SZAB-2-1/2021

ADATVÉDELMI ÉS INCIDENSKEZELÉSI SZABÁLYZAT

A PÉLDÁNY TULAJDONOSA:

Készítette: Országos Kórházi Főigazgatóság megbízásából, WSH Számítástechnikai, Oktató és Szolgáltató Kft.

Jóváhagyta: .....
Dr. Dobosi Zsolt főigazgató

Jahn Ferenc Dél-pesti Kórház és Rendelőintézet FŐIGAZGATÓ

Országos Kórházi Főigazgatóság

Tudásközpont rendszer támogatás projekt

Intézményi adatvédelmi és incidenskezelési szabályzat

- végleges -

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
2.0	2020.11.27	WSH Kft. / SFÜI	teljeskörűen felülvizsgált mintaszabályzat véglegesített verziója
2.1	2021.01.27	WSH Kft. / SFÜI	felülvizsgált mintaszabályzat alábbi intézményre testreszabott munkaanyag változata
3.0	2021.03.25	WSH Kft. / SFÜI	felülvizsgált mintaszabályzat alábbi intézményre testreszabott végleges változata

A Jahn Ferenc Dél-pesti Kórház és Rendelőintézet adatvédelmi és incidenskezelési szabályzata

Tartalomjegyzék

1. A szabályzat célja, hatálya, alapelvek, alapfogalmak 5

1.1. Bevezető rendelkezések 5

1.2. A Szabályzat célja 6

1.3. A szabályzat személyi hatálya 7

1.4. A szabályzat tárgyi hatálya 7

1.5. Dokumentálási kötelezettség 7

2. Alapfogalmak 8

3. A szabályzathoz kapcsolódó jogszabályok, belső szabályzatok 10

4. Az adatvédelmi tevékenység szervezete és irányítása az intézménynél 12

4.1. Az adatvédelmi tevékenység ellátásában résztvevők 12

4.2. Az adatvédelmi tisztviselő 14

5. Adatkezelés bevezetésével, módosításával és megszüntetésével kapcsolatos feladatok 17

5.1. Adatkezelés bevezetésével kapcsolatos feladatok 17

5.2. Az adatkezelési megbízott feladatai az adatkezelés során 21

5.3. Adatkezelés megszüntetésével kapcsolatos feladatok 22

5.4. Az érdekmérlegelési teszt elvégzésének módszertana 22

5.5. Az adatvédelmi hatásvizsgálat elvégzésének módszertana 23

6. az érintetti jogok gyakorlásának elősegítése 25

6.1. Az adatkezelési tevékenység nyilvánossága 25

6.2. A gyermekek tájékoztatáshoz való jogának biztosítása 26

6.3. Korlátozottan cselekvőképes és cselekvőképtelen (gondokság alatt álló) személyek tájékoztatáshoz való jogának biztosítása 26

6.4. Gyermekek és gondokság alatt álló személyek személyes adatainak kezelése hozzájáruló nyilatkozat alapján 26

6.5. Hozzátartozók tájékoztatása 27

7. Az érintettől származó kérelmek, panaszok megválaszolásának rendje 28

7.1. Az adatvédelmi bejelentések típusai 28

7.2. Az adatvédelmi beadványok elintézése 29

8. Az adatbiztonsági intézkedések (technikai és szervezési intézkedések) meghatározása és végrehajtása 32

9. A közös adatkezelői és az adatfeldolgozói szerződések megkötésének és végrehajtása ellenőrzésének szabályai 33

9.1. Közös adatkezelés 33

9.2. Adatfeldolgozói szerződések 34

10. Az Adatkezelési Nyilvántartás 37

11. Az adatvédelmi incidensek kezelése 39
11.1. Az adatvédelmi incidens minősítése 39
11.2. Az adatvédelmi incidens bejelentése 40
11.3. Incidensprotokoll általában 40
11.4. Az adatvédelmi incidens kivizsgálása 41
11.5. Az érintett tájékoztatása a súlyos adatvédelmi incidensről 44
11.6. Az adatvédelmi incidens bejelentése a Hatóságnak 45
11.7. Az adatvédelmi incidensek nyilvántartása 45
12. Harmadik országba irányuló adattovábbítás különös szabályai 46
13. Belső adatvédelmi ellenőrzési eljárás 46
14. Záró rendelkezések 48

1. A SZABÁLYZAT CÉLJA, HATÁLYA, ALAPELVEK, ALAPFOGALMAK

1.1. Bevezető rendelkezések

1. A Jahn Ferenc Dél-pesti Kórház és Rendelőintézet (a továbbiakban: Intézmény) 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 Intézmény 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 Intézményre irányadó egyéb jogszabályok rendelkezései szerint kezelni. Az Intézmény 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 Intézmény 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 Intézmény tevékenysége során a személyes adatok védelméhez fűződő jog érvényesülését, továbbá, hogy az Intézmény által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes és különleges adatok kezelése során irányadó adatvédelmi és adatbiztonsági szabályokat.

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

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

1.3. A szabályzat személyi hatálya

7. Jelen Szabályzat személyi hatálya kiterjed az Intézmény munkavállalóira, 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 Intézmény megbízásából személyes adatok kezelését vagy feldolgozását végzők esetén az erre a jogviszonyra az Intézmény által kötött szerződésben a GDPR 28. cikkének megfelelően rendelkezni kell arról, hogy az Intézmény 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 Intézmény 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);
   c/ 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);
   d/ az Intézménnyel szerződéses kapcsolatban álló társaságok képviselőinek, kapcsolattartóinak az adataira vonatkoznak.

1.5. Dokumentálási kötelezettség

9. Az Intézmény felelős a személyes adatok kezelésére vonatkozó alapelvek [GDPR 5. cikk (1) bek.] betartásáért. Az Intézménynek 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 Intézmény – 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 Intézmény – 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 0. fejezetében meghatározott adattartalmú, folyamatosan karbantartott nyilvántartás;

c/ adatkezelésért felelős szervezeti egység: az Intézmény azon szervezeti egysége, amelynek feladatkörébe tartozik az Intézmény 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 Intézmény szervezetében működő, a GDPR 39. cikkében meghatározott feladatokat az Intézmény jelen szabályzatában foglaltak szerint ellátó, az Intézmény-nyel 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 Intézmény 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 Intézmény tevékenységére vonatkozó jogszabályokban az Intézmény 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]
Ibtv.	2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
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
	a Jahn Ferenc Dél-pesti Kórház és Rendelőintézet Közérdekű és közérdekből nyilvános adatok közzétételének szabályzata
	a Jahn Ferenc Dél-pesti Kórház és Rendelőintézet Informatikai Biztonsági Szabályzata, Katasztrófavédelmi terve, valamint a Létfontosságú rendszerelemek üzemeltetői biztonsági terve
	a Jahn Ferenc Dél-pesti Kórház és Rendelőintézet Vagyonvédelmi Szabályzata
	a Jahn Ferenc Dél-pesti Kórház és Rendelőintézet Betegjogok, Betegadatok és Betegbiztonság Védelmi Szabályzata
	a Jahn Ferenc Dél-pesti Kórház és Rendelőintézet Iratkezelési Szabályzata
	a Jahn Ferenc Dél-pesti Kórház és Rendelőintézet szervezeti egységei által kezelt nyilvántartási rendszereket szabályozó belső rendelkezések
	a Jahn Ferenc Dél-pesti Kórház és Rendelőintézet Közalkalmazotti szabályzata, valamint az egyes munkavállalói juttatásokat szabályozó külön szabályzatok

	a Jahn Ferenc Dél-pesti Kórház és Rendelőintézet Intézeti Adatainak Védelme és a Kezelt Egészségügyi-, valamint Személyes Adatok Integrált Kockázatkezelésének Szabályzata.

4. AZ ADATVÉDELMI TEVÉKENYSÉG SZERVEZETE ÉS IRÁNYÍTÁSA AZ INTÉZMÉNYNÉL

4.1. Az adatvédelmi tevékenység ellátásában résztvevők

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

13. A főigazgató felelős azért, hogy az Intézmény – mint adatkezelő, illetve adatfeldolgozó – működése az adatvédelmi szabályoknak megfeleljen. Ennek érdekében:
    a/ gondoskodik az adatvédelmi tevékenység irányításában és ellátásában résztvevő szervezeti egységek kijelöléséről, feladataik, az adatvédelmi tárgyú ügyekkel kapcsolatos döntési jogkörök meghatározásáról, az egyes adatkezelési döntési szintek kialakításáról;
    b/ biztosítja az adatvédelmi tevékenység irányításához és ellátásához, valamint az érintett jogai gyakorlásához szükséges személyi és tárgyi feltételeket;
    c/ felelős az adat- és titokvédelmi, valamint biztonsági és információbiztonsági szabályzatok kiadásáért és betartatásáért;
    d/ gondoskodik arról, hogy az adatvédelmi tevékenység során esetleg előforduló, feltárt hiányosságok megszűntetéséről, szükség szerint a felelősségre vonásról;
    e/ kinevezi az Intézmény adatvédelmi tisztviselőjét, és az adatvédelmi tisztviselő nevét és elérhetőségét bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak;
    f/ munkajogi értelemben vett közvetlen felettese az adatvédelmi tisztviselőnek;
    g/ biztosítja az Intézmény adatvédelmi tisztviselője feladatainak ellátásához szükséges személyi és tárgyi feltételeket.

14. Az Intézmény 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 Jogi Irodával, valamint az informatikai szakterülettel együttműködve gondoskodnak az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról;
    b/ 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 Intézmény döntéselőkészítésre vonatkozó szabályainak megfelelően – döntenek a jelen utasításban, illetve az adatkezeléssel járó folyamatot szabályozó egyéb belső szabályzatokban a feladat- és hatáskörébe utalt kérdésekben.

15. Az igazgatásszervezési referens
    a/ adatvédelmi incidens esetén közreműködik az érintettek tájékoztatásának módjáról és a tájékoztatás tartalmáról való döntés előkészítésében,
    b/ adatvédelmi incidens esetén – az adatvédelmi tisztviselő közreműködésével – szükség esetén sajtóközleményt bocsát ki és – a főigazgató ilyen tartalmú utasítása esetén – kizárólagos kapcsolatot tart a sajtó képviselőivel.

16. Az igazgatási, jogi és minőségügyi főigazgató-helyettes:

    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. Az informatikai szakterület szervezeti egységei az Intézmény szervezeti és működési szabályzatában, valamint az Intézmény Informatikai Biztonsági Szabályzatában meghatározott feladatkörükben:
    a/ ellátják az informatikai biztonsági biztonsággal kapcsolatos feladatokat a folyamatos üzemeltetési feladatok kivételével, különösen az Intézmény Informatikai Biztonsági Szabályzatában 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 Intézmény Informatikai Biztonsági Szabályzatában 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 Jogi Iroda:
    a/ szakmai támogatást nyújt az adatkezeléssel összefüggő, nem adatvédelmi jogszabályok értelmezésében,
    b/ biztosítja, hogy az adatvédelmi tisztviselő véleményét kikérjék az Intézmény adatvédelmi tárgyú vagy adatvédelmi vonatkozású belső szabályzatainak előkészítése során,
    c/ biztosítja az Intézmény képviseletét az érintett által az Intézmény ellen az érintett adatvédelmi jogainak megsértése miatt indított, illetve az Intézmény által a Nemzeti Adatvédelmi és Információszabadság Hatóság határozatainak felülvizsgálata iránt indított perekben, illetve egyéb eljárásokban.

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 adatkezelések nyilvántartásának naprakészen tartása 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 Intézmény kezelésében lévő az adatok biztonsági osztályba sorolásában.

20. Adatkezelési megbízottat minden szervezeti egységnél (kiemelten a betegellátó osztályokon, valamint a humánerőforrás-gazdálkodás, a pénzügy és az informatika területén) ki kell jelölni. Adatkezelési megbízottnak olyan személyt kell kijelölni, aki az adott szakterületet, üzleti/adminisztratív folyamato(ka)t, illetve – az informatikai szakterületen – a szakterületek tevékenységét támogató informatikai rendszereket illetően kellő ismeretekkel bír.

4.2. Az adatvédelmi tisztviselő

21. Az adatvédelmi tisztviselőt a főigazgató nevezi ki az olyan, az Intézménnyel foglalkoztatási jogviszonyban álló természetes személyek közül, aki ismeri az Intézmény működését, feladatait, munkafolyamatait és rendelkezik:
    a/ lehetőleg jogi végzettséggel vagy informatikai főiskolai (BSc) vagy egyetemi (MSc) szintű végzettséggel;

b/ az európai és hazai adatvédelemmel kapcsolatos főbb szabályozók, hatósági és bírósági határozatok, iránymutatások ismeretével;
c/ alapvető adatkezelési és informatikai folyamatok ismeretével;
d/ legalább 2 év adatvédelmi területen szerzett gyakorlattal.

22. Az adatvédelmi tisztviselő kinevezése mellett az Intézmény 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 bocsátható el. Jelen Szabályzatban foglalt tevékenysége ellátása során autonóm, szakmai ügyekben kizárólag a főigazgatónak tartozik felelősséggel.

24. Az Intézmény elősegíti az adatvédelmi tisztviselő megfelelő szakmai feladatellátását, ennek érdekében az Intézmény biztosítja különösen az adatvédelmi tisztviselő feladatai végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáférést, valamint a szakértői szintű ismereteinek fenntartásaihoz szükséges forrást, elegendő időt a 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 Jogi Iroda 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 minden olyan információ tekintetében, amely nem minősül közérdekű vagy közérdekből nyilvános adatnak.

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

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

29. Az adatvédelmi tisztviselő nevét és elérhetőségeit az Intézmény honlapján, székhelyén, telephelyén a nyilvánosság részére mindenkor elérhetővé kell tenni. Az Intézmény továbbá közli 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 Intézmény egyéb belső szabályzatai rendelkezéseinek a megtartását, belső adatvédelmi ellenőrzési eljárást folytat le;
    c/ kivizsgálja – az érintett szakterületek és a Jogi Iroda bevonásával – a neki címzett panaszokat, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
    d/ a Jogi Irodával és az informatikai szakterülettel együttműködve elkészíti az adatvédelmi és adatbiztonsági szabályzatot;
    e/ az igazgatásszervezési referenssel együttműködve gondoskodik az adatvédelmi ismeretek oktatásáról [elsősorban az intraneten közzétett segédanyagok útján];
    f/ a Jogi Irodával együttműködve személyes adatok kezelésére vonatkozó előírásokról tájékoztatást nyújt, tanácsot ad;
    g/ személyes adatot is kezelő új informatikai rendszer belső fejlesztéssel történő bevezetése során közreműködik a beépített adatvédelem alapelve érvényesülésének érdekében, vagy ha szükséges, az adatvédelmi hatásvizsgálat lefolytatásában;
    h/ az adatvédelmi incidenskezeléssel kapcsolatban ellátja a jelen szabályzat szerinti feladatokat;
    i/ az Intézmény adatvédelmi helyzetéről éves összefoglaló jelentést készít a főigazgatónak;
    j/ kapcsolatot tart és – a Jogi Iroda és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – együttműködik a Hatósággal;
    k/ az Országos Kórházi Főigazgatóság számára adatszolgáltatást teljesít;
    l/ nyomon követi és érvényre juttatja az Országos Kórházi Főigazgatóság Adatvédelmi Tudásközpont által kiadott állásfoglalásokat, iránymutatásokat és más mintadokumentumokat, valamint kapcsolatot tart, illetve konzultációt kezdeményez a személyes adatok védelmét érintő ügyekben (szükség esetén megoldási javaslat, elemzés stb.).

5. ADATKEZELÉS BEVEZETÉSÉVEL, MÓDOSÍTÁSÁVAL ÉS MEGSZÜNTETÉSÉVEL KAPCSOLATOS FELADATOK

5.1. Adatkezelés bevezetésével kapcsolatos feladatok

31. Jogszabályban elrendelt vagy jogszabály rendelkezése miatt szükséges, vagy az Intézmény 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 a [döntéselőkészítés rendjére vonatkozó belső szabályokat] 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:
        aa/ az adatok felvételének, módosításának, törlésének rendje,
        ab/ adatszolgáltatási kötelezettségek meghatározása az adatok naprakészen tartása érdekében,
        ac/ a nyilvántartási rendszerből történő adattovábbítás, az ahhoz való hozzáférés rendje;
    b/ az adatkezelésre vonatkozó különös adatbiztonsági intézkedések meghatározása;
    c/ mellékletként
        ca/ a GDPR-nak, az Infotv-nek és egyéb alkalmazandó jogszabálynak megfelelő adatkezelési tájékoztatót,
        cb/ 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. Az informatikai szakterület 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):
        aa/ meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, és ilyen tartalmú javaslatot készít a döntésre jogosultnak (GDPR 4. cikk 7. és 16. pont);
        ab/ az aa/ alpontban meghatározott feladat részeként előterjesztést tesz a döntésre jogosultnak arról, hogy az eltérő célú adatkezelés összeegyeztethető-e az eredeti céllal, és így szolgálhat-e a tervezett adatkezelés új jogalapjául [GDPR 6. cikk (4) bek.];
        ac/ az aa/ pontban meghatározott feladat részeként, amennyiben az adatkezelés jogalapja a jogos érdek lehet, elkészíti az érdekmérlegelési teszt dokumentumának tervezetét [GDPR 6. cikk (1) bek. f) pont];
        ad/ az aa/ pontban meghatározott feladat részeként az adatvédelmi tisztviselő véleményének kikérése után dokumentálja az adatvédelmi hatásvizsgálat el nem végzésének indokait vagy 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 az adatvédelmi hatásvizsgálatot, elkészíti ennek dokumentumát, és kikéri róla az adatvédelmi tisztviselő, valamint – ha alkalmazható – az érintettek vagy képviselőik véleményét [GDPR 35. cikk (1)-(2) és (9) bek.];
        ae/ az aa/ pontban meghatározott feladat részeként előterjesztést tesz a döntésre jogosultnak arról, hogy az adatkezelést közös adatkezelésként indokolt-e ellátni, illetve indokolt-e adatfeldolgozót bevonni;
        af/ az aa/ pontban meghatározott feladat részeként javaslatot tesz automatizált döntéshozatali módszer, illetve profilalkotási módszer alkalmazására [GDPR 22. cikk (1) bek.];
        ag/ az aa/ pontban meghatározott feladat részeként megszövegezi a hozzájáruló nyilatkozatot [GDPR 7. cikk (2) bek.], illetve, ha közös adatkezelés vagy adatfeldolgozó bevonása miatt szükséges, a megfelelő szerződéses rendelkezéseket;

ah/ megfogalmazza az új adatkezelésre, vagy a meglévő adatkezelés módosítására vonatkozó információkkal kiegészíti az adatkezelésről szóló tájékoztatást (GDPR 13-14. cikk);

ai/ az adatkezelésről szóló döntést követően az informatikai szakterület közreműködésével gondoskodik az adatkezelésről szóló új vagy módosított tájékoztatás könnyen hozzáférhető módon való közzétételéről [GDPR 12. cikk (1) bek.];

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

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

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

b/ az informatikai szakterület adatkezelési megbízottjai – szervezeti egységük feladatkörében – a személyes adatot kezelő rendszer fejlesztése és beszerzése során közreműködnek

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

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

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

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

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

bf/ az adott adatkezelés különös (az Intézmény Informatikai Biztonsági Szabályzatától eltérő) adatbiztonsági intézkedések meghatározásában;

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

37. A 36. pont alkalmazása során döntésre jogosultnak minősül az személy, aki – az Intézmény 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:
        aa/ a Jogi Iroda véleményét a 36. pont aa/, ae/, af/, ag/, ah/ és al/ alpont tekintetében;
        ab/ az informatikai szakterület véleményét a 36. pont aa/, ad/, ae/, af/, ah/ és al/ alpont tekintetében;

    b/ megvizsgálja a véleményezésre megküldött dokumentumot/leírást
        ba/ adatvédelmi jogi szempontból,
        bb/ abból a szempontból, hogy azok milyen módon illeszthetők be az Intézmény 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 az informatikai szakterület 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 Jogi Iroda vagy az informatikai szakterület 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. Az adatkezelési megbízott feladatai az adatkezelés során

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 az adatkezelő vagy harmadik személy jogos érdeke, illetve közérdekű feladat vagy közfeladat ellátása jogalapon (ideértve az említett jogalapokon alapuló profilalkotást is) történő adatkezeléssel szembeni tiltakozási jogra, és hogy az erről szóló tájékoztatást egyértelműen és más információtól elkülönítve jelenítsék meg [GDPR 21. cikk (4) bek.];
    e/ rendszeres időközönként, de legalább évente áttekinti az adatvédelmi hatásvizsgálatban azonosított kockázatok alakulását, szükség esetén dokumentálja, illetve jelzi az adatvédelmi tisztviselőnek az adatkezeléssel járó kockázatok változását és az azok csökkentését célzó intézkedéseket, elvégzi, illetve közreműködik az adatvédelmi hatásvizsgálatok utóellenőrzésében és annak dokumentálásában [GDPR 35. cikk (11) bek.].

46. Az adatkezelés során (informatikai rendszerben kezelt adatok esetén az informatikai rendszer üzemeltetési szakaszában) az informatikai szakterület adatkezelési megbízottja(i) – a feladatkörükbe tartozó kérdésekben – gondoskodnak arról, hogy az adatkezelés általános adatbiztonsági kontrolljainak működtetése az erre vonatkozó eljárásrendeknek és az informatikai szakterület által meghatározott elvárásoknak megfelelően történjék, ezen belül gondoskodva különösen
    a/ a fizikai és logikai hozzáférés-védelem kontrolljairól,
    b/ a rendkívüli esemény-kezelési eljárásokról (adatvédelmi incidensek feladatkörükbe tartozó kezelése, kedvezőtlen külső vagy belső behatásokkal szembeni ellenállási képesség biztosítása),
    c/ jogosultságkezelésről és
    d/ az adatminőséggel, illetve adatrejtéssel kapcsolatos intézkedések végrehajtásáról.

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. Adatkezelés megszüntetésével kapcsolatos feladatok

48. Amennyiben a kezelt adatokra a továbbiakban nincs szükség (az adatkezelési cél megvalósult vagy a kezelt adatokra vonatkozó megőrzési idő letelt), 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 Jogi Iroda és az informatikai szakterület véleményének kikérése után – javaslatot tesz a döntésre jogosultnak:
    a/ az adatkezelés egészének vagy egyes adatfajták nyilvántartásának megszüntetésére (az adatok archiválására a megőrzési 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 –
        ca/ az informatikai rendszerekben archiválni kell, illetve
        cb/ az informatikai rendszerekből törölni kell, a papír alapú nyilvántartásban kezelt adatokat pedig – az Intézmény iratkezelési szabályzatáról szóló főigazgatói utasítás szerint – selejtezni kell.

5.4. Az érdekmérlegelési teszt elvégzésének módszertana

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

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 a mérlegelés során.

53. Az érdekmérlegelési teszt részei:
    a/ a tervezett adatkezelés leírása és az annak keretében kezelni tervezett személyes adatok (körének vagy típusának) 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/ a személyes adatok védelme 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 adatvédelmi hatásvizsgálatot kell végezni. Olyan, egymással hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló kockázatokkal járnak, 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 ad/ alpontja szerinti módon. A hatásvizsgálat megállapításait írásban kell rögzíteni. Az elkészült hatásvizsgálati dokumentációt az adatvédelmi tisztviselőnek kell megküldeni, amely azt 8 munkanapon belül szakmai szempontból véleményezi és beszerzi az információbiztonsági szakterület véleményét is. Ha az adatkezelési megbízott úgy ítéli meg, hogy az adatkezelés nem jár magas kockázattal a természetes személyek jogaira, úgy ezt meg kell indokolnia és – ha ez lehetséges – 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 (jogait) 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 közös adatkezelő vagy 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 dokumentáltan felül kell vizsgálni, szükség esetén újra el kell végezni.

6. AZ ÉRINTETTI JOGOK GYAKORLÁSÁNAK ELŐSEGÍTÉSE

6.1. Az adatkezelési tevékenység nyilvánossága

66. Az Intézmény a honlapján egy olyan, „Adatvédelem" nevű oldalt tart fenn, amely bármely oldalról közvetlenül elérhető. Az „Adatvédelem" oldalon közzé kell tenni:
    a/ az Intézmény adatvédelmi politikáját;
    b/ az Intézmény általános adatkezelési tájékoztatóját;
    c/ az Intézmény egyes adatkezelési tevékenységeihez kapcsolódó (különös) adatkezelési tájékoztatókat, 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);
    f/ tájékoztatást az e-Papír szolgáltatásról, az Intézmény Hivatali Kapu elérhetőségéről, valamint arról, hogy az Intézmény milyen típusú adatvédelmi beadványokat fogad az e-Papír szolgáltatás útján.

67. Az Intézmény 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 Intézmény az Országos Kórházi Főigazgatóság megbízásából kidolgozott mintadokumentumok (pl. adatkezelési tájékoztató, hozzájáruló nyilatkozat) Intézményre adaptált változatát alkalmazza a tevékenysége során.

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

70. Az Intézmény kezelésében lévő közérdekű adatok és közérdekből nyilvános adatok közzétételéről, illetve rendelkezésre bocsátásáról külön szabályzat rendelkezik.

6.2. A gyermekek tájékoztatáshoz való jogának biztosítása

71. Az Intézmény szervezeti egységeinek vezetői az adatkezelési megbízottak közreműködésével gondoskodnak arról, hogy az Intézményben 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 kapcsolatba lépő munkavállaló 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 kapcsolatba lépő munkavállaló – 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 kapcsolatba lépő munkavállaló írásban közvetlenül a gyermeket is tájékoztatja az adatkezelésről. A speciális, gyermekeknek szóló tájékoztató dokumentumot az adatvédelmi tisztviselő készíti el az Intézmény 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 Intézmény szervezeti egységeinek vezetői az adatkezelési megbízottak közreműködésével gondoskodnak arról, hogy az Intézményben 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 gondnoksága alatt álló érintettel.

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

73. Az Intézmény szervezeti egységeinek vezetői az adatkezelési megbízottak közreműködésével gondoskodnak arról, hogy az Intézményben 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 Intézmény szervezeti egységeinek vezetői az adatkezelési megbízottak közreműködésével gondoskodnak arról, hogy az Intézményben 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 Intézmény általi kezelését érintő beadványok érkezhetnek:
    a/ bejelentheti az Intézmény által nyilvántartott adatok megváltozását;
    b/ tájékoztatást kérhet személyes adatai [milyen személyes adato(ka)t, milyen célból, milyen jogalapon, milyen forrásból szerezve, meddig kezeli az Intézmény, alkalmaz-e automatizált döntéshozatalt és/vagy profilalkotást az adatkezelés során, és a személyes adatokat kinek, milyen jogalapon továbbítja)] – hozzáféréshez való jog (GDPR 15. cikk);
    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 Intézmény rendelkezésére bocsátott és elektronikus adatbázisban, a hozzájárulása, a személyes adatok különleges kategóriái esetén a kifejezett hozzájárulása, vagy a vele kötött szerződés teljesítéséhez szükséges jogalapon automatizált módon kezelt adatait 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 jogai 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 elintézése

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 Intézményhez érkező, a 78. pontban meghatározott beadványokat az Intézmény Betegjogi, betegadatok és betegbiztonság védelmének intézeti szabályzatában 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 panasz kezelését végző személy vagy 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 – az informatikai szakterület 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, a 81. pont szerinti eset kivételével meg kell megkísérelni a beadványozó személyének azonosítását, beleértve a személyes megjelenés igénylését, vagy az e-Papír szolgáltatás igénybevételének ajánlását. 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 81. pont szerinti eset kivételével, illetve 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 nem biztonságos elektronikus úton. A kapcsolatfelvételre olyan időben kell sort keríteni, hogy a beadványt akkor is meg lehessen válaszolni a határidő betartásával, ha a beadványozó ragaszkodik a nem biztonságos elektronikus úthoz vagy még nincs Ügyfélkapu regisztrációja;

i/ a 81. pont szerint eset kivételével 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 Intézmény 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 Intézmény 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. Ha az Intézmény rendelkezik hivatali tárhellyel (Hivatali Kapu), akkor az általános célú elektronikus kérelem űrlap (e-Papír) szolgáltatás igénybevételével az Intézménynek címzett adatvédelmi beadvány feladója azonosítottnak tekintendő, részére (értesítési tárhelyére) a válasz elektronikus úton megküldhető.

82. Az adatvédelmi beadványokról olyan ügyiratnyilvántartást 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

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

84. Az Intézmény működése során betartandó adatbiztonsági szabályokat (GDPR 32. cikk) külön szabályzatok tartalmazzák, így különösen a mindenkor hatályos
    a/ Informatikai Biztonsági Szabályzat,
    b/ Katasztrófavédelmi terv,
    c/ Létfontosságú rendszerelemek üzemeltetési biztonsági terve.

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

86. 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.

87. Az adatbiztonság elveinek egy adatkezelés bevezetésének (lsd. 32. pont) vagy személyes adatkezelést és/vagy -feldolgozást eredményező módosításának előkészítése során történő érvényesítése az informatikai szakterület adatkezelési megbízottjának (megbízottjainak) feladata, aki(ke)t az adatkezelési tevékenységet támogató nyilvántartási rendszerek kifejlesztésének, módosításának folyamatába kötelezően be kell vonni (lsd. 0. pont).

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

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

9.1. Közös adatkezelés

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

90. A közös adatkezelésről szóló megállapodásban meg kell határozni különösen

a/ az adatkezelés célját, a kezelendő adatok körét, az adatkezelés időtartamát, az alkalmazandó adatbiztonsági intézkedéseket, az adatkezelés egyéb feltételeit,
b/ azt, hogy a közös adatkezelésben érintett egyes adatkezelők
ba/ mely adatkezelési műveleteket (pl. hozzájáruló nyilatkozatok felvétele, adatok tárolása, adatok felhasználása stb.) végzik,
bb/ az érintett tájékoztatását hogyan végzik (pl. melyik adatkezelő készíti el az adatkezelési tájékoztatót és bocsátja az érintettek rendelkezésére stb.),
bc/ az érintett jogai gyakorlását hogyan biztosítják (pl. egyesített vagy elkülönített ügyfélszolgálat stb.),
bd/ az esetleges jogellenes adatkezelés következményeit milyen arányban viselik;
c/ az adatvédelmi incidens észlelése esetén követendő eljárást, különösen azt, hogy
ca/ az adatvédelmi incidens tudomásra jutása esetén a másik adatkezelő adatvédelmi tisztviselőjét (adatvédelmi tisztviselő hiányában a kijelölt kapcsolattartót) haladéktalanul kötelesek értesíteni az adatvédelmi rendellenességről vagy incidensről,
cb/ egymással kötelesek együttműködni az adatvédelmi rendellenesség vagy incidens okának kiderítésében és következményeinek felszámolásában,
cc/ az egyes adatkezelőket mely adatvédelmi incidensek tekintetében terheli a bejelentési kötelezettség;
d/ kijelölnek-e kapcsolattartót az érintettek számára, és ha igen, a kapcsolattartó személyét és elérhetőségét naprakészen kell tartani,
e/ a megállapodásról az érintett rendelkezésére bocsátandó összefoglalót, aminek – a GDPR 13-14. cikkeiben írtakon túl – tartalmaznia kell az adatkezelők által végzett adatkezelési műveleteket, és azt, hogy az érintett hogyan gyakorolhatja jogait a közös adatkezelés tekintetében.

91. A közös adatkezelés szükségességét az adatkezelési megbízott az adatkezelés bevezetéséről való döntés előkészítése részeként [36. pont af/ alpont] vizsgálja meg.

92. 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.

93. Amennyiben döntés születik a közös adatkezelés bevezetéséről, az illetékes adatkezelési megbízott(ak) az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő, az egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a Jogi Iroda közreműködésével, továbbá az informatikai szakterület 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.

94. A 93. pont alkalmazásában a szerződés megkötésére jogosult személy az, aki – az Intézmény 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.

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

9.2. Adatfeldolgozói szerződések

96. 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.

97. Adatfeldolgozó igénybevétele esetén az adatfeldolgozóval kötendő szerződésnek tartalmaznia kell a GDPR 28. cikk (1)-(4) bekezdésében foglalt tartalmi elemeket a 98. pontban foglalt kiegészítések és pontosítások szerint.

98. 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 Intézmény által alkalmazott adatbiztonsági intézkedések, és az adatfeldolgozónak az adatbiztonsági intézkedések végrehajtásával kapcsolatos feladatait;
    b/ rögzíteni kell az adatfeldolgozónak az érintettől származó kérelmek, panaszok megválaszolásában való közreműködésének eljárásrendjét;
    c/ rögzíteni kell az adatfeldolgozó kötelezettségeit adatvédelmi incidens észlelése esetén, így különösen
        ca/ az adatvédelmi incidens tudomásra jutása esetén az Intézmény adatvédelmi tisztviselőjét haladéktalanul köteles értesíteni az adatvédelmi incidensről,
        cb/ köteles együttműködni az Intézmény adatvédelmi tisztviselőjével és más közreműködő szervezeti egységgel az adatvédelmi incidens okának feltárásban és következményeinek felszámolásában,
        cc/ 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.

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

100. Az adatbiztonsági intézkedések technikai megfelelőségének megítélése az informatikai szakterület 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.

101. 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 Jogi Iroda közreműködésével, továbbá az informatikai szakterület véleményének kikérésével előkészíti az adatfeldolgozóval kötendő szerződés tervezetét és azt felterjeszti a szerződés megkötésére a 94. pont szerint jogosult személynek.

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

103. A 97.-102. 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 Jogi Iroda, továbbá az informatikai szakterület véleményét is.

10. AZ ADATKEZELÉSI NYILVÁNTARTÁS

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

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

106. Az Intézmény adatvédelmi tisztviselője az Adatkezelési Nyilvántartásba való betekintést – a Hatóság képviselőin kívül – az Intézmény érintett szakterületei, továbbá a közös adatkezelést érintő rész tekintetében a közös adatkezelő részére biztosítja.

107. A nyilvántartási célú adatállományt kezelő szervezeti egység vezetője az új adatállomány kialakítását a tevékenység megkezdése előtt 5 munkanappal bejelenti az adatvédelmi tisztviselőnek, aki azt Adatkezelési Nyilvántartásba bejegyzi.

108. Az Adatkezelési Nyilvántartásba bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelésért felelős szervezeti egység vezetője 5 munkanapon belül köteles bejelenteni az adatvédelmi tisztviselőnek, aki ennek megfelelően módosítja az Adatkezelési Nyilvántartás adatait.

109. Az Adatkezelési Nyilvántartással összefüggésben az adatvédelmi tisztviselő:
   a/ biztosítja, hogy az adatkezelések bevezetését megelőző döntéselőkészítés során az érintett szakterületek az adatkezelési tevékenységek nyilvántartása adatait megismerhessék a felesleges, párhuzamos adatkezelések elkerülése, illetve az új adatkezelésnek a meglévő adatkezelésekhez való illeszkedése érdekében;
   b/ ellenőrzi az adatkezelések, közös adatkezelők, illetve adatfeldolgozók adatainak az Adatkezelési Nyilvántartásba történő rögzítését és jelzi az adatkezelésért felelős szervezeti egység vezetőjének a hiányos, hibás vagy valószínűleg megváltozott adatokat, információkat;
   c/ a Jogi Irodával együttműködve figyelemmel kíséri az adatkezelést érintő jogszabályok változását és a szükséges módosításokra felhívja az adatkezelési megbízottak figyelmét;
   d/ az adatvédelmi felügyeleti hatóság megkeresésére adatot szolgáltat az Adatkezelési Nyilvántartásból.

11. AZ ADATVÉDELMI INCIDENSEK KEZELÉSE

11.1. Az adatvédelmi incidens minősítése

110. Adatvédelmi incidens csak akkor következik be, ha az adatbiztonsági intézkedések [0. 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 bizalmas jellegének sérülését eredményezheti;

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

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

112. Az elektronikus információs rendszereket érintő (biztonsági vagy egyéb) események adatvédelmi incidensnek is minősülnek, amennyiben személyes adatokra nézve következik be. A jelen Szabályzat adatvédelmi incidens kezelésére vonatkozó rendelkezéseinek alkalmazása nem mentesít az elektronikus információs rendszereket 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. Az adatvédelmi incidens bejelentése

113. Az a munkavállaló, aki az Intézmény által kezelt vagy feldolgozott személyes adatokkal kapcsolatban, vagy az Intézmény szerződéses partnere által kezelt vagy feldolgozott személyes adataival kapcsolatban adatvédelmi incidenst vagy annak gyanúját észleli, köteles azt haladéktalanul bejelenteni a szervezeti egység vezetőjének és az adatvédelmi tisztviselőnek e-mail-en vagy az intraneten erre a célra létrehozott űrlapot kitölteni. Az előbbieken túli egyéb bejelentő az Intézmény elektronikus elérhetőségén vagy az Intézmény honlapján elérhető űrlap kitöltésével jelentheti be az adatvédelmi incidenst.

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

115. 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.

116. 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 adatvédelmi tisztviselőt a 113. pontban meghatározott elérhetőségen köteles haladéktalanul, de legkésőbb az észlelést követő 24 órán belül értesíteni. A szerződésnek tartalmaznia kell továbbá a közös adatkezelő, illetve az adatfeldolgozó kötelezettségeit adatvédelmi incidens bejelentésében és kivizsgálásában [lsd. 98. c/ pont].

11.3. Incidensprotokoll általában

117. Az informatikai szakterület bevonásával a riasztásokban szereplő sérülékenység elhárításakor a következők szerint kell eljárni:
   a/ figyelembe kell venni a különböző informatikai biztonsági szabályozásokban a sérülékenységek elhárítására vonatkozó rendelkezéseket;
   b/ amennyiben a riasztás személyes adatot tartalmazó alkalmazás sérülékenységével kapcsolatban keletkezett, az adatvédelmi tisztviselőt haladéktalanul tájékoztatni kell;
   c/ amennyiben az Intézmény rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt azzal az eszközzel azonnal el kell kezdeni;

d/ ha az Intézmény – a mindenkor hatályos Informatikai Biztonsági Szabályzatában, továbbá a Katasztrófavédelmi tervben és a Létfontosságú rendszerelemek üzemeltetői biztonsági tervében foglaltakkal összhangban – nem rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt manuális módon kell azonnal elkezdeni;

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

118. A nem papíralapon kezelt adattal kapcsolatos incidensek kezelésére az Intézmény mindenkor hatályos Informatikai Biztonsági Szabályzatában, továbbá a Katasztrófavédelmi tervben és a Létfontosságú rendszerelemek üzemeltetői biztonsági tervében 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 Intézmény 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

119. Adatvédelmi incidens (papíralapú és nem papíralapú adatokra vonatkozóak egyaránt) felmerülése esetén az Intézmény adatvédelmi tisztviselője a Jogi Iroda és az informatikai szakterület kijelölt munkatársának (a továbbiakban együtt: incidensvizsgáló bizottság) közreműködésével megvizsgálja, és a 110. 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.

120. 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 (ide nem értve a főigazgatót).

121. Az adatvédelmi incidensről az adatvédelmi tisztviselő értesíti az Intézmény főigazgatóját, a főigazgató-helyetteseket, az igazgatókat és – szükség esetén – az Intézmény igazgatásszervezési referensét.

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

123. 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 a Katasztrófavédelmi tervben és a Létfontosságú rendszerelemek üzemeltetői biztonsági tervében vagy a Vagyonvédelmi Szabályzatban foglaltak szerint kell folytatni.

124. 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, valamint arról, hogy szükséges-e az incidens részletes vizsgálata:
   a/ az Intézmény főigazgatóját;
   b/ Jogi Iroda vezetőjét;
   c/ informatikai rendszert is érintő incidens esetén az informatikai szakterület vezetőjét;
   d/ a szakmailag illetékes szervezeti egység vezetőjét;
   e/ az igazgatásszervezési referenst.

125. 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 124. pontban meghatározott egyéb személyeket.

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

127. 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.

128. 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.

129. Az incidensvizsgáló bizottság a részletes vizsgálat megállapításairól, illetve a javasolt intézkedésekről a részletes vizsgálat befejezését követő 2 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.

130. A részletes vizsgálatról szóló jelentést a 124. pont a/-d/ alpontjában említett vezetőknek kell megküldeni.

131. 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.

132. 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 részére.

133. 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.

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

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 Intézmény megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
   b/ az Intézmény az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, 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 Intézmény főigazgatójának döntése alapján az Intézmény az érintetteket az Intézmény honlapján vagy országos lefedettségű sajtótermékben közzétett hirdetmény útján is értesítheti.

11.6. Az adatvédelmi incidens bejelentése a Hatóságnak

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 Intézmény 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 132. pont szerinti jóváhagyás után haladéktalanul) részletekben is közölhetők.

11.7. Az adatvédelmi incidensek nyilvántartása

143. Az adatvédelmi incidensekről az adatvédelmi tisztviselő elektronikus nyilvántartást vezet.

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 észlelésének és tudomásszerzésének időpontját,
   d/ az adatvédelmi incidens körülményeit, hatásait,
   e/ az adatvédelmi incidens elhárítására megtett intézkedéseket,
   f/ az adatvédelmi incidenssel kapcsolatban adott tájékoztatások adatait.

145. Az Intézmény 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 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.

147. Az adatvédelmi tisztviselő – szükség esetén a Jogi Iroda és az informatikai szakterület 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 Intézmény 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 adatkezelésért felelős szervezeti egység ellenőrzésére sor kerüljön. Az éves ellenőrzési tervet legkésőbb adott év február 28. napjáig kell elkészíteni és az Intézmény főigazgatója részére bemutatni.

150. Az éves ellenőrzési tervet az Intézmény 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 – az adatvédelmi tisztviselő által javasolt időponthoz képest 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, továbbá a 152. pont szerinti tevékenység során rögzített tényeket, megállapításokat, információkat 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, valamint az adatvédelmi tisztviselő megállapításait. A vizsgálati jelentés tervezetére a szervezeti egység vezetője 10 napon belül észrevételt tehet. Az észrevételek közlésének elmaradását úgy kell tekinteni, hogy a szervezeti egység vezetője a vizsgálati jelentés megállapításait elfogadja.

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 adatvédelmi tisztviselő javaslata alapján megtett intézkedésekről a szervezeti egység vezetője tájékoztatja az adatvédelmi tisztviselőt. Az adatvédelmi tisztviselő a megtett intézkedéseket, illetve azok betartását bármikor jogosult ellenőrizni (utóellenőrzés). Az utóellenőrzésre a 151-154. pontban foglaltakat alkalmazni kell.

156. Az adatvédelmi tisztviselő rendkívüli ellenőrzést is lefolytathat, ha adatvédelmi szempontból indokolt, különösen, ha a személyesadat-kezeléssel érintettek száma jelentős. Rendkívüli ellenőrzésnek minősül az éves ellenőrzési tervben nem szereplő ellenőrzés. A rendkívüli ellenőrzést az Intézmény főigazgatója előzetesen engedélyezi. A rendkívüli ellenőrzésre a 152-154. pont rendelkezéseit is alkalmazni kell.

157. Az adatvédelmi tisztviselő az adatvédelmi ellenőrzés (ideértve a 155. pont szerinti utóellenőrzést is) lefolytatását követően tájékoztatja az Intézmény főigazgatóját az adatvédelmi ellenőrzés adatairól és eredményeiről. A főigazgató tájékoztatása történhet szóban vagy a 154. pont szerinti, a vizsgált szervezeti egység vezetője által elfogadott vizsgálati jelentés megküldésével is. Az adatvédelmi tisztviselő jelen Szabályzat 30.i/ pont szerinti, az Intézmény adatvédelmi helyzetéről szóló éves jelentése tartalmazza az adott évben lefolytatott adatvédelmi ellenőrzésekkel és utóellenőrzésekkel kapcsolatos összegző információkat és megállapításokat is.

14. ZÁRÓ RENDELKEZÉSEK

158. Jelen Szabályzat a kiadásáról szóló főigazgatói utasítás aláírását követő napon lép hatályba.

159. Jelen Szabályzat hatálybalépésével visszavonom a Jahn Ferenc Kórház és Rendelőintézet Intézeti Adatainak Védelme és a Kezelt Egészségügyi-, valamint Személyes Adatok Integrált Kockázatkezelésének Szabályzatát (továbbiakban: Adatvédelmi és kockázatkezelési szabályzat) a következő részek kivételével:
   a/ a III/I. alfejezet 4. pont;
   b/ a III/I-1. alfejezet „Adatbiztonság" cím alatti része (18-20. oldal);
   c/ a III/I-1. alfejezet „Az Intézet adatkezelési rendszerének biztonságvédelmi előírásai" cím alatti részéből „Az adatkezelési rendszer karbantartásának szabályozása", „Az adatkezelési rendszer dokumentálására vonatkozó szabályok", „Az adatkezelési rendszer megváltoztatásának szabályai" és „Az adatkezelők, adatfeldolgozók munkavégzése során felmerülő adatvédelmi kérdések" alcímeiből az adatbiztonsági rendelkezések;
   d/ a III/I-4. alfejezet;
   e/ a III/II. alfejezet;
   f/ az V-IX. fejezet;
   g/ az a/-f/ pont alatt említett rendelkezésekhez kapcsolódó mellékletek.

160. Az Adatvédelmi és kockázatkezelési szabályzatnak a 159. pont a/-e/ alpontjaiban említett rendelkezéseit és a az említett rendelkezésekhez kapcsolódó mellékleteket 2021. .....-ig felül kell vizsgálni és az Informatikai Biztonsági Szabályzatba kell beilleszteni

161. Az Adatvédelmi és kockázatkezelési szabályzatnak a 159. pont d/ alpontjában említett rendelkezéseit 2021. .....-ig felül kell vizsgálni, és
   a/ a GDPR 13-14. cikke szerinti kérdéseket érintő rendelkezéseket az Intézmény adatkezelési tájékoztatójába, illetve adatkezelési tájékoztatóiba kell beilleszteni és – amennyiben alkalmazandó – a jelen Szabályzat 6.1. fejezetének megfelelően közzé kell tenni;
   b/ az adatkezelés feltételeit tartalmazó rendelkezéseket a jelen Szabályzat 32. pontja szerinti tartalommal és formában újra kiadni.

162. Az Adatvédelmi és kockázatkezelési szabályzatnak a 159. pont f/ alpontjában említett rendelkezéseit 2021. .....-ig felül kell vizsgálni, és jelen Szabályzat szervezeti és döntéshozatali rendjéhez kell igazítani.

ORSZÁGOS KÓRHÁZI FŐIGAZGATÓSÁG

WSH SZÁMÍTÁSTECHNIKAI, OKTATÓ ÉS SZOLGÁLTATÓ KFT

DAB-2-1/2024

Jahn Ferenc Dél-pesti Kórház és Rendelőintézet

hálózati biztonsági vizsgálati jelentés

Országos Kórházi Főigazgatóság Tudásközpont rendszer támogatás projekt

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
0.8	2021.01.07.	WSH Kft / SFÜI	sablon formátum
0.9	2021.02.21.	WSH Kft / SFÜI	vizsgálati eredmények rögzítése
1.0	2021.02.23.	WSH Kft / SFÜI	belső minőségbiztosítás

Tartalomjegyzék

1 Vezetői összefoglaló 4
1.1 Feltárt sérülékenységek és kockázatok összefoglalója 4
2 Módszertani összefoglaló 5
2.1 Vizsgálat hatóköre 5
2.2 Kockázati besorolások 5
2.3 Külső sérülékenységvizsgálat 6
3 Detektált szolgáltatások összefoglalója 7
4 Feltárt sérülékenységek 8
4.1 Magas kockázatú sérülékenységek 8
4.1.1 M1 – Elavult, nem támogatott operációs rendszerek 8
4.1.2 M2 - Sérülékeny kiszolgálói szoftver verziók 9
4.2 Közepes kockázatú sérülékenységek 10
4.2.1 K1 – Elavult vpn (pptp) szolgáltatás 10
4.2.2 K2 - Nyílt kommunikációs csatornák használata 11
4.2.3 K3 - Jelszavas hitelesítéssel elérhető ssh 12
4.2.4 K4 – SSH – engedélyezett gyenge titkosító algoritmusok 13
4.3 Alacsony kockázatú sérülékenységek 14
5 Mellékletek 15
5.1 Portfelderítés naplója 15
5.2 Automata sérülékenységvizsgálat eredménye 17
5.3 Hozzájáruló nyilatkozat 17

1 VEZETŐI ÖSSZEFOGLALÓ

Az Országos Kórházi Főigazgatóság (OKFŐ), mint megrendelő a „Tudásközpont rendszer támogatás" projekt keretében megbízta a WSH Kft.-t, hogy végezze el az intézmény internet felől elérhető informatikai rendszereinek biztonsági felmérését. A projekt célja a vizsgált rendszerben a sérülékenységek és biztonsági funkciók nem megfelelőségének feltárása, azok részletes dokumentálása és biztonságnövelő javaslatok kidolgozása.

A vizsgálat megállapította, hogy az intézmény informatikai rendszereinek internet felőli elérhetősége korlátozott, egészségügyi szakrendszerek közvetlen elérhetősége nem lehetséges, viszont két Linux szerver SSH szolgáltatása publikusan elérhető. Ezeken a szervereken lehetősége van a támadónak jelszavakat próbálgatva belépni, siker esetén közvetlenól elérheti ezeket a szervereket. Javasolt ezeken a szervereken az SSH konfigurációt megerősíteni, és a távoli hozzáférést korlátozni (pl. IP cím szűrés).

A menza rendszer (menza.delpestikorhaz.hu) kiszolgálója (Windows 2008R2) elavult, a gyártó már nem ad rá ki frissítéseket. Javasolt a kiszolgálót lecserélni gyártói támogatással rendelkező verzióra.

A további feltárt kockázatok frissítéssel, konfiguráció módosítással javíthatók.

A vizsgálat 2 magas és 4 közepes kockázatú sérülékenységet tárt fel.

1.1 Feltárt sérülékenységek és kockázatok összefoglalója

Az alábbi táblázatban összefoglaljuk és kategorizáljuk a feltárt sérülékenységeket.

Azonosító	Sérülékenység	Kockázati besorolás
M1	Elavult, nem támogatott operációs rendszerek	magas
M2	Sérülékeny kiszolgálói szoftver verziók	magas
K1	Elavult VPN (pptp) szolgáltatás	közepes
K2	Nyílt kommunikációs csatornák használata	közepes
K3	Jelszavas hitelesítéssel elérhető SSH	közepes
K4	SSH – engedélyezett gyenge titkosító algoritmusok	közepes

2 MÓDSZERTANI ÖSSZEFOGLALÓ

2.1 Vizsgálat hatóköre

A vizsgálat az alábbi ip címekre történt.

IP / IP tartomány/ Hoszt
84.206.67.8 - ftp.delpestikorhaz.hu,vpn.delpestikorhaz.hu,www.delpestikorhaz.hu,webmail.delpestikorhaz.hu, webmail.jahndelpest.hu
84.206.67.9 - menza.delpestikorhaz.hu
84.206.67.10
84.206.67.11
84.206.67.12
84.206.67.13
84.206.67.14
84.206.67.15

1. táblázat – vizsgálat hatóköre (scope)

2.2 Kockázati besorolások

A vizsgálatok során feltárt sérülékenységeket az OWASP Risk Rating Methodology[1] kategorizáljuk, amely szerint a kockázat a bekövetkezési valószínűség és a hatás szorzata.

Ez alapján a feltárt sérülékenységek kockázatát az alábbi három (+1) kategóriába soroljuk:

magas	Egy támadó a vizsgált rendszerben tárolt összes adathoz hozzáfér, vagy képes azokat vagy egy részét módosítani, vagy az adott rendszer elérhetőségét meggátolni. A javítást javasolt minél előbb elvégezni.
közepes	Egy támadó a vizsgált rendszerben részlegesen hozzáférhet az adatokhoz, vagy képes azok egy kis részét módosítani vagy az adott rendszer elérhetőségét kis mértékben befolyásolni.
alacsony	A vizsgált rendszerben tárolt adatokra nincs közvetlen hatással, de olyan implementálási, konfigurációs hibák, amelyek elősegíthetik a további támadásokat. Javításuk általában könnyen kivitelezhető.

[1] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

információ	A vizsgált rendszerben tárolt adatokra nincs hatással, de plusz információt jelenthetnek egy potenciális támadónak.

2.3 Külső sérülékenységvizsgálat

A külső vizsgálat az intézmény hálózatának internet felől történő (külső) informatikai biztonsági vizsgálata. A cél elsősorban a kívülről elérhető szolgáltatások felderítése, meghatározása belső technikai információk felhasználása nélkül (blackbox). Feladata a látható IP tartományok, szerverek, szolgáltatások felderítése és validálása, továbbá a felderített szolgáltatások biztonsági vizsgálata.

A vizsgálat az alábbi főbb lépésekből áll:

- hozzájáruló nyilatkozat ellenőrzése: scope validálása, hibás vagy hiányos kitöltések kiszűrése (hiba esetén a nyilatkozat újbóli bekérésére volt szükség).
- portfelderítés: a vizsgálat hatókörébe tartozó ip címekre teljes tcp (1-65535) és részleges (leggyakoribban használt) udp portok felderítése
- szolgáltatás beazonosítás: nyitott porton elérhető szolgáltatás típusának, kiszolgáló szoftver verziójának beazonosítása
- automata vulnerability scan: felfedezett szolgáltatásokra automata vulnerability scan futtatása Tenable Nessus Professional szoftverrel, szolgáltatások sérülékenységeinek ellenőrzése publikus sérülékenységi adatbázisok alapján
- manuális vizsgálatok: felfedezett szolgáltatásokra manuális módszerekkel és szükség szerint egyedi eszközökkel végezett vizsgálatok
- autentikáció tesztek: azonosítást, hitelesítést igénylő, illetve távoli hozzáférést biztosító szolgáltatások esetén alapértelmezett, gyári és leggyakoribb felhasználói adatokkal autentikáció tesztelés, illetve szolgáltatás beállítások ellenőrzése amennyiben lehetséges és releváns.
- dokumentálás

A vizsgálatok során exploitálás, a rendszerekbe történő, szoftver sérülékenységen keresztüli behatolás nem kerül végrehajtásra.

3 DETEKTÁLT SZOLGÁLTATÁSOK ÖSSZEFOGLALÓJA

Az alábbi táblázatban összefoglaljuk a vizsgálat során megvizsgált ip címeken elérhető szolgáltatásokat, azok beazonosított verzióit a szolgáltatás típusát és nevét.

IP / Hoszt	PORT	SZOLGÁLTATÁS TÍPUS	SZOLGÁLTATÁS NÉV
84.206.67.8	25/tcp	smtp – Postfix	levélküldés (smtp)
	80/tcp	http - Apache	web (http)
	110/tcp	pop3- Courier pop3d	levelezés (pop3)
	145/tcp	imap – (Courier Imapd (released 2011))	levelezés (imap)
	443/tcp	https – Apache	web (https) - Wordpress
	587/tcp	smtp – Postfix	levélküldés (smtp)
	1723/tcp	pptp – Mikrotik	vpn (pptp)
	8080/tcp	https - IIS httpd 8.5	web (https) - CareStream
	10722/tcp	ssh - OpenSSH 3.8.1p1 Debian 8.sarge.6	ssh
	34214/tcp	ssh - OpenSSH 3.8.1p1 Debian 8.sarge.6	ssh
84.206.67.9	80/tcp	http - Microsoft IIS httpd 7.5	web (http) - menü

2. táblázat – szolgáltatás áttekintő

4 FELTÁRT SÉRÜLÉKENYSÉGEK

4.1 Magas kockázatú sérülékenységek

A fejezet a vizsgálat során feltárt magas kockázatokat jelentő sérülékenységeket tartalmazza.

4.1.1 M1 – Elavult, nem támogatott operációs rendszerek

4.1.1.1 Találat leírása

A vizsgálat elavult operációs rendszereket talált (Windows 2008 R2).

Érintett rendszerek

- 84.206.67.9 (menza.delpestikorhaz.hu) Windows 2008R2 gyártói támogatása lejárt: 2020-01-14

4.1.1.2 Kockázat

A nem támogatott operációs rendszerekre a gyártó már nem ad ki biztonsági frissítéseket így a nyilvánosságra kerülő sérülékenységeken keresztül támadhatók az adott rendszerek, akár internet felől egy támadó jogosulatlanul hozzáférhet a rendszerbe.

4.1.1.3 Javaslatok

Cseréljék az elavult operációs rendszereket gyártó által támogatott verziókra.

4.1.1.4 Hivatkozások

https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-server-eos-faq/end-of-support-windows-server-2008-2008r2

4.1.2 M2 - Sérülékeny kiszolgálói szoftver verziók

4.1.2.1 Találat leírása

Az alábbi kiszolgálói szoftverek ismert sérülékenységeket tartalmaznak, mert a gyártó által kiadott hibajavítások nem kerültek telepítésre.

Érintett kiszolgálók és kiszolgálói szoftverek:

- 84.206.67.8 10722/tcp (ssh) OpenSSH (CVE-2006-4925, CVE-2006-5794, CVE-2007-0726, CVE-2007-4752, CVE-2007-2243) sérülékenységek
- 84.206.67.9 34214/tcp (ssh) OpenSSH (CVE-2006-4925, CVE-2006-5794, CVE-2007-0726, CVE-2007-4752, CVE-2007-2243) sérülékenységek

4.1.2.2 Kockázat

A frissítés nélküli sérülékeny kiszolgálói szoftvereket futtató kiszolgálók a sérülékenységeken keresztül támadható, akár internet felől egy támadó jogosulatlanul hozzáférhet a rendszerbe.

4.1.2.3 Javaslatok

Telepítsék az érintett kiszolgálói szoftverekre az elérhető biztonsági frissítéseket, vagy cseréljék a szoftvert a legfrissebb verzióra.

4.1.2.4 Hivatkozások

http://web.nvd.nist.gov/view/vuln/detail?vulnId= CVE-2006-4925

http://web.nvd.nist.gov/view/vuln/detail?vulnId= CVE-2006-5794

http://web.nvd.nist.gov/view/vuln/detail?vulnId= CVE-2007-0726

http://web.nvd.nist.gov/view/vuln/detail?vulnId= CVE-2007-4752

http://web.nvd.nist.gov/view/vuln/detail?vulnId= CVE-2007-2243

4.2 Közepes kockázatú sérülékenységek

A fejezet a vizsgálat során feltárt közepes kockázatokat jelentő sérülékenységeket tartalmazza.

4.2.1 K1 – Elavult VPN (pptp) szolgáltatás

4.2.1.1 Találat leírása

Az internet felől elérhető szolgáltatások között megtalálható a 1723/tcp porton a Microsoft pptp VPN szolgáltatás, amely már nem tekinthető biztonságos VPN megoldásnak.

Érintett szolgáltatás:

- 84.206.67.8 1723/tcp

4.2.1.2 Kockázatok

A PPTP protokoll titkosítási algoritmusa (128bit RC4) és autentikációs eljárásai (MSCHAP,MSCHAPv2) elavultak, így a pptp-n folyó kommunikáció lehallgatható, amely veszélyezteti a kommunikáció bizalmasságát

4.2.1.3 Javaslatok

PPTP helyett használjanak megfelelő védelemmel rendelkező VPN csatornát.

4.2.1.4 Hivatkozások

https://www.schneier.com/academic/pptp/faq/

4.2.2 K2 - Nyílt kommunikációs csatornák használata

4.2.2.1 Találat leírása

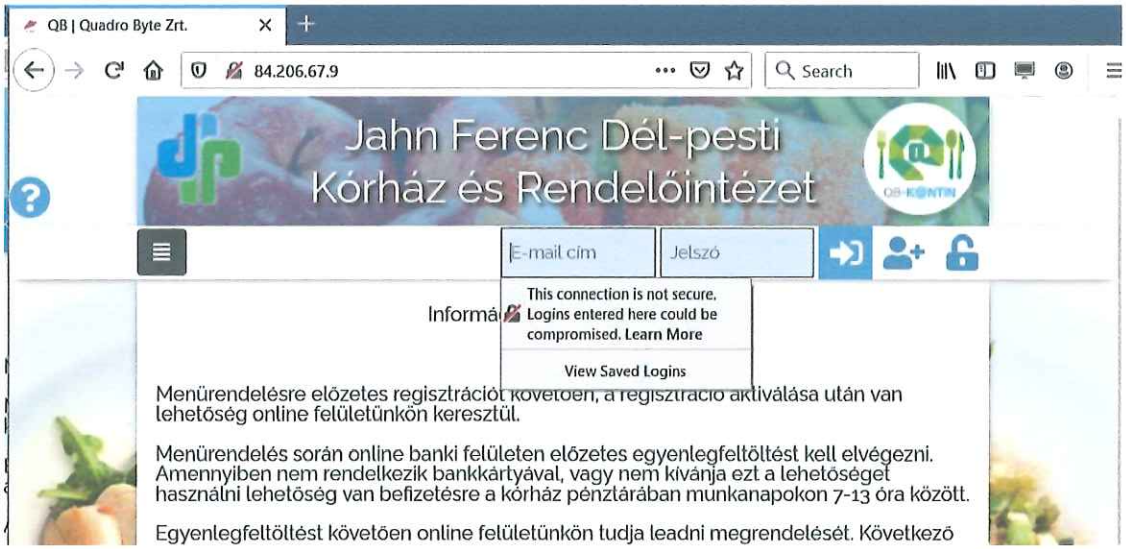
A vizsgált szolgáltatások egy része nyílt kommunikációt használ, nem alkalmaz kriptográfiai védelmet a kommunikációs csatornára.

Ilyen kommunikációk például: http, ftp, pop3, ftp

Érintett kiszolgálók és szolgáltatások:

- 84.206.67.8 110/tcp (pop3)
- 84.206.67.9 80/tcp (http webes menürendelés)

Az alábbi ábra a böngésző figyelmeztetését mutatja a nyílt kommunikációra vonatkozóan.



4.2.2.2 Kockázat

Rosszindulatú támadó lehallgathatja a kommunikációt, amelyből érzékeny adatokat (pl. jelszavakat) ismerhet meg.

4.2.2.3 Javaslatok

Vizsgálják át a nyílt kommunikációt használó szolgáltatásokat és törekedjenek azokat biztonságos csatornát használó szolgáltatásokra cserélni. Minden nyílt kommunikációnak van biztonságos alternatívája: ftp->ftps, http->https, pop3->pop3s, imap->imaps, stb.

4.2.2.4 Hivatkozások

https://cwe.mitre.org/data/definitions/319.html

4.2.3 K3 - Jelszavas hitelesítéssel elérhető SSH

4.2.3.1 Találat leírása

Az alábbi kiszolgálók esetében publikusan elérhető SSH szolgáltatás, amelyen engedélyezett jelszavas hitelesítés is.

Érintett kiszolgálók:

- 84.206.67.8 10722/tcp (ssh)
- 84.206.67.9 34214/tcp (ssh)

4.2.3.2 Kockázat

Rosszindulatú támadó jelszópróbálgatással (brute-force) közvetlen hozzáférést szerezhet a kiszolgáló Linux operációs rendszeréhez és ott akár magas privilégiumokat szerezve a teljes kiszolgáló felett átveheti az irányítást.

4.2.3.3 Javaslatok

Vizsgálják meg szükséges-e a nagy számú jelszavas SSH szolgáltatások elérése az internet felől, ha nem korlátozzák az elérhetőséget belső hálózatra.

Kapcsolják ki az SSH konfigurációban a jelszavas hitelesítést, helyette csak kulcsos hitelesítést engedélyezzenek.

4.2.3.4 Hivatkozások

https://help.ubuntu.com/community/SSH/OpenSSH/Configuring

4.2.4 K4 – SSH – engedélyezett gyenge titkosító algoritmusok

4.2.4.1 Találat leírása

Az alábbi kiszolgálókon található SSH szolgáltatás engedélyezi az alábbi gyenge titkosító algoritmusok használatát.

- 84.206.67.8 10722/tcp (ssh)
- 84.206.67.9 34214/tcp (ssh)

```
The following weak server-to-client encryption algorithms are supported :
  arcfour
The following weak client-to-server encryption algorithms are supported :
  arcfour
```

4.2.4.2 Kockázat

A gyenge kriptográfiai algoritmusok (pl. rc4) veszélyeztetik a kommunikáció bizalmasságát, lehallgatás esetén a nyílt adatok egyes esetekben visszafejthetők.

4.2.4.3 Javaslatok

- Konfigurálják az SSH beállításokat és tiltsák a jelzett gyenge titkosító algoritmusok használatát.

4.2.4.4 Hivatkozások

https://tools.ietf.org/html/rfc4253#section-6.3

4.3 Alacsony kockázatú sérülékenységek

A fejezet a vizsgálat során feltárt alacsony kockázatokat jelentő sérülékenységeket tartalmazza.

A vizsgálat nem állapított meg alacsony kockázatú sérülékenységet.

5 MELLÉKLETEK

5.1 Portfelderítés naplója

```
Nmap scan report for 84.206.67.8
Host is up (0.0043s latency).
Not shown: 65523 filtered ports
PORT    STATE SERVICE VERSION
25/tcp  open  smtp    Postfix smtpd
|_smtp-commands: mail.jahndelpest.hu, PIPELINING, SIZE 202400000, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
80/tcp  open  http    Apache httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
|_http-title: Did not follow redirect to https://www.delpestikorhaz.hu/
110/tcp open  pop3    Courier pop3d
|_pop3-capabilities: USER STLS IMPLEMENTATION(Courier Mail Server) TOP LOGIN-DELAY(10) PIPELINING UIDL
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US
| Issuer: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2016-12-10T18:28:05
| Not valid after:  2017-12-10T18:28:05
| MD5:   bc85 3103 35d4 62c8 cb8c 57fe fca6 254a
|_SHA-1: c0cf b18a 0b10 49ea 6dc2 f573 1e17 f161 bed1 e07a
|_ssl-date: TLS randomness does not represent time
143/tcp open  imap    Courier Imapd (released 2011)
|_imap-capabilities: STARTTLSA0001 CAPABILITY IDLE CHILDREN QUOTA ACL completed THREAD=REFERENCES ACL2=UNION SORT UIDPLUS
OK THREAD=ORDEREDSUBJECT IMAP4rev1 NAMESPACE
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US
| Issuer: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2016-12-10T18:27:56
| Not valid after:  2017-12-10T18:27:56
| MD5:   43c1 0418 6018 3a0f 0208 287d c277 e1ff
|_SHA-1: 9c5f a56e 8124 aebd a05c e762 b244 d729 7ac1 2dd1
|_ssl-date: TLS randomness does not represent time
443/tcp open  ssl/http Apache httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
|_http-title: Did not follow redirect to https://www.delpestikorhaz.hu/
| ssl-cert: Subject: commonName=www.delpestikorhaz.hu
| Subject Alternative Name: DNS:www.delpestikorhaz.hu, DNS:delpestikorhaz.hu
| Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo
Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-12-22T00:00:00
| Not valid after:  2021-12-22T23:59:59
| MD5:   7c77 8198 9749 06e0 48e3 593a 81ad 24fa
|_SHA-1: 6724 4da3 7d5e 95cd 0d7d c2cd 4765 5782 999d 6700
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
587/tcp open  smtp    Postfix smtpd
|_smtp-commands: smtp2.jahndelpest.hu, PIPELINING, SIZE 202400000, VRFY, ETRN, STARTTLS, AUTH PLAIN LOGIN,
ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=smtp2.jahndelpest.hu
| Subject Alternative Name: DNS:smtp2.jahndelpest.hu, DNS:www.smtp2.jahndelpest.hu
```

```
| Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-05-05T00:00:00
| Not valid after: 2022-05-05T23:59:59
| MD5: 6f06 c633 5c12 9395 02e7 0f8c a8df 7210
|_SHA-1: 01ae 1da2 9213 0d21 c9b1 f3bb 4a26 e351 be50 b982
|_ssl-date: 2021-02-10T04:37:09+00:00; -2m07s from scanner time.
1195/tcp closed rsf-1
1196/tcp closed netmagic
1723/tcp open pptp MikroTik (Firmware: 1)
8080/tcp open ssl/http Microsoft IIS httpd 8.5
|_http-favicon: Unknown favicon MD5: 1C4B2C10ACCCC48852D12EDDADAF7944
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Microsoft-IIS/8.5
| http-title: Browser Not Supported
|_Requested resource was /portal/BrowserNotSupported.aspx?ReturnUrl=%2fportal%2f
|_http-trane-info: Problem with XML parsing of /evox/about
| ssl-cert: Subject: commonName=delpestikorhaz.hu
| Subject Alternative Name: DNS:delpestikorhaz.hu, DNS:www.delpestikorhaz.hu
| Issuer: commonName=Let's Encrypt Authority X3/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-11-09T11:33:57
| Not valid after: 2021-02-07T11:33:57
| MD5: 42f7 5aef 3b62 a41b ad4f c6d8 5098 895b
|_SHA-1: ec3f 3173 9c43 6246 84ab 1cb2 2b81 f2ae e66c ca84
10722/tcp open ssh OpenSSH 3.8.1p1 Debian 8.sarge.6 (protocol 2.0)
| ssh-hostkey:
| 1024 d5:b8:5c:91:4c:27:46:31:76:b0:a1:35:b1:04:5c:8d (DSA)
|_ 1024 7f:32:56:86:87:a0:94:52:56:3d:e7:4a:5b:df:d8:86 (RSA)
34214/tcp open ssh OpenSSH 3.8.1p1 Debian 8.sarge.6 (protocol 2.0)
| ssh-hostkey:
| 1024 aa:52:fa:ca:28:91:e5:df:95:7a:88:85:99:aa:42:21 (DSA)
|_ 1024 30:61:c3:66:09:4c:1a:83:75:93:dc:43:b4:01:68:08 (RSA)
Service Info: Hosts: mail.jahndelpest.hu, smtp2.jahndelpest.hu, Del-Pest; OSs: Windows, Linux; CPE: cpe:/o:microsoft:windows, cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: -2m07s

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Feb 10 05:39:16 2021 -- 1 IP address (1 host up) scanned in 58805.68 seconds

Nmap scan report for 84.206.67.9
Host is up (0.0042s latency).
Not shown: 65527 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp Postfix smtpd
|_smtp-commands: mail.jahndelpest.hu, PIPELINING, SIZE 202400000, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
80/tcp open http Microsoft IIS httpd 7.5
|_http-favicon: Unknown favicon MD5: 0C7A4138C1D2A2C9A4465EFC9E37BE03
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Microsoft-IIS/7.5
|_http-title: QB | Quadro Byte Zrt.
110/tcp open pop3 Courier pop3d
|_pop3-capabilities: USER UIDL IMPLEMENTATION(Courier Mail Server) TOP PIPELINING STLS LOGIN-DELAY(10)
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US
| Issuer: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US
| Public Key type: rsa
| Public Key bits: 4096
```

```
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2016-12-10T18:28:05
| Not valid after:  2017-12-10T18:28:05
| MD5:   bc85 3103 35d4 62c8 cb8c 57fe fca6 254a
|_SHA-1: c0cf b18a 0b10 49ea 6dc2 f573 1e17 f161 bed1 e07a
|_ssl-date: TLS randomness does not represent time
143/tcp  open  imap    Courier Imapd (released 2011)
|_imap-capabilities: IMAP4rev1 completed CAPABILITY OK ACL2=UNION THREAD=REFERENCES STARTTLSA0001 SORT QUOTA CHILDREN
NAMESPACE ACL IDLE UIDPLUS THREAD=ORDEREDSUBJECT
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US
| Issuer: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2016-12-10T18:27:56
| Not valid after:  2017-12-10T18:27:56
| MD5:   43c1 0418 6018 3a0f 0208 287d c277 e1ff
|_SHA-1: 9c5f a56e 8124 aebd a05c e762 b244 d729 7ac1 2dd1
|_ssl-date: TLS randomness does not represent time
1195/tcp  closed rsf-1
1196/tcp  closed netmagic
10722/tcp open  ssh     OpenSSH 3.8.1p1 Debian 8.sarge.6 (protocol 2.0)
| ssh-hostkey:
|   1024 d5:b8:5c:91:4c:27:46:31:76:b0:a1:35:b1:04:5c:8d (DSA)
|_  1024 7f:32:56:86:87:a0:94:52:56:3d:e7:4a:5b:df:d8:86 (RSA)
34214/tcp open  ssh     OpenSSH 3.8.1p1 Debian 8.sarge.6 (protocol 2.0)
| ssh-hostkey:
|   1024 aa:52:fa:ca:28:91:e5:df:95:7a:88:85:99:aa:42:21 (DSA)
|_  1024 30:61:c3:66:09:4c:1a:83:75:93:dc:43:b4:01:68:08 (RSA)
Service Info: Host:  mail.jahndelpest.hu; OSs: Windows, Linux; CPE: cpe:/o:microsoft:windows, cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Feb 12 16:26:14 2021 -- 1 IP address (1 host up) scanned in 57754.51 seconds
```

5.2 Automata sérülékenységvizsgálat eredménye

A vizsgálat részeként lefuttatott Nessus automata sérülékenységvizsgáló eszköz kimenete pdf formátumban:

- OKFŐ_ JFDPKR_Hálózatbiztonsági vizsgálat jelentés_melléklet_v1.pdf

5.3 Hozzájáruló nyilatkozat

A vizsgálatot engedélyező hozzájáruló nyilatkozat tartalma:

JÓVÁHAGYÓ NYILATKOZAT

informatikai hálózati biztonsági vizsgálathoz

Alulírott Dr. Dobosi Zsolt Géza, mint az Jahn Ferenc Dél-pesti Kórház és Szakrendelő (székhely: 1204 Budapest Köves u. 1., adószám: 15491020-2-43) (a továbbiakban: „**Jóváhagyó**") képviselője,

a jelen Jóváhagyó nyilatkozat aláírásával igazoltan, feltétlenül és visszavonhatatlanul tudomásul veszem, hogy

az ÁEEK/44917-18/2020 számú szerződésre hivatkozva a WSH Számítástechnikai, Oktató és Szolgáltató Kft. (székhely: 1117 Budapest, Budafoki út 97. cégjegyzékszám: 01 09 461038, adószám: 12048898243 képviseli: Debrődy István) alvállalkozójaként a Dr. Suba Ferenc Ügyvédi Iroda (székhely: 1188 Budapest, Topáz u. 7.; adószáma: 18260230-2-43; képviseli: Dr. Suba Ferenc irodavezető ügyvéd) (a továbbiakban: „**Auditor**") és alvállalkozója a „Tudásközpont rendszer támogatása" projekt részeként informatikai hálózati biztonsági vizsgálatot (a továbbiakban: „**Vizsgálat**") végezzen az egészségügyi intézményben.

Jelen Jóváhagyó nyilatkozat időbeli hatálya
2021 (év). január (hónap) 6. (nap) 23:59 (óra:perc) - tól
2021 (év). február (hónap) 28. (nap) 23:59 (óra:perc)-ig tart.

A Vizsgálat az alábbi IP címeket, IP tartományokat domain neveket érinti:
(IP cím, IP tartomány, url, stb.):
https://delpestikorhaz.hu, https://menza.delpestikorhaz.hu, https://webmail.jahndelpest.hu/
https://www.delpestikorhaz.hu:8080/, 84.206.67.84.206.67.15 (NISZ IP)

Jelen Jóváhagyó nyilatkozat aláírásával a Jóváhagyó az Auditor által végzett informatikai biztonsági vizsgálatával kapcsolatban az alábbiakat elfogadja és tudomásul veszi:

1. Az Auditor szakemberei a Jelen Jóváhagyó nyilatkozat időbeli hatályánál megjelölt időszakban, a Jóváhagyó részére előzetesen rendelkezésre bocsátott, *ÁEEK_Informatikai hálózatbiztonsági vizsgálatok-műszaki leírás* dokumentum szerinti, a valós életre is jellemző információszerző és biztonsági hibákat kereső eszközökkel dolgoznak. A biztonsági vizsgálatok a Jóváhagyóval előzetesen egyeztetve és az ő jóváhagyásával egyidejűleg kerülnek végrehajtásra, így a Vizsgálat szabályos és rendeltetésszerű elvégzése esetén, ezzel kapcsolatosan – a további kikötéseket meghaladóan – a Jóváhagyó az Auditorral szemben semmilyen hátrányos jogkövetkezményt nem alkalmazhat, jogi lépéseket nem foganatosíthat, semmilyen követelést, illetőleg igényt nem érvényesíthet.

2. Jóváhagyó tudomásul veszi, hogy a Vizsgálatot a Auditor munkatársai, illetve szerződéses alvállalkozói és azok munkatársai (továbbiakban együttesen: az Auditor munkatársai) végzik el, akikre a jelen Jóváhagyó nyilatkozat hatálya – szerződésük alapján – kiterjed.

3. A Jóváhagyó biztosítja, hogy a kijelölt kapcsolattartókon keresztül e-mailben vagy telefonon előre egyeztetett időpontokban végzett Vizsgálatokat technikai módszerekkel szándékosan nem akadályozzák.

4. Az Auditor munkatársainak törekedni kell a károkozás elkerülésére, illetve minimalizálására, ennek érdekében az egyes lépéseknél szükség szerint folyamatos kapcsolatban kell állniuk a Jóváhagyó által kijelölt szakemberekkel.

5. Az Auditor köteles eljárása során mindent megtenni annak érdekében, hogy a Jóváhagyót károsodás ne érje. Az Auditor az általa szándékosan vagy súlyos gondatlansággal okozott károkért a Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.) szerinti kártérítési felelősséggel tartozik.

6. Jóváhagyó köteles a Vizsgálat megkezdése előtt az elektronikusan tárolt adataihoz kapcsolódó információbiztonsági védelmi igényét definiálni annak érdekében, hogy Auditor a vizsgálati tevékenysége során megfelelő védelmi szintet tudjon biztosítani számukra. Jóváhagyó köteles a Auditort teljeskörűen tájékoztatni a Vizsgálat tárgyát képező információs rendszer és benne tárolt adatok típusáról, minőségéről, illetve azok rendelkezésre állási követelményeikről (pl.: tesztelésre nem használható idősávokról).

7. Auditor értesíti Jóváhagyót, amennyiben üzleti titkot, magántitkot, levéltitkot, személyes adatokat, különleges adatokat tartalmazó információhoz, adathoz fér hozzá, illetőleg amennyiben ilyen adatok, információk a birtokába kerülnek, azokat tartalmuk részletes megismerése nélkül, a megszerzésre való utalás rögzítésével egyidejűleg a Vizsgálat befejezését követően jelentés mellékletként átad a Jóváhagyó részére. Auditor a Vizsgálat befejezését követően kizárólag a vizsgálati eredmény állományokat őrzi meg (log-ok), minden egyéb adatot (esetlegesen fájlok, dokumentumok, hozzáférések adatai stb.) biztonságos módon, véglegesen törlésre kerülnek. A jelen pontban meghatározott kötelezettségek, előírások megszegéséért Auditor a Ptk. szerinti kártérítési felelősséggel tartozik.

8. A Jóváhagyó kezelésében lévő személyes és különleges adatok tekintetében az Auditor – mint adatfeldolgozó – az Európai Parlament és Tanács (EU) 2016/679 rendeletének (általános adatvédelmi rendelet, GDPR) 82. cikk (2) bekezdése alapján csak abban az esetben tartozik felelősséggel az adatkezelés (a szerződés tárgyát képező tevékenységek) által okozott károkért, ha nem tartja be a hivatkozott rendeletben meghatározott, kifejezetten az adatfeldolgozókat terhelő kötelezettségeket, vagy ha az adatkezelő jogszerű utasításait figyelmen kívül hagyja vagy azokkal ellentétesen jár el. Az Auditor e körben kifejezetten kizárja a Jóváhagyó által alkalmazott adatbiztonsági intézkedések nem megfelelő volta, illetve hiányosságai miatt a szerződés tárgyát képező tevékenységek végzése közben bekövetkező adatvédelmi jogsértésekért, adatvédelmi incidensekért, valamint a vétlen adatvesztésekből eredő károkért való felelősséget.

9. Auditor elvárható gondossággal jár el annak érdekében, hogy a Jóváhagyó informatikai rendszeréből származó adat, információ ne jusson illetéktelen személyek tudomására sem az Auditor társaságán belül, sem azon kívül, ne váljon hozzáférhetővé vagy elérhetővé. A jelen pontban meghatározott kötelezettségek, előírások megszegéséért az Auditor a Ptk. szerinti kártérítési felelősséggel tartozik. Ha az elvárható gondosság betartása mellett a Jóváhagyót – nem a Jóváhagyó hibájából – károsodás éri, a Auditort kártérítési kötelezettség nem terheli. Auditort abban az esetben sem terheli felelősség, ha a Jóváhagyó nem, vagy nem megfelelően tesz eleget a jelen Jóváhagyó nyilatkozatban foglalt kötelezettségének.

Amennyiben Auditor a Vizsgálat során olyan adatok birtokába jut, amely az 7. pontban foglalt tájékoztatási kötelezettségen kívül esik, abban az esetben Auditor etikusan és jóhiszeműen jár el, és az így birtokába került adatokat rendszeréből – az adatok megismerése nélkül – biztonságos törlési eljárással véglegesen eltávolítja.

10. Az Auditor köteles mindent elkövetni annak érdekében, hogy tevékenysége során és annak eredményeképpen a Jóváhagyó informatikai rendszer(ek) működésében ne álljon be üzemzavar, fennakadás.

11. Az Auditor a vállalkozási szerződés, illetve a kapcsolódó iratok, megrendelés és egyéb dokumentáció, valamint Jóváhagyó írásbeli rendelkezései szerint köteles eljárni. Ha a Jóváhagyó célszerűtlen vagy szakszerűtlen utasítást ad, a Auditor köteles őt erre írásban figyelmeztetni. Ha a Jóváhagyó az utasításához e figyelmeztetés ellenére is írásban közölten ragaszkodik, az utasításból eredő károk őt terhelik. Amennyiben a Jóváhagyó utasításának megvalósítása bűncselekmény elkövetését jelentené, az Auditor jogosult és köteles ezen utasítás végrehajtásának megtagadására.

12. Amennyiben Jóváhagyót az Auditor olyan tevékenységéből eredően éri kár, amelyet a Jóváhagyó előzetesen jóváhagyott és az Auditor szakszerűen látott el, az Auditort kártérítési felelősség nem terheli, tekintettel az Auditori tevékenység megkezdését megelőző Jóváhagyó általi előzetes vizsgálatra és Jóváhagyó hozzájárulására.

13. Amennyiben a Jóváhagyót olyan kár éri, melyért az Auditor nem felelős, a Jóváhagyó kérése esetén az Auditor a műszaki és humán erőforrással a Jóváhagyó rendelkezésére áll a zavar elhárítása érdekében az Auditor üzletszabályzatában meghatározott eseti díjszabás szerinti ellenszolgáltatás fejében.

14. Auditor a sérülékenység vizsgálat felderítési szakaszának végén a felderített, vizsgálni kívánt informatikai erőforrások listáját validálásra visszamutatja a Jóváhagyó számára. A Jóváhagyó jóváhagyásáig az Auditor aktív vizsgálatokat nem végez az érintett rendszerek tekintetében.

15. Amennyiben az Auditor, illetve valamely részéről eljáró személy ellen a Vizsgálat elvégzése során tanúsított jogszerű magatartása miatt hatósági vagy szabálysértési, vagy büntető eljárás indul, a Jóváhagyó köteles teljeskörűen együttműködni a mentesítés során, valamennyi, a szankciók elkerüléséhez, minimalizálásához szükséges nyilatkozatot megtenni.

16. Jóváhagyó köteles beszerezni minden olyan hozzájárulást harmadik személyektől, amelyek nélkül jelen tevékenység nem lenne jogszerűen folytatható. Az ilyen nyilatkozat hiányából fakadó kárért a Jóváhagyó felelős.

17. Jóváhagyó kifejezetten hozzájárul a jelen jóváhagyó nyilatkozatban körülírt tevékenység elvégzéséhez.

Budapest, 2021 év .január hó 25 nap

.....

Dr. Dobosi Zsolt
Jóváhagyó
orvosigazgató
főigazgató általános helyettese

Szent Ferenc Dél-pesti Kórház és Rendelőintézet FŐIGAZGATÓ