet érint, az adatkezelésért felelős valamennyi érintett szervezeti egység adatkezelési megbízottját be kell vonni az adatkezelés feltételeinek kidolgozása folyamatába. A Számítástechnika és Informatikai Csoport adatkezelési megbízottját/megbízottjait minden esetben be kell vonni a folyamatba. A fejlesztési igényt megfogalmazó szervezeti egység vezetője az egyéb területek adatkezelési megbízottjai bevonásának szükségességéről az érintett adatkezelési megbízottakat és az adatvédelmi tisztviselőt értesíti.

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

36. Az adatkezelés bevezetésével, az adatkezelés feltételeinek meghatározásával kapcsolatban

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

a.a/ 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);

a.b/ az a.a/ 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.];

a.c/ az a.a/ 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];

a.d/ az a.a/ pontban meghatározott feladat részeként az adatvédelmi tisztviselő véleményének kikérése után javaslatot tesz a döntésre jogosultnak adatvédelmi hatásvizsgálat elvégzésére [54-65. 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 megbízott 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.];

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

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

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

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

a.i/ a Számítástechnika és Informatikai Csoport közreműködésével gondoskodik az adatkezelésről szóló tájékoztatás könnyen hozzáférhető módon való közzétételéről [GDPR 12. cikk (1) bek.];

a.j/ az adatkezelés bevezetéséről való döntést követően megküldi az adatvédelmi tisztviselőnek az új adatkezelésnek az Adatkezelési Nyilvántartásban történő rögzítéséhez szükséges információkat, illetve a nyilvántartott adatokban bekövetkezett valamennyi változást [GDPR 30. cikk (1) bek.], új tevékenység esetén legalább az adatkezelési tevékenység megkezdését megelőző 15 nappal, változás esetén 8 nappal korábban;

a.k/ 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;

a.l/ amennyiben ennek szükségessége felmerül, a 12. fejezet szabályait is figyelembe véve egyedi esetben előterjesztést tesz a döntésre jogosultnak arról, hogy személyes adatok harmadik országba továbbíthatók-e egyedi ügyekben [GDPR 49. cikk (1) bek.];

b/ a Számítástechnika és Informatikai Csoport adatkezelési megbízottjai – szervezeti egységük feladatkörében – a személyes adatot kezelő rendszer fejlesztése és beszerzése során közreműködnek

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

b.b/ annak biztosításában, hogy az adathordozhatóság, adattörlés és adattisztítás célú módosítások szabályozott és dokumentált módon valósuljanak meg;

b.c/ annak biztosításában, hogy az adatvédelmi tájékoztatók és nyilatkozatok könnyen elérhetők legyenek az ügyfelek számára,

b.d/ annak biztosításában, hogy az adatkezeléssel kapcsolatos ügyfélrendelkezéseket visszakereshető formában tárolják;

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

b.f/ az adott adatkezelés különös (az Intézet Informatikai biztonsági szabályzatától eltérő) adatbiztonsági intézkedések meghatározásában;

b.g/ az a.a/, a.d/, a.e/, a.f/, a.h/ és a.l/ alpont szerinti döntések előkészítésében.

37. A 36. pont alkalmazása során döntésre jogosultnak minősül az személy, aki – az Intézet 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.

38. A 36. pontban meghatározott döntések, javaslatok véglegesítése előtt ki kell kérni az adatvédelmi tisztviselő véleményét, úgy, hogy az adatvédelmi tisztviselőnek legalább 10 munkanapja legyen a vélemény adására.

39. 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 36. pontban meghatározott egyéb döntési javaslatokat.

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

a/ beszerzi az alábbi szervezeti egységek véleményét is:

a.a/ a jogtanácsos véleményét a 36. pont a.a/, a.e/, a.f/, a.g/, a.h/ és a.l/ alpont tekintetében;

a.b/ a Számítástechnika és Informatikai Csoport véleményét a 36. pont a.a/, a.d/, a.e/, a.f/, a.h/ és a.l/ alpont tekintetében;

b/ megvizsgálja a véleményezésre megküldött dokumentumot/leírást

b.a/ adatvédelmi jogi szempontból,

b.b/ abból a szempontból, hogy azok milyen módon illeszthetők be az Intézet informatikai rendszereibe, illetve nincs-e a tervezett adatkezeléssel azonos vagy hasonló adatkezelés.

41. A végleges dokumentumok szakmai megfelelőségéért a dokumentum létrehozását kezdeményező adatkezelési megbízott, az adatvédelmi megfelelőségéért az adatvédelmi tisztviselő, az informatikai, információbiztonsági megfelelőségért pedig a Számítástechnika és Informatikai Csoport 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.

42. A 40. 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 megbízottakkal és a véleményezőkkel való konzultáció után.

43. Amennyiben az adatkezelés feltételei kidolgozásában részt vevő adatkezelési megbízottak között véleményeltérés van, illetve a jogtanácsos vagy a Számítástechnika és Informatikai Csoport kifogást fogalmaz meg, az adatvédelmi tisztviselő – szükség esetén az adatkezelési megbízottakkal és a véleményezőkkel való konzultáció után – javaslatot tesz a lehetséges megoldásra.

44. 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. <u>Az adatkezelési megbízott feladatai az adatkezelés során</u>

45. Az adatkezelés során az adatkezelésért felelős szervezeti egység adatkezelési megbízottja 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, ellenőrzi, hogy az érintett a hozzájárulását szabályosan szerezték-e be [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.].

46. Az adatkezelés során (informatikai rendszerben kezelt adatok esetén az informatikai rendszer üzemeltetési szakaszában) a Számítástechnika és Informatikai Csoport adatkezelési megbízottja(i) – a feladatkörükbe tartozó kérdésekben – gondoskodnak arról, hogy az adatkezelés általános adatbiztonsági kontrolljainak működtetése az erre vonatkozó eljárásrendeknek és a Számítástechnika és Informatikai Csoport 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.

47. A 45. pont b/ alpont alá eső esetekben

a/ megfelelően alkalmazni kell a 32-44. pont rendelkezéseit,
b/ az adatkezelés megváltozott adatait – a változást elrendelő döntés után – át kell vezetni az Adatkezelési Nyilvántartásban.

5.3. <u>Adatkezelés megszüntetésével kapcsolatos feladatok</u>

48. Amennyiben a kezelt adatokra a továbbiakban nincs szükség (az adatkezelési cél megvalósult), vagy jogszabályi változások miatt, vagy az adatvédelmi felügyeleti hatóság vagy bíróság döntése értelmében az adatok kezelését meg kell szüntetni, az adatkezelési megbízott – az adatvédelmi tisztviselő és rajta keresztül a jogtanácsos és a Számítástechnika és Informatikai Csoport 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.

49. A 48. pontban meghatározott esetben

a/ megfelelően alkalmazni kell a 32-44. pont rendelkezéseit,
b/ az Adatkezelési Nyilvántartásból az adatkezelést vagy az egyes adatfajtákat törölni kell,

c/ az adatokat – a 48. pont a/ és b/ pontjában tett megkülönböztetés szerint –

c.a/ az informatikai rendszerekben archiválni kell, illetve

c.b/ az informatikai rendszerekből törölni kell, a papír alapú nyilvántartásban kezelt adatokat pedig – az Intézet iratkezelési szabályzatáról szóló főigazgatói utasítás szerint – selejtezni kell.

5.4. Az érdekmérlegelési teszt elvégzésének módszertana

50. Amennyiben az Intézet valamely adatkezelésének az Intézet 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.

51. Az érdekmérlegelési tesztet a tervezett adatkezelésért felelős szervezeti egység adatkezelési megbízottja végzi el. Az érdekmérlegelési tesztet írásban kell elvégezni. Az elkészült dokumentumot – a 38-40. 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 44. pont rendelkezéseit jelen esetben is alkalmazni kell.

52. 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.

53. 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/ az adatkezelés biztosítékainak leírása,

f/ az érdekmérlegelési teszt eredménye.

5.5. Az adatvédelmi hatásvizsgálat elvégzésének módszertana

54. 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.

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

56. A hatásvizsgálat elvégzését a tervezett adatkezelésért felelős szervezeti egység adatkezelési megbízottja koordinálja a 36. pont a.d/ 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 megbízott úgy ítéli meg, hogy az adatkezelés nem jár magas kockázattal, úgy meg kell indokolnia és dokumentumokkal igazolnia a mellőzés okait. A 44. pont rendelkezéseit jelen esetben is alkalmazni kell. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

57. 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.

58. 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/az ügyfelet jelentős mértékben érinti.

59. 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).

60. 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 leírását.

61. 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.

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

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

a/ a 60-62. 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 való konzultációra.

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

65. A hatásvizsgálatot legalább évente felül kell vizsgálni, szükség esetén újra el kell végezni.

6. AZ ÉRINTETTI JOGOK GYAKORLÁSÁNAK ELŐSEGÍTÉSE

6.1. <u>Az adatkezelési tevékenység nyilvánossága</u>

66. Az Intézet a honlapján egy olyan, „Adatvédelem” nevű oldalt tart fenn, amely bármely oldalról közvetlenül elérhető. Az „Adatvédelem” oldalon közzé kell tenni:

a/ az Intézet adatvédelmi politikáját;
b/ az Intézet általános adatkezelési tájékoztatóját;
c/ az Intézet egyes adatkezelési tevékenységeihez kapcsolódó (különös) adatkezelési tájékoztatók, ide nem értve a munkavállalók, egyéb jogviszonyban foglalkoztatottak adatainak kezelésére vonatkozó tájékoztatókat;
d/ közös adatkezelés esetén a közös adatkezelésben résztvevők közötti megállapodás lényegét, ha azt a különös adatkezelési tájékoztatók nem tartalmazzák;
e/ tájékoztatást arról, hogy az érintett kihez fordulhat az adatkezelést érintő kérdéseivel, panaszaival (az adatkezelő és az adatvédelmi tisztviselő elérhetősége, az adatvédelmi felügyeleti hatóság elérhetősége).

67. Az Intézet honlapjának olyan aloldalain, amelyek személyes adatok kezelésével járó egyes tevékenységekről tájékoztatnak (pl. egyes ellátási formák igénybevételének feltételeit tartalmazzák), el kell helyezni legalább az adott tevékenységhez kapcsolódó

a/ adatkezelési tájékoztatóra mutató hivatkozást;
b/ egyéb releváns dokumentumokat (pl. betegtájékoztatókat, formanyomtatványokat).

68. Az Intézet az Állami Egészségügyi Ellátó Központ Adatkezelési megbízásából kidolgozott mintadokumentumok Intézetre adaptált változatát alkalmazza a tevékenysége során.

69. Az Intézet szervezeti egységeinek vezetői gondoskodnak arról, hogy a szervezeti egység tevékenységeinek helyszínén az Intézet általános adatkezelési tájékoztatóján kívül az adott szervezeti egység tevékenységi körébe tartozó adatkezelésekről szóló (különös) adatkezelési tájékoztatók kinyomtatott formában is rendelkezésre álljanak.

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

6.2. A gyermekek tájékoztatáshoz való jogának biztosítása

71. Az Intézet szervezeti egységeinek vezetői az adatkezelési megbízottak közreműködésével gondoskodnak arról, hogy az Intézetben kezelt vagy az intézménnyel más módon kapcsolatba kerülő gyermekek az adataik kezelésével kapcsolatos tájékoztatást a gyermek számára világos és elérhető módon megkapják. A tájékoztatás az alábbi módokon történhet:

a/ a gyermek törvényes képviselője útján: a gyermeket érintő adatkezelésről a gyermekkel az Intézet részéről kapcsolatba lépő személy írásban tájékoztatja a gyermek törvényes képviselőjét, és írásban nyilatkoztatja arra vonatkozóan, hogy a tájékoztatást közli a gyermekkel;

b/ a gyermek vagy a törvényes képviselő kifejezett kérésére a gyermekkel az Intézet részéről kapcsolatba lépő személy – a fentieken túlmenően – biztosítja a gyermek részére a rövid, szóbeli tájékoztatást is az adatai kezelésével kapcsolatban;

c/ amennyiben a gyermek életkora és érettsége lehetővé teszi, a gyermekkel az Intézet részéről kapcsolatba lépő személy írásban közvetlenül a gyermeket is tájékoztatja az adatkezelésről. A speciális, gyermekeknek szóló tájékoztató dokumentumot az adatvédelmi tisztviselő készíti el az Intézet szervezeti egységeinek adatkezelési megbízottjai bevonásával. A különböző életkorú gyermekek számára a gyerekek életkorához igazodó tartalmú tájékoztató anyagot kell készíteni.

6.3. Korlátozottan cselekvőképes és cselekvőképtelen (gondokság alatt álló) személyek tájékoztatáshoz való jogának biztosítása

72. Az Intézet szervezeti egységeinek vezetői az adatkezelési megbízottak közreműködésével gondoskodnak arról, hogy az Intézetben kezelt korlátozottan cselekvőképes vagy cselekvőképtelen nagykorú személyek törvényes képviselői, illetve – állapotától függően – a korlátozottan cselekvőképes személy is megfelelő tájékoztatást kapjanak a személyes adatok kezeléséről. A törvényes képviselőt írásban nyilatkoztatni kell, hogy a tájékoztatást közli a gondnokság alatt álló érintettel.

6.4. Gyermekek és gondokság alatt álló személyek személyes adatainak kezelése hozzájáruló nyilatkozat alapján

73. Az Intézet szervezeti egységeinek vezetői az adatkezelési megbízottak közreműködésével gondoskodnak arról, hogy az Intézetben kezelt vagy az Intézménnyel más módon kapcsolatba kerülő gyermekek, illetve gondnokság alatt álló személyek tekintetében – amennyiben az adatkezelés hozzájáruláson alapul – a személyes adatok kezeléséhez való hozzájárulást törvényes képviselőjük adja meg.

74. A hozzájáruló nyilatkozatnak tartalmaznia kell a törvényes képviselőnek arra vonatkozó nyilatkozatát, hogy jogosult az érintett helyett a jognyilatkozat megtételére.

75. Amennyiben az érintett törvényes képviselői (pl.: szülői felügyelet gyakorlására jogosult szülők) eltérő nyilatkozatot tesznek az adatkezeléshez való hozzájárulásról, úgy az adatkezeléshez való hozzájárulást meg nem adottnak kell tekinteni.

6.5. Hozzátartozók tájékoztatása

76. Az Intézet szervezeti egységeinek vezetői az adatkezelési megbízottak közreműködésével gondoskodnak arról, hogy az Intézetben kezelt vagy az Intézménnyel más módon kapcsolatba kerülő személyek hozzátartozóit az adatvédelmi szabályoknak megfelelően tájékoztassák, amelyben – az érintett személy képességeit is figyelembe véve – magát az érintettet is bevonhatja.

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

7. AZ ÉRINTETTŐL SZÁRMAZÓ KÉRELMEK, PANASZOK MEGVÁLASZOLÁSÁNAK RENDJE

7.1. Az adatvédelmi bejelentések típusai

78. Az érintettől a következő, személyes adatai Intézet általi kezelését érintő beadványok érkezhetnek:

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

d/ kérheti nyilvántartott személyes adatai törlését – törléshez való jog (GDPR 17. cikk);
e/ kérheti személyes adatai kezelésének korlátozását (a pontatlan adat helyesbítéséig terjedő időre; a jogellenesen kezelt személyes adatok törlése helyett; jogszerűen kezelt, de szükségtelenné vált adatok törlése helyett az érintett kérésére az érintett jogi igényének előterjesztéséhez, érvényesítéséhez vagy védelméhez; jogos érdeken alapuló adatkezelés elleni tiltakozás elbírálásáig) – az adatkezelés korlátozásához való jog (GDPR 18. cikk);
f/ kérheti, hogy a rá vonatkozó, általa az Intézet 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. §].

7.2. Az adatvédelmi beadványok kezelésének eljárásrendje

79. Az egyes belső szabályzatoknak az érintettek adatainak felvételére, módosítására vagy helyesbítésére, illetve törlésére vonatkozó rendelkezései alkalmazását jelen főigazgatói utasítás 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).

80. Az Intézethez érkező, a 78. pontban meghatározott beadványokat az Intézet érintett szervezeti egységeinek a rájuk irányadó belső szabályzatokban foglaltaknak megfelelően kell – a GDPR 12. cikkében írt határidők figyelembevételével – elintézni, az alábbi kiegészítésekkel és eltérésekkel:

a/ a beadvány érkezése dátumát és időpontját pontosan rögzíteni kell;

b/ a 78. 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,

c/ a beadványokat intéző szervezeti egység bármely beadvány esetén kérheti az adatvédelmi tisztviselő véleményét a tekintetben, hogy a beadvány a 78. pontban meghatározott tárgyú-e, illetve, hogy az érintett kérte-e az adatkezelés korlátozását [zárolás, GDPR 18. cikk – lsd. 78. pont e/ alpont], és kérés esetén az adatvédelmi tisztviselő – a Számítástechnika és Informatikai Csoport útján – 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,

d/ az adatvédelmi tisztviselő dönt abban a kérdésben, hogy a 78. pontban meghatározott tárgyú beadvány egyértelműen megalapozatlan vagy túlzó-e,

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

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

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

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

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

j/ az Intézet szervezeti egységei a 78. pontban meghatározott tárgyú ügyekben készített válaszlevél-tervezetét jóváhagyás végett bemutatják az adatvédelmi tisztviselőnek;

k/ a beadvány határidőben megválaszoltnak minősül, ha a válaszadásra köteles szervezeti egység a választ a határidő utolsó napján postára adja vagy elektronikus üzenetet küld a beadványozónak a megtett intézkedésekről.

81. Az adatvédelmi beadványokról olyan ügyirat-nyilvántartást kell vezetni, amely segítségével bármikor egyértelműen azonosíthatók a 78. pont szerinti beadványok, nyomon követhetők a beadványok elintézése során tett intézkedések, és a rendelkezésre álló adatokból bármikor statisztika készíthető a következő szempontok szerint:

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

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

82. Az adatbiztonsági szabályok kialakítása során különös gondot kell fordítani a beépített és az alapértelmezett adatvédelem elveinek (GDPR 25. cikk) betartására, valamint arra, hogy az Intézet által alkalmazott adatbiztonsági intézkedések megfeleljenek a GDPR 32. cikkében írt követelményeknek.

83. Az Intézet működése során betartandó adatbiztonsági szabályokat (GDPR 32. cikk) külön szabályzatok tartalmazzák, így különösen a mindenkor hatályos Informatikai Biztonsági Szabályzata.

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

85. Az adatbiztonsági intézkedéseket érintően az adatkezelésért felelős szervezeti egység adatkezelési megbízottja:

a/ a szakterületére vonatkozó információk szolgáltatásával közreműködik az érintett informatikai elemek védelmi osztályokba sorolásában;
b/ a szakterületére vonatkozó információk szolgáltatásával közreműködik az adatkezelés biztonságát fenyegető kockázatok felmérésében és meghatározásában;
c/ az informatikai rendszert üzemeltető szervezeti egységgel együttműködve közreműködik azon információbiztonságot érintő feladatok végrehajtásában, amelyek az adatbiztonsági követelmények megvalósulásához szükségesek;
d/ figyelemmel kíséri a belső adatvédelmi szabályok érvényre juttatását a szakterületen belül, felhívja a szakterületen dolgozók figyelmét a szabályok betartására, jelzi a szabályok

megsértését az érintett munkavállaló felettesének, közreműködik a szakterületen dolgozók adatvédelmi tudatosságának növelésében.

86. Az adatbiztonság elveinek egy adatkezelés (lsd. 31. pont) bevezetésének vagy személyes adatkezelést és/vagy -feldolgozást eredményező módosításának előkészítése során történő érvényesítése a Számítástechnika és Informatikai Csoport adatkezelési megbízottjának (megbízottjainak) feladata, aki(ke)t az adatkezelési tevékenységet támogató nyilvántartási rendszerek kifejlesztésének, módosításának folyamatába kötelezően be kell vonni (lsd. 34. pont).

87. Az adatbiztonsági intézkedések mindennapi működésben történő betartására az Intézet minden alkalmazottja, valamint az Intézet informatikai rendszereihez hozzáférő személy köteles.

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

9.1. Közös adatkezelés

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

89. 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

b.a/ mely adatkezelési műveleteket (pl. hozzájáruló nyilatkozatok felvétele, adatok tárolása, adatok felhasználása stb.) végzik,

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

b.c/ az érintett jogai gyakorlását hogyan biztosítják (pl. egyesített vagy elkülönített ügyfélszolgálat stb.),

b.d/ az esetleges jogellenes adatkezelés következményeit milyen arányban viselik;

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

c.a/ 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,

c.b/ egymással kötelesek együttműködni az adatvédelmi rendellenesség vagy incidens okának kiderítésében és következményeinek felszámolásában,

c.c/ 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.

90. A közös adatkezelés szükségességét az adatkezelési megbízott az adatkezelés bevezetéséről való döntés előkészítése részeként [36.a.e/alpont] vizsgálja meg.

91. Amennyiben a közös adatkezelésben érintett másik adatkezelő harmadik országbeli adatkezelő, először abban a kérdésben kell dönteni – a 12. fejezet megfelelő alkalmazásával –, hogy a harmadik országbeli adatkezelő képes-e a GDPR-nak megfelelő adatbiztonsági követelmények teljesítésére. Amennyiben a harmadik országbeli adatkezelő nem képes a GDPR által elvárt adatbiztonsági követelmények érvényesítésére, illetve nem tud a GDPR szerinti garanciákat nyújtani a személyes adatok kezelésére, az adatkezelővel nem köthető megállapodás közös adatkezelésre.

92. Amennyiben döntés születik a közös adatkezelés bevezetéséről, az illetékes adatkezelési megbízott(ak), az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő és egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a jogtanácsos közreműködésével, továbbá a Számítástechnika és Informatikai Csoport 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.

93. A 92. pont alkalmazásában a szerződés megkötésére jogosult személy az, aki – az Intézet 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.

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

9.2. Adatfeldolgozói szerződések

95. Amennyiben harmadik országbeli adatfeldolgozó igénybevétele merül fel, először abban a kérdésben kell dönteni – a 12. fejezet megfelelő alkalmazásával –, hogy a harmadik országbeli adatfeldolgozó képes-e a GDPR-nak megfelelő adatbiztonsági követelmények teljesítésére. Amennyiben a harmadik országbeli adatfeldolgozó nem képes a GDPR által elvárt adatbiztonsági követelmények érvényesítésére, illetve nem tud a GDPR szerinti garanciákat nyújtani a személyes adatok kezelésére, az adatfeldolgozóval nem köthető szerződés.

96. Adatfeldolgozó igénybevétele esetén az adatfeldolgozóval kötendő szerződésnek tartalmaznia kell a GDPR 28. cikk (1)-(4) bekezdésében foglalt tartalmi elemeket a 97. pontban foglalt kiegészítések és pontosítások szerint.

97. 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 az Intézet 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

c.a/ az adatvédelmi incidens tudomásra jutása esetén az Intézet adatvédelmi tisztviselőjét haladéktalanul köteles értesíteni az adatvédelmi incidensről,

c.b/ köteles együttműködni az Intézet adatvédelmi tisztviselőjével és más közreműködő szervezeti egységgel az adatvédelmi incidens okának feltárásban és következményeinek felszámolásában,

c.c/ köteles együttműködni 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.

98. Az adatfeldolgozó igénybevételének szükségességét az adatkezelési megbízott az adatkezelés bevezetéséről való döntés előkészítése részeként [36. pont a.f/ pont] vizsgálja meg. Ezt a szabályt kell alkalmazni akkor is, ha az adatfeldolgozó igénybevételéről az adatkezelés folyamán születik döntés.

99. Az adatbiztonsági intézkedések megfelelőségének megítélése a Számítástechnika és Informatikai Csoport 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.

100. Amennyiben döntés születik az adatfeldolgozó igénybevételéről, az adatkezelési megbízott az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő és egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a jogtanácsos közreműködésével, továbbá a Számítástechnika és Informatikai Csoport véleményének kikérésével előkészíti az adatfeldolgozóval kötendő szerződés tervezetét és azt felterjeszti a szerződés megkötésére a 93. pont szerint jogosult személynek.

101. Az adatkezelési megbízott az adatfeldolgozói szerződés megkötését követően az adatfeldolgozó adatait (név és cím, kapcsolattartó neve és elérhetősége) megküldi az adatvédelmi tisztviselőnek, aki az információkat rögzíti az Adatkezelési Nyilvántartásban.

102. A 95.-101. 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 megbízott kikéri az adatvédelmi tisztviselő és rajta keresztül a jogtanácsos, továbbá a Számítástechnika és Informatikai Csoport véleményét is.

10. AZ ADATKEZELÉSI NYILVÁNTARTÁS

103. Az adatvédelmi tisztviselő vezeti az Adatkezelési Nyilvántartást. Az Adatkezelési Nyilvántartás valamennyi, az Intézet 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.

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

105. Az adatvédelmi tisztviselő az Adatkezelési Nyilvántartásba való betekintést – a Hatóság képviselőin kívül – az Intézet érintett szakterületei részére biztosítja.

106. Az adatkezelési megbízott az új adatkezelés bevezetését, az adatkezelés megkezdése előtt 15 munkanappal bejelenti az adatvédelmi tisztviselőnek [vö. 36.aj/ pont], aki azt az Adatkezelési Nyilvántartásba bejegyzi.

107. Az Adatkezelési Nyilvántartásba bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelési megbízott 5 munkanapon belül köteles bejelenteni az adatvédelmi tisztviselőnek [vö. 49. pont], aki ennek megfelelően módosítja az Adatkezelési Nyilvántartás adatait.

108. Az Adatkezelési Nyilvántartással összefüggésben az adatvédelmi tisztviselő:

a/ biztosítja, hogy az adatkezelések bevezetését megelőző döntés előkészítése során az érintett szakterületek az Adatkezelési Nyilvántartás adatait megismerhessék a felesleges, párhuzamos adatkezelések elkerülése, illetve az új adatkezelésnek a meglévő adatkezelésekhez való illeszkedése érdekében;

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

c/ a jogtanácsossal együttműködve figyelemmel kíséri az adatkezelést érintő jogszabályok változását és a szükséges módosításokra felhívja az adatkezelési megbízottak figyelmét;

d/ az adatvédelmi felügyeleti hatóság megkeresésére adatot szolgáltat az Adatkezelési Nyilvántartásból.

11. AZ ADATVÉDELMI INCIDENSEK KEZELÉSE

11.1. <u>Az adatvédelmi incidens minősítése</u>

109. Adatvédelmi incidens csak akkor következik be, ha az adatbiztonsági intézkedések [8. 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 állíthatóak helyre). Magas kockázatúnak minősül az az eset, amely fizikai, vagyoni vagy nem vagyoni károkat okozhat az érintetteknek, pl. az érintetteknek a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, pénzügyi veszteséget, jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok integritásának, illetve bizalmas jellegének sérülését eredményezheti;

b/ enyhe incidens: minden incidens, amely nem tartozik az a) pont alá (pl. átmeneti szolgáltatásleállás, -kiesés az Intézet munkavállalói által használt olyan belső rendszerekben, amely nem jár adatsérüléssel vagy adatvesztéssel).

110. Az adatvédelmi incidensre vonatkozó szabályokat kell alkalmazni az Intézet tulajdonát képező adathordozón, mobiltelefonon, laptopon, egyéb számítástechnikai eszközön tárolt adatokra, továbbá az Intézet 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 az Intézet birtokában lévő papíralapú adathordozón lévő adatokra is alkalmazni kell.

111. Az elektronikus információs rendszereket érintő (biztonsági vagy egyéb) események adatvédelmi incidensnek is minősülnek, amennyiben személyes adatokra nézve következik be. A jelen Szabályzatnak az adatvédelmi incidens kezelésére vonatkozó rendelkezéseinek alkalmazása nem mentesít az elektronikus információs rendszerek érintő (biztonsági vagy egyéb) események kezelésére (bejelentésére, kivizsgálására stb.) vonatkozó szabályok betartása alól, azaz az elektronikus információs rendszereket érintő (biztonsági vagy egyéb) események kezelésére vonatkozó szabályokat jelen Szabályzat előírásaival párhuzamosan alkalmazni kell.

11.2. <u>Az adatvédelmi incidens bejelentése</u>

112. Az Intézet irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező azon természetes személy (a munkavégzésre irányuló jogviszony jellegétől függetlenül), aki az Intézet által kezelt vagy feldolgozott személyes adatokkal kapcsolatban, vagy az Intézet szerződéses partnere által kezelt vagy feldolgozott személyes adataival kapcsolatban adatvédelmi incidenst vagy annak gyanúját észleli, köteles azt haladéktalanul bejelenteni az adatvédelmi tisztviselőnek az informatika@magy.eu e-mail címen, telefonon a 37/886-716 számon, vagy az intraneten erre a célra létrehozott űrlapot kitölteni. Az előbbieken túli egyéb bejelentő az Intézet elektronikus elérhetőségén (igazgatas@magy.eu) jelentheti be az adatvédelmi incidenst.

113. Amennyiben az adatvédelmi incidens bejelentése szóban (telefonon vagy személyesen) történik (beleértve az Intézet telefonos elérhetőségein tett közérdekű bejelentéseket is), azt a szóbeli közlést követő legfeljebb 1 napon belül – a 112. pontban írottak figyelembevételével – írásban is meg kell erősíteni. Ilyen esetben a szóbeli közlés időpontját külön fel kell tüntetni.

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

115. 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 az Intézet adatvédelmi tisztviselőjét köteles haladéktalanul, de legkésőbb az észlelést követő 24 órán belül értesíteni írásban és telefonon is. A szerződésnek tartalmaznia kell továbbá a közös adatkezelő, illetve az adatfeldolgozó kötelezettségeit adatvédelmi incidens bejelentésében és kivizsgálásában [lsd. 97.c/ pont].

11.3. <u>Incidensprotokoll általában</u>

116. Az érintett szakterület bevonásával a riasztásokban szereplő incidens gyanús esemény kezelésekor a következők szerint kell eljárni:

a/ figyelembe kell venni a különböző biztonsági szabályozásokban az incidens- gyanús események elhárítására vonatkozó rendelkezéseket;

b/ amennyiben a riasztás személyes adatot tartalmazó alkalmazás sérülékenységével kapcsolatban keletkezett, az incidens elhárítását végző személy az adatvédelmi tisztviselőt haladéktalanul tájékoztatja;

c/ amennyiben az Intézet rendelkezik automatizált módszerrel az adott sérülés (incidens) elhárítására, akkor azt azzal az eszközzel azonnal el kell kezdeni;

d/ ha az Intézet – a mindenkor hatályos Információ Biztonsági Szabályzatában foglaltakkal összhangban – nem rendelkezik automatizált módszerrel az adott sérülés (incidens) elhárítására, akkor azt manuális módon kell azonnal elkezdeni;

e/ amennyiben a sérülés elhárítása belső erőforrásból nem kivitelezhető, akkor külső szakértőket kell bevonni az elhárítás folyamatába.

117. A nem papíralapon kezelt adattal kapcsolatos incidensek kezelésére az Intézet mindenkor hatályos Információ Biztonsági Szabályzatában foglaltak is irányadóak. A papíralapon kezelt iratokkal kapcsolatban a jelen Szabályzat személyi hatálya alá tartozó személyek 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 személyi hatálya alá tartozó személyek kötelesek az Intézet egyéb belső szabályzatai, így különösen az iratkezelés rendjéről, illetve a biztonsági előírásokról szóló mindenkor hatályos belső szabályzatnak megfelelően eljárni.

11.4. Az adatvédelmi incidens kivizsgálása

118. Adatvédelmi incidens (papíralapú és nem papíralapú adatokra vonatkozóak egyaránt) felmerülése esetén az Intézmény adatvédelmi tisztviselője a jogtanácsos és az informatikai szakterület, továbbá szükség esetén az adott szakterületért felelős szervezeti egység kijelölt munkatársának (a továbbiakban együtt: incidensvizsgáló bizottság) közreműködésével megvizsgálja, és a 109. pont szerint kategorizálja a bekövetkezett incidenst és meghatározza az esetleges elhárítás érdekében szükséges további intézkedéseket. A bejelentőt – szükség esetén – további információk közlésére kell felkérni. Az incidensvizsgáló bizottságot az adatvédelmi tisztviselő hívja össze, az említett személyeknek szükség esetén munkaidőn kívül is rendelkezésre kell állniuk. Az incidensvizsgáló bizottság munkáját az adatvédelmi tisztviselő koordinálja, és képviseli az Intézmény egyéb szervezeti egységei felé.

119. Az incidensvizsgáló bizottság üléseiről emlékeztetőt, döntéseiről indoklást is tartalmazó jegyzőkönyvet, vizsgálatairól pedig intézkedési javaslatokat is tartalmazó jelentést kell készíteni. Az incidensvizsgáló bizottság munkáját tartalmazó dokumentumok kezelésére az Intézmény mindenkori iratkezelési szabályai az irányadók. Az incidensvizsgáló bizottság korlátozhatja a munkájáról szóló dokumentumokba betekintők körét.

120. Az adatvédelmi incidensről az adatvédelmi tisztviselő értesíti az Intézmény főigazgató főorvosát.

121. 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 (beleértve a törlést/megsemmisítést is) történt,

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

f/ melyek az adatvédelmi incidensből eredő, valószínűsíthető következmények,

g/ az Intézet által alkalmazott technikai és szervezési védelmi intézkedések az incidensben érintett személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik-e az adatokat.

122. Ha a bejelentés előzetes megvizsgálása azzal az eredménnyel jár, hogy az elektronikus információs rendszereket érintő (biztonsági vagy egyéb) esemény nem érintett személyes adatokat, akkor a vizsgálatot az Intézmény mindenkor hatályos Informatikai Biztonsági Szabályzatában, illetve az Adatvédelmi és Informatikai incidens kezelési szabályzatában foglaltak szerint kell folytatni.

123. Az incidensvizsgáló bizottság – az adatvédelmi tisztviselő útján – 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, az érintettek tájékoztatásának szükségességéről és módjáról, valamint arról, hogy szükséges-e az incidens részletes vizsgálata:

a/ az Intézet főigazgatóját;

b/ informatikai rendszert is érintő incidens esetén az informatikai szakterület vezetőjét;

c/ a szakmailag illetékes szervezeti egység vezetőjét.

124. Az incidensvizsgáló bizottság javaslata alapján a főigazgató legkésőbb a bizottság javaslatának kézhezvételét követő 1 napon belül dönt a GDPR 33. cikkében írt adatvédelmi felügyeleti hatósági bejelentés szükségességéről. A főigazgató döntéséről az adatvédelmi tisztviselő értesíti a 122. pontban meghatározott egyéb személyeket.

125. Az adatvédelmi incidens részletes vizsgálatának szükségességéről az incidensvizsgáló bizottság dönt. A részletes vizsgálatot a vizsgálat megkezdése után a lehető leghamarabb, de legfeljebb megkezdésének napjától számított 16 munkanapon belül le kell zárni.

126. A vizsgálat során elsősorban az alábbi módszerek alkalmazhatóak:

a/ személyes megbeszélés az adatvédelmi incidenst észlelő személyekkel, valamint az érintett szervezeti egységek munkatársaival és vezetőivel,

b/ írásbeli tájékoztatás kérése az érintett szervezeti egységektől,

c/ dokumentumok vizsgálata,

d/ informatikai rendszerek, hálózatok és eszközök vizsgálata, beleértve a naplóállományok vizsgálatát is.

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

128. Az incidensvizsgáló bizottság a részletes vizsgálat megállapításairól, illetve a javasolt intézkedésekről a részletes vizsgálat megkezdését követő 16 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 is.

129. A részletes vizsgálatról szóló jelentést a 122. pont a/-c/ alpontjában említett vezetőknek kell megküldeni.

130. A jelentés alapján a vizsgálatban érintett szervezeti egységek vezetői 15 napon belül a megvalósításhoz szükséges határidőre tett javaslatot is tartalmazó intézkedési tervet készítenek és azt megküldik az adatvédelmi tisztviselő útján az incidensvizsgáló bizottságnak.

131. Az intézkedési tervet és a megvalósításhoz szükséges határidőt tartalmazó szakterületi javaslatot az incidensvizsgáló bizottság a kézhezvételtől számított 3 munkanapon belül véleményezi, majd jóváhagyásra megküldi a főigazgató főorvos részére.

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

133. Abban az esetben, ha az illetékes vezető módosítani kívánja az intézkedési tervben a rá vonatkozó határidőt, indokolással ellátott módosítási javaslatát megküldi az adatvédelmi tisztviselő részére. A főigazgató főorvos dönt a módosítási javaslat elfogadásáról, vagy elutasításáról, és erről az adatvédelmi tisztviselő útján értesíti az illetékes vezetőt.

134. Az adatvédelmi tisztviselő az intézkedési tervben foglaltak végrehajtásáról, az összes intézkedés befejezését követő 3 munkanapon belül tájékoztatást küld a főigazgató főorvos részére.

11.5. Az érintett tájékoztatása a súlyos adatvédelmi incidensről

135. Súlyos adatvédelmi incidens esetén az Intézmény – az érintettel kapcsolatban rendelkezésére álló elérhetőségeken, ennek hiányában vagy alkalmazásuk lehetetlensége esetén (vö. GDPR 34. cikk) az Intézmény honlapján közzétett közlemény útján – indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. Az érintettek tájékoztatásának módjára az incidensvizsgáló bizottság javaslatot tesz. Az érintettek tájékoztatását – az érintett szervezeti egységek bevonásával – az adatvédelmi tisztviselő koordinálja.

136. Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az alábbi információkat és intézkedéseket:

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

b/ az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

c/ az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

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

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

b/ az Intézet 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 áll fenn;

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.

138. Az Intézet főigazgatójának döntése alapján az Intézet az érintetteket az Intézet honlapján vagy országos lefedettségű sajtótermékben közzétett hirdetmény útján is értesítheti.

11.6. <u>Az adatvédelmi incidens bejelentése a Hatóságnak</u>

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

140. A bejelentés összeállításának és beadásának felelőse az adatvédelmi tisztviselő. Az adatvédelmi incidensről szóló bejelentéshez szükséges információkat az adatvédelmi tisztviselő rendelkezésére kell bocsátani.

141. 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 az Intézet által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

142. Ha nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később (pl. a 131. pont szerinti jóváhagyás után haladéktalanul) részletekben is közölhetők.

11.7. Az adatvédelmi és egyéb incidensek nyilvántartása

143. Az adatvédelmi incidensekről az adatvédelmi tisztviselő nyilvántartást vezet. E szabályzat nem érinti az egyéb jogszabályok szerint a biztonsági események kezelésével kapcsolatban vezetendő nyilvántartásokra vonatkozó szabályok alkalmazását.

144. 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 tudomásszerzés időpontját,

d/ az adatvédelmi incidens körülményeit, hatásait,

e/ az adatvédelmi incidens elhárítására megtett intézkedéseket,

f/ az adatvédelmi incidenssel kapcsolatban adott tájékoztatások adatait.

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

12. HARMADIK ORSZÁGBA IRÁNYULÓ ADATTOVÁBBÍTÁS KÜLÖNÖS SZABÁLYAI

146. 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, figyelembe véve a GDPR szabályait és az aktuális országbesorolást.

147. Az adatvédelmi tisztviselő – szükség esetén a jogtanácsos és a Számítástechnika és Informatikai Csoport véleményének kikérése után – javaslatot tesz az adattovábbítás módjára, az adatátadás során alkalmazandó biztosítékok körére.

13. BELSŐ ADATVÉDELMI ELLENŐRZÉSI ELJÁRÁS

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

149. 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 szervezeti egység ellenőrzésére sor kerüljön. Az éves ellenőrzési tervet legkésőbb adott év február 28. napjáig kell elkészíteni és az Intézet főigazgatója részére bemutatni.

150. Az éves ellenőrzési tervet az Intézet főigazgatója hagyja jóvá.

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

152. 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.

153. 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.

154. 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.

155. 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.

156. 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 az Intézet főigazgatója előzetesen engedélyezi.

157. Az adott ellenőrzéssel kapcsolatban az Intézet 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 az Intézet főigazgatója részére küld meg.

14. ZÁRÓ RENDELKEZÉSEK

158. Jelen szabályzat az aláírást követő napon lép hatályba.

159. Jelen utasítás hatálybalépésével visszavonom:

a/ a Mátrai Gyógyintézet Adatkezelési Szabályzatát,

b/ a Mátrai Gyógyintézet Adatvédelmi és informatikai incidenskezelési szabályzatának 3-6. fejezeteit.