PÉTEGISZ Járóbeteg Szakellátó Központ

4090 Polgár, Hősök útja 1.

ADATVÉDELMI SZABÁLYZAT

Érvénybelépés időpontja: 2024.05.27.

PÉTEGISZ
Járóbeteg Szakellátó Központ

Jóváhagyta:…….

Dr. Pásztor Ibolya főigazgató

Tartalom

1. A SZABÁLYZAT CÉLJA, HATÁLYA, ALAPELVEK

1.1. Bevezető rendelkezések

1. A PÉTEGISZ Járóbeteg Szakellátó Központ (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 (az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (a továbbiakban: Eüak.)) 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 Szabályzat Mu_SzE_0001_230416_Adatvédelmi Szabályzat 5/55 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.

1.2. A szabályzat célja

3. Jelen szabályzat az Intézmény kezelésében lévő személyes adatok tekintetében a legfontosabb adatvédelmi szabályokat tartalmazza, különös tekintettel a GDPR által az adatkezelővel szemben támasztott követelményekre és a GDPR III. fejezetében meghatározott érintetti jogok érvényesülésének biztosítására.

4. A Szabályzattal az Intézmény biztosítani kívánja a nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, meg kívánja akadályozni az adatokhoz való jogosulatlan hozzáférést, azok jogosulatlan megváltoztatását, illetve nyilvánosságra hozatalát.

5. Jelen szabályzatot az Intézmény egyéb – különösen az adatkezelés és adatbiztonság vonatkozásában rendelkezéseket tartalmazó – szabályzataival és eljárásrendjeivel összhangban kell értelmezni és alkalmazni. 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.

2. A SZABÁLYZAT HATÁLYA

2.1. A szabályzat személyi hatálya

6. Jelen Szabályzat személyi hatálya kiterjed az Intézmény irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek (a munkavégzésre irányuló jogviszony jellegétől függetlenül), továbbá azon természetes személyekre (a továbbiakban: érintett), akik személyes adatait a jelen Szabályzat hatálya alá tartozó adatkezelések tartalmazzák, továbbá azon érintettekre, akik jogait vagy jogos érdekeit az adatkezelés érinti. Az 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.

2.2. A szabályzat tárgyi hatálya

7. 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 6. 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.

2.3. A szabályzat szervezeti hatálya

Jelen szabályzat szervezeti hatálya kiterjed az Intézmény minden szervezeti egységére.

2.4. Dokumentálási kötelezettség

8. 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.

9. 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.

3. ALAPFOGALMAK

10. Jelen Szabályzat alkalmazása során a GDPR 4. cikkében és az Infotv. 3. § szerint az alábbi fogalmakat kell alkalmazni:

a) ***érintett***: bármely információ alapján azonosított vagy azonosítható természetes személy;

b) ***személyes adat***: az érintettre vonatkozó bármely információ;

c) ***különleges adat***: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok,

d) ***egészségügyi adat***: egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

e) ***genetikai adat***: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó

minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered;

f) ***biometrikus adat***: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat;

g) ***adatkezelő***: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

h) ***adatkezelés***: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj-vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

i) ***adatkezelésért felelős szervezeti egység***: az Intézmény azon szervezeti egysége, amelynek feladatkörébe tartozik az Intézmény kezelésében lévő valamely nyilvántartási rendszer létrehozása, fenntartása, illetve üzemeltetése,

j) ***közös adatkezelő***: az az adatkezelő, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - az adatkezelés céljait és eszközeit egy vagy több másik adatkezelővel közösen határozza meg, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket egy vagy több másik adatkezelővel közösen hozza meg és hajtja végre vagy hajtatja végre az adatfeldolgozóval

k) ***adatvédelmi felügyeleti hatóság***: a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság),

l) ***adattovábbítás***: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

m) ***nyilvánosságra hozatal***: az adat bárki számára történő hozzáférhetővé tétele;

n) ***adattörlés***: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

o) ***adatkezelés korlátozása***: a tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölése útján;

p) ***adatmegsemmisítés***: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;

q) ***adatfeldolgozás***: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége;

r) ***adatfeldolgozó***: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel - az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel;

s) ***adatfelelős***: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;

t) ***adatközlő***: az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatot honlapon közzéteszi;

u) ***adatállomány***: az egy nyilvántartásban kezelt adatok összessége;

v) ***harmadik személy***: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek;

w) ***EGT-állam***: az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez;

x) ***harmadik ország***: minden olyan állam, amely nem EGT-állam;

y) ***adatvédelmi hatásvizsgálat***: olyan vizsgálat, amelyet az adatkezelésért felelős szervezeti egység kijelölt munkavállalója (adatvédelmi 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,

z) ***adatvédelmi incidens***: az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

aa) *hozzájárulás*: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez; bb) *adatvédelmi tisztviselő*: az Intézmény szervezetében működő, a GDPR 39. cikkében meghatározott feladatokat az Intézmény jelen szabályzatában foglaltak szerint ellátó, az Intézménnyel foglalkoztatási jogviszonyban álló természetes személy,

cc) *álnevesítés (pszeudonimizálás)*: személyes adat olyan módon történő kezelése, amely - a személyes adattól elkülönítve tárolt - további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely érintettre vonatkozik, valamint műszaki és szervezési intézkedések megtételével biztosítja, hogy azt azonosított vagy azonosítható természetes személyhez ne lehessen kapcsolni;

dd) *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,

ee) *dolgozói személyes adat*: az Intézménnyel foglalkoztatási jogviszonyban álló személyek adata,

ff) *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,

gg) *Informatikai Osztály*: az informatikai rendszerek üzemeltetéséért, az informatikai biztonság ellátásáért felelős szervezeti egység vagy egységek, ideértve az Intézmény információbiztonsági felelősét is,

hh) *titkosítás*: az adatok olyan átalakítása, melynek során az adat értelmezhetetlenné válik a megfelelő kulcs ismerete nélkül,

ii) *törlés*: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása a továbbiakban már nem lehetséges. A törlés célja megvalósítható deperszonalizálással (anonimizálással),

jj) *ügyvitel*: az Intézmény tevékenységére vonatkozó jogszabályokban az Intézmény részére meghatározott közfeladatok ellátásával összefüggő eljárás.

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

4. AZ ADATKEZELÉS CÉLJAI

11. Az egészségügyi és személyazonosító adat kezelésének alapvető céljai az alábbiak:

- az egészség megőrzésének, javításának, fenntartásának előmozdítása,
- a betegellátó eredményes gyógykezelési tevékenységének elősegítése,
- az érintett egészségi állapotának nyomon követése,
- a népegészségügyi, közegészségügyi és járványügyi érdekből szükségessé váló intézkedések megtétele,
- a betegjogok érvényesítése.

12. A fenti célokon felül az Eüak. 4. § (2) bekezdésében foglalt célokból is kezelhető egészségügyi és személyazonosító adat.

13. Az Intézmény a gyógykezelés céljából történő adatkezelés során a jogszabályok maradéktalan betartása mellett elsősorban az orvosi titok megtartását, az érintett teljeskörű tájékoztatását és a gyógykezelés bizalmasságának elvét tartja szem előtt.

14. Az Intézmény közegészségügyi és járványügyi célból történő adatkezelése során a jogszabályokban előírt módon az egészségügyi államigazgatási szervnek végez adattovábbítást.

15. Az Intézmény népegészségügyi célból történő adatkezelése során a jogszabályokban előírt módon végez adattovábbítást a különböző országos regiszterek számára.

16. Az Intézmény a statisztikai célból történő adatkezelés során az érintettek egészségügyi adatait jellemzően csak személyazonosításra alkalmatlan módon kezeli. Ez alól kizárólag kifejezett jogszabályi rendelkezés esetén tesz kivételt.

17. Az Intézmény a tárolt egészségügyi és személyazonosító adatokba tudományos kutatás céljából történő betekintést csak a jogszabályi rendelkezések betartásával, ellenőrzött és nyilvántartott módon engedélyez és megköveteli, hogy tudományos közleményben ne szerepelhessenek egészségügyi és személyazonosító adatok oly módon, hogy az érintett személyazonossága megállapítható legyen. Tudományos kutatás során a tárolt adatokról nem készíthető személyazonosító adatokat is tartalmazó másolat.

18. Az Intézmény egészségügyi ellátóhálózaton kívüli szerv megkeresésére csak a jogszabályban meghatározott esetekben és módon végez adattovábbítást.

5. AZ ADATKEZELÉS JOGALAPJA

5.1. A jogalapra vonatkozó általános rendelkezések

Az adatkezelés jogalapját az Intézmény minden adatkezelési folyamatnál meghatározza. Az adatkezelésre jogalapot csak a GDPR 6. cikk (1) és 9. cikk (2) bekezdésekben rögzítettek szerint határoz meg az Intézmény. Az Intézmény az adatkezelési rendszerét úgy alakítja ki, hogy minden személyes adatra vonatkozóan bizonyítani tudja, hogy mikor, milyen formában történt a személyes adat felvétele és milyen tájékoztatást kapott az érintett a személyes adat felvételekor.

5.2. Az adatkezelés lehetséges jogalapjai személyes adatok esetében

19. Az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez.

20. Az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges.

21. Az adatkezelés az Intézmény vonatkozó jogi kötelezettség teljesítéséhez szükséges.

22. Az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges.

23. Az adatkezelés közérdekű vagy az Intézményre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.

24. Az adatkezelés az Intézmény vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

5.3. Körülmények, amelyek esetén az Intézmény személyes adatok különleges kategóriáiba tartozó adatokat kezelhet

25. Az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha az uniós vagy a hatályos magyar jog úgy rendelkezik, hogy az 5.1 pontban foglalt tilalom az érintett hozzájárulásával sem oldható fel.

26. Az adatkezelés az Intézménynek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy hatályos magyar jog lehetővé teszi.

27. Az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni.

28. Az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott.

29. Az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges.

30. Az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy a hatályos magyar jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.

31. Az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy hatályos magyar jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, amennyiben az adatkezelés adatok kezelése olyan szakember által vagy olyan szakember felelőssége mellett történik, akire szakmai titoktartási kötelezettség hatálya alatt áll.

32. Az adatkezelés a népegészségügy területét érintő közérdekből szükséges.

33. Az adatkezelés közérdekű archiválás, tudományos és történelmi kutatási vagy statisztikai célból szükséges olyan uniós vagy hatályos magyar jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.

5.4. A hozzájárulásra, mint jogalapra vonatkozó különleges szabályok

34. Amennyiben az adatkezelés az érintett hozzájárulásán alapszik, úgy az érintett a hozzájárulását bármilyen bizonyítható módon megadhatja, így írásban (nyilatkozaton, dokumentumon), szóban és ráutaló magatartással is. Az intézmény nem tesz különbséget a hozzájárulások között azok formáját tekintve, a hozzájárulások formái egyenértékűek, de fenntartja magának a jogot, hogy egyes adatkezelések esetén a hozzájárulás egyes formáit kizárja.

35. Az Intézmény minden adatkezelési folyamatát úgy határozza meg jelen szabályzat kiadásakor és minden, a későbbiekben bevezetendő adatkezelés esetén, hogy amennyiben annak jogalapja az érintett hozzájárulása, úgy képes legyen annak bizonyítására, hogy az érintett személyes adatainak kezeléséhez hozzájárult. Az Intézmény ennek úgy tesz eleget, hogy elsődlegesen nem írásban szerzi be az érintett hozzájárulását, hanem szóban (ráutaló magatartás által) és az írásbeliség esetén pedig amelyet így aláírt példánnyal tud igazolni.

36. Amennyiben az Intézmény a ráutaló magatartást vagy a szóbeliséget is elfogadja a hozzájárulás jogalapjául, úgy az adatkezelés minden körülményét megvizsgálja és dokumentálja, hogy utóbb is igazolni tudja a hozzájárulást.

37. Az Intézmény az adatkezelései során lehetőség szerint a személyes adatnál feltünteti, hogy a hozzájárulás mikor érkezett, milyen formában történt (írásban/szóban/ráutaló magatartással), milyen cselekmény eredménye, ha ez értelmezhető (például: feliratkozás/jelentkezés/kapcsolatfelvétel/stb.).

38. Az Intézmény biztosítja a jogot arra is, hogy az érintett ugyanúgy, ahogy a hozzájárulást megadta, a hozzájárulását visszavonja. A ráutaló magatartással megtett hozzájárulás visszavonását csak írásban fogadja el az Intézmény.

5.5. A szerződéses jogviszonyra, mint jogalapra vonatkozó különleges szabályok

39. Ha az adatkezelés jogalapja az Intézménnyel írásban kötött szerződés megkötését megelőzően lépések tétele vagy teljesítése, úgy a szerződésnek minimálisan tartalmaznia kell az arra való utalást, hogy az adatkezelés a jelen Szabályzat szerint történik és arra a konkrét adatkezelési folyamatleírásra való hivatkozást, amely a konkrét adatkezelést rögzíti.

40. A szerződéses jogviszonyra hivatkozó jogalap csak akkor alkalmazható, ha az szerződés egyik szerződő fele az érintett.

5.6. A jogi kötelezettségre, mint jogalapra vonatkozó különleges szabályok

41. Amennyiben az adatkezelés jogalapja jogi kötelezettség teljesítése, úgy e jogi kötelezettséget csak és kizárólag az Európai Unió vagy Magyarország hatályos és alkalmazandó jogszabályának kell megállapítania.

42. Amennyiben az Intézmény az adatkezelése során a jogalapként a jogi kötelezettséget határozza meg, úgy az adatkezelési nyilvántartásban a jogi kötelezettséget előíró jogszabályi rendelkezést a jogszabályra és a jogszabályi helyre történő pontos hivatkozással kell megjelölni.

5.7. A létfontosságú érdekre, mint jogalapra vonatkozó különleges szabályok

43. Az Intézmény természetes személy létfontosságú érdekére hivatkozó jogalappal akkor végez adatkezelést, ha az adott adatkezelés egyéb jogalappal nem végezhető.

44. Az elszámoltathatóság elve miatt az Intézmény az adatkezelés megkezdését megelőzően köteles megvizsgálni, hogy a személyes adat kezelése megvalósítható-e bármely más jogalappal. Ugyancsak az elszámoltathatóság elvéből fakadóan az Intézménynek tudnia kell bizonyítania a létfontosságú érdek fennálltát.

5.8. A jogos érdekre, mint jogalapra vonatkozó különleges szabályok

45. A jogos érdekre hivatkozó jogalapot a szükségesség-arányosság elve alapján alkalmazza az Intézmény, ha az adatkezeléssel elérendő cél más jogalappal nem megvalósítható és az érintett magánszférájának korlátozása arányban áll az elérendő céllal.

46. Az Intézmény a jogos érdekre hivatkozó jogalappal végzett adatkezelés megkezdése előtt az érintettek magánszférájának, érdekeinek és alapvető jogainak biztosítása érdekében – amennyiben szükséges - érdekmérlegelési tesztet végez el. Az érdekmérlegelési teszt célja az adatkezelő vagy egy harmadik fél jogos érdekeinek és az érintett érdekeinek, illetve alapvető jogainak és szabadságainak összevetése annak eldöntése érdekében, hogy jogos érdekre hivatkozó jogalappal elvégezhető-e a tervezett adatkezelés. A jogos érdekre történő hivatkozásnál érdekmérlegelési teszt elvégzésével kell összevetni, illetve az érintettet tájékoztatni kell arról, hogy az adatkezelés az adatkezelő jogos érdekén alapul.

Az érdekmérlegelési tesztnek ki kell terjednie:

- a kezelni kívánt személyes adatok körének meghatározására,
- annak a személynek a meghatározása, akinek a jogos érdekében az adatkezelés szükséges,
- a jogos érdek lehető legpontosabb meghatározására,

• az adatkezelés céljának meghatározására,

• annak vizsgálatára, hogy az adatkezelés feltétlenül szükséges-e a feltárt jogos érdek érvényesítéséhez,

• a jogos érdek és az érintetti alapjogi korlátozás összevetésére.

47. Amennyiben az érdekmérlegelési teszt eredményeként az Intézmény megállapítja, hogy az adatkezeléssel érintett jogos érdekkel szemben elsőbbséget élveznek az érintett érdekei és alapvető jogai, a jogos érdekre hivatkozó jogalapot nem alkalmazza.

6. A SZABÁLYZATHOZ KAPCSOLÓDÓ JOGSZABÁLYOK, SZABÁLYZATOK

GDPR	Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [az Infotv-nek a GDPR hatálya alá eső adatkezelésekre alkalmazandó szabályai – lsd. Infotv. 2. § (2) és (4) bekezdése]
Eüak.	1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről, és a végrehajtására kiadott jogszabályok
Eütv.	1997. évi CLIV. törvény az egészségügyről, és a végrehajtására kiadott jogszabályok
Ebtv.	1997. évi LXXXIII. törvény kötelező egészségbiztosítás ellátásairól, és a végrehajtására kiadott jogszabályok

Eszjtv.	az egészségügyi szolgálati jogviszonyról szóló 2020. évi C. törvény
Mt.	2012. évi I. törvény a Munka Törvénykönyvéről
	közérdekű adatok közzétételének rendjéről szóló szabályzat
	Informatikai Biztonsági Szabályzat
	Iratkezelési szabályzat
	Panaszkezelési szabályzat

7. AZ ADATVÉDELMI TEVÉKENYSÉG SZERVEZETE ÉS IRÁNYÍTÁSA AZ INTÉZMÉNYNÉL

7.1. . Általános rendelkezések

48. Az Intézmény jelen szabályzatban határozza meg az adatvédelmi előírások megvalósításához szükséges feladat- és hatásköröket.

49. Az Intézmény minden adatkezelése felett a felügyeletet elsődlegesen az adatvédelmi tisztviselő látja el.

50. A Szabályzatban előírtak betartatásáért az Intézmény minden munkatársa felelős. Mindenki köteles gondoskodni arról, hogy jogosulatlan személyek ne tekinthessenek be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

7.2. Az adatvédelmi tevékenység ellátásában résztvevők

51. Az adatvédelmi tevékenység irányításában és ellátásában az Intézmény szervezeti egységei

- az Intézmény Szervezeti és Működési Szabályzatában meghatározott feladatkörükön belül az alábbiak szerint vesznek részt.

52. 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.

53. 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 ügyekért felelős szervezeti egységgel, valamint az Informatikai Osztállyal együttműködve gondoskodnak az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról;

b/ gondoskodnak arról, hogy az irányításuk alá tartozó szervezeti egységek felelősségi körébe tartozó nyilvántartási rendszerek naprakészek, megbízhatóak legyenek;

c/ gondoskodnak arról, hogy az irányításuk alatt álló személyek az adatkezelés meghatározott feltételeinek megfelelően járjanak el [GDPR 32. cikk (4) bek.];

d/ döntenek a jelen utasításban, illetve az adatkezeléssel járó folyamatot szabályozó egyéb belső szabályzatokban a feladat- és hatáskörébe utalt kérdésekben.

54. A főigazgató

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

b/ adatvédelmi incidens esetén – az adatvédelmi tisztviselő közreműködésével – szükség esetén sajtóközleményt bocsát ki és kizárólagos kapcsolatot tart a sajtó képviselőivel.

55. A jogász:

a/ az adatvédelmi tisztviselő szükség szerinti közreműködésével ellátja az érintetti jogok gyakorlásával kapcsolatos beadványok megválaszolását a személyes adatok kezelését, illetve a GDPR szerinti jogaik gyakorlását érintő panaszok kezelése mellett.

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

c/ az Intézmény minőségügyi dokumentumok készítésének és kezelésének szabályzatában foglaltaknak megfelelően biztosítja, hogy az adatvédelmi tisztviselő véleményét kikérjék az Intézmény adatvédelmi tárgyú vagy adatvédelmi vonatkozású belső szabályzatainak előkészítése során,

d/ 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.

56. Az Informatikus felelős azért, hogy az Intézmény szervezeti és működési szabályzatában, valamint az Intézmény információbiztonsági szabályzatában meghatározott feladatkörében:

a/ ellátja az informatikai biztonsági biztonsággal kapcsolatos feladatokat a folyamatos üzemeltetési feladatok kivételével, különösen az Intézmény információbiztonsági szabályzatában meghatározott feladatokat;

b/ ellátja 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 ellátja a személyes adatok kezelésével kapcsolatos technikai védelem megvalósítását, ellátja – az Intézmény információbiztonsági szabályzatában meghatározott – hatáskörébe tartozó információbiztonsági feladatokat, valamint rendelkezésre állási kontrollok biztosítását, a tárolt és továbbított személyes adatok bizalmasságának védelmét, az incidensfelderítési és -kezelési tevékenység támogatását,

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

57. 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 tartásához szükséges információk átadása az adatvédelmi tisztviselő részére stb.), illetve abban közreműködik;

c/ együttműködik az ugyanazon adatkezelésben érintett más adatkezelési megbízottakkal;

d/ közreműködik az érintettek jogai gyakorlásának biztosításában;

e/ közreműködik az adatvédelmi incidensek következményeinek elhárításában;

f/ közreműködik az adatvédelmi tisztviselő vizsgálataiban;

g/ közreműködik az adatvagyon-felmérés elkészítésében,

h/ közreműködik az Intézmény kezelésében lévő az adatok biztonsági osztályba sorolásában.

58. Adatkezelési megbízottnak olyan személyt kell kijelölni, aki az adott szakterületet, üzleti/adminisztratív folyamato(ka)t, illetve a szakterületek tevékenységét támogató informatikai rendszereket illetően kellő ismeretekkel bír.

7.3. Az adatvédelmi tisztviselő

59. Az adatvédelmi tisztviselőt a főigazgató nevezi ki az olyan, az Intézménnyel foglalkoztatási, szerződési vagy megbízotti jogviszonyban álló természetes személyek közül, aki ismeri az Intézmény működését, feladatait, munkafolyamatait és rendelkezik:

a/ 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 adatvédelmi és informatikai folyamatok ismeretével;

d/ legalább 3 év adatvédelmi területen szerzett gyakorlattal.

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

61. Az adatvédelmi tisztviselő független, függetlensége biztosítása érdekében szakmai feladatai ellátása során utasítást nem fogadhat el, szakmai feladatai ellátásával összefüggésben nem

bocsájtható el. Jelen szabályzatban foglalt tevékenysége ellátása során autonóm, szakmai ügyekben kizárólag a főigazgatónak tartozik felelősséggel.

62. 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 forrás biztosítását, elegendő idő biztosítását feladatai ellátásához, valamint az informatikai és a biztonsági szakterület együttműködése révén az adatvédelmi tisztviselő bevonását:

a/ a megfelelő technikai-eljárási intézkedésekhez szükséges források meghatározása (költségvetési tervezés) során annak érdekében, hogy teljesüljenek az adatvédelem alapelvei a technikai vívmányok alkalmazása (beépített adatvédelem) és az adatvédelem barát megoldások (alapértelmezett adatvédelem) révén;

b/ a felügyeleti hatósággal történő együttműködés során, amellyel az adatvédelmi tisztviselő – a Jogász és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – tartja a kapcsolatot.

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

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

65. Az Intézményben nem lehet adatvédelmi tisztviselő az a természetes személy, aki az Intézményben az adatkezelési tevékenység céljainak, kereteinek, eszközeinek meghatározásáról dönt, különösen a főigazgató, adatkezelésért felelős szervezeti egység vezetője ((1/A)a) pont) és a belső ellenőr.

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

67. 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.

68. 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 Jogász bevonásával – a neki címzett panaszokat, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;

d/ a Jogásszal és az Informatikussal együttműködve elkészíti az adatvédelmi és adatbiztonsági szabályzatot;

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

f/ a Jogásszal együttműködve személyes adatok kezelésére vonatkozó előírásokról tájékoztatást nyújt, tanácsot ad;

g/ személyes adatot is kezelő új informatikai rendszer belső fejlesztéssel történő bevezetése során közreműködik az adatvédelmi hatásvizsgálatot lefolytatásában;

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

i/ vezeti az Adatkezelési Nyilvántartást (13. fejezet);

j/ éves összefoglaló jelentést készít a főigazgatónak;

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

l/ a Főigazgató iránymutatásával további előírt adatszolgáltatást teljesít.

8. ADATKEZELÉS BEVEZETÉSÉVEL, MÓDOSÍTÁSÁVAL ÉS MEGSZÜNTETÉSÉVEL KAPCSOLATOS FELADATOK

8.1. Alapvetések

69. Az Intézmény kizárólag a hatályos jogszabályok rendelkezései alapján végez adatkezelést.

70. Az Intézmény személyes adatot csak és kizárólag a GDPR 6. cikkébe, a személyes adatok különleges kategóriáiba tartozó személyes adatot csak és kizárólag a GDPR 9. cikk (2) bekezdésében foglalt jogalapokkal, jog gyakorlása vagy kötelezettség teljesítés érdekében kezel.

71. A konkrét adatkezelési folyamattal érintett jogosultság vagy kötelezettség keletkezhet az Intézmény, az érintett vagy harmadik fél oldalán is.

72. Az Intézmény kezelésében lévő személyes adat az adatkezelés során mindaddig megőrzi személyes adat minőségét, amíg belőle az érintett azonosított vagy azonosítható. Az Intézmény akkor tekint egy adatot személyes adatnak, amennyiben rendelkezik azzal a technikai feltétellel, amely segítségével képes az adatból azonosítani az érintettet.

73. Az Intézmény csak úgy folytat adatkezelést, hogy az minden szakaszában megfelel az adatkezelési célnak.

74. Az Intézmény munkaszervezési, fizikai, informatikai és jogosultságkezelési eszközökkel gondoskodik arról, hogy illetéktelen személyek a személyes adatokat ne ismerhessék meg.

8.2. A személyes adatokkal kapcsolatos titoktartási szabályok

75. Az Intézmény munkatársai és az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek munkatársai és megbízottjai (alvállalkozói) kötelesek az adatkezelés során megismert személyes adatokat titokként megőrizni.

76. A személyes adatok egyetlen része vagy töredéke sem tehető közzé, nem bocsátható rendelkezésre vagy nem tárható fel semmilyen módon harmadik személy előtt, kivéve, ha a személyes adat közérdekből nyilvános adatként történő nyilvánosságra hozatalát jogszabály írja elő.

77. Az Intézmény munkatársai kötelesek megtenni azokat az intézkedéseket, amelyek kizárják, hogy a szóban elhangzott, papíralapon vagy elektronikus formátumban rögzített személyes adatot bármely harmadik személy jogosulatlanul megismerje.

78. Személyes adatról papíralapú vagy elektronikus másolat csak abban az esetben készíthető, ha azt az adatkezelés folyamata szükségessé teszi vagy jogszabály előírja.

79. Ha az Intézmény valamely munkatársa a Szabályzatot megszegi, az Intézmény és közte lévő jogviszony jellegétől függően felelősséggel tartozik.

80. Ha a Szabályzatot az Intézménnyel munkaviszonyban álló személy szegi meg és ezzel kárt okoz, úgy a munkaviszony ellátásra vonatkozó általános (a mindenkori munka törvénykönyvéről szóló, a Szabályzat kiadásakor a munka törvénykönyvéről szóló 2012. évi I. törvény) vagy speciális jogszabály munkaviszonyból származó kötelezettségének megszegésével okozott kárra vonatkozó szabályok szerint felel.

81. Ha a Szabályzatot az Intézménnyel egyéb jogviszonyban álló személy szegi meg és ezzel kárt okoz, úgy a mindenkori polgári törvénykönyv (a Szabályzat kiadásakor a Polgári Törvénykönyvről szóló 2013. évi V. törvény) károkozásért való felelősségre vonatkozó szabályok szerint felel.

8.3. Adatkezelés bevezetésével kapcsolatos feladatok

82. 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 minőségügyi dokumentumok készítésének és kezelésének szabályzatát e fejezet rendelkezéseit figyelembe véve kell alkalmazni.

83. Adatkezelés bevezetése főigazgatói utasítással történik.

A főigazgatói utasítás tartalmazza:

- az adatkezelésért felelős szervezeti egységnek és egyéb szervezeti egységeknek az adatkezeléssel kapcsolatos feladatait, így különösen:

  (a) az adatok felvételének, módosításának, törlésének rendje,

  (b) adatszolgáltatási kötelezettségek meghatározása az adatok naprakészen tartása érdekében,

  (c) a nyilvántartási rendszerből történő adattovábbítás, az ahhoz való hozzáférés rendje;
- az adatkezelésre vonatkozó különös adatbiztonsági intézkedések meghatározása;
- mellékletként

  (d) a GDPR-nak, az Infotv-nek és egyéb alkalmazandó jogszabálynak megfelelő adatkezelési tájékoztatót,

  (e) hozzájáruláson alapuló adatkezelés esetén a hozzájáruló nyilatkozat mintáját.

84. Az adatkezelési megbízottat az új adatkezelés bevezetésére vonatkozó igény megfogalmazásától kezdve be kell vonni az adatkezelés feltételeinek kidolgozása folyamatába.

85. A fejlesztési igényt megfogalmazó szervezeti egység vezetője az egyéb területek bevonásának szükségességéről az adatkezelési megbízottat és az adatvédelmi tisztviselőt értesíti.

86. Az adatkezelés feltételeinek kidolgozásában érintett szakterületek/szervezeti egységek kötelesek egymással, az adatkezelési megbízottal és az adatvédelmi tisztviselővel együttműködni. Az

adatkezelés feltételeinek kidolgozásában érintett szakterületek koordinálásáról az adatvédelmi tisztviselő gondoskodik.

87. Az adatkezelés bevezetésével, az adatkezelés feltételeinek meghatározásával kapcsolatban

a/ a leendő adatkezelésért annak tárgya szerint felelős adatkezelési megbízott:

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

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

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

ad/ az aa/ pontban meghatározott feladat részeként az adatvédelmi tisztviselő véleményének kikérése után javaslatot tesz a döntésre jogosultnak adatvédelmi hatásvizsgálat elvégzésére [8.7-es fejezet]; a döntésre jogosult erre vonatkozó pozitív döntése esetén elvégzi a hatásvizsgálatot, elkészíti ennek dokumentumát, és kikéri róla az adatvédelmi tisztviselő, valamint – ha alkalmazható – az érintettek vagy képviselőik véleményét [GDPR 35. cikk (1)-(2) és (9) bek.];

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

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

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

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

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

aj/ az adatkezelés bevezetéséről való döntést követően megküldi az adatvédelmi tisztviselőnek az új adatkezelésnek az Adatkezelési Nyilvántartásában történő rögzítéséhez

szükséges információkat, 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, a 15. fejezet szabályait is figyelembe véve egyedi esetben előterjesztést tesz a döntésre jogosultnak arról, hogy személyes adatok harmadik országba továbbíthatók-e egyedi ügyekben [GDPR 49. cikk (1) bek.];

am/az Informatikus feladatkörében közreműködik a személyes adatot kezelő rendszer fejlesztése és beszerzése során

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

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

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

ar/ 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;

as/ az adott adatkezelés különös (az Intézmény információbiztonsági szabályzatától eltérő) adatbiztonsági intézkedések meghatározásában; at/ az aa/, ad/, ae/, af/, ah/ és al/ alpont szerinti döntések előkészítésében.

88. Az előző 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.

89. Az előző 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.

90. 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.

91. 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 Jogsz véleményét a 87. pont aa/, ae/, af/, ag/, ah/ és al/ alpont tekintetében;

ab/ az Informatikus véleményét a 87. 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.

92. A végleges dokumentumok szakmai megfelelőségéért a dokumentum létrehozását kezdeményező adatkezelési megbízott, az adatvédelmi megfelelőségéért az adatvédelmi tisztviselő, az informatikai, információbiztonsági megfelelőségért pedig az Informatikus 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.

93. A 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.

94. Amennyiben a Jogász vagy az Informatikus kifogást fogalmaz meg, az adatvédelmi tisztviselő – szükség esetén az adatkezelési megbízottal és a véleményezőkkel való konzultáció után – javaslatot tesz a lehetséges megoldásra.

95. 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.

8.4. Az adatkezelési megbízott feladatai az adatkezelés során

96. Az adatkezelés során az adatkezelési megbízott az adatkezelésért felelős szervezeti egység feladatkörébe tartozó kérdésekben:

a/ képviseli az adatkezelőt az adatfeldolgozó felé vagy – közös adatkezelés esetén – a többi adatkezelő felé (amennyiben releváns);

b/ figyelemmel kíséri az adatkezelés feltételeinek folyamatos fennállását (beleértve az adatkezelés jogszerűségéhez szükséges tájékoztatások megadását, nyilatkozatok beszerzését stb.) és szükség esetén megteszi vagy kezdeményezi a szükséges intézkedéseket az adatkezelés feltételeinek módosítása iránt;

c/ amennyiben az adatkezelés hozzájáruláson alapul, ellenőrzi, hogy az érintett a hozzájárulását szabályosan szerezték-e be [GDPR 7. cikk (1) bek.];

d/ gondoskodik arról, hogy legalább az érintettel való első kapcsolatfelvételkor felhívják a figyelmét a tiltakozási jogra, és hogy az erről szóló tájékoztatást egyértelműen és más információtól elkülönítve jelenítsék meg [GDPR 21. cikk (4) bek.];

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

97. Az adatkezelés során (informatikai rendszerben kezelt adatok esetén az informatikai rendszer üzemeltetési szakaszában) az Informatikus – a feladatkörébe tartozó kérdésekben – gondoskodik arról, hogy az adatkezelés általános adatbiztonsági kontrolljainak működtetése az erre vonatkozó eljárásrendeknek 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.

98. A 96. pont b/ alpont alá eső esetekben

a/ megfelelően alkalmazni kell a 83-95. pont rendelkezéseit,

b/ az adatkezelés megváltozott adatait – a változást elrendelő döntés után – át kell vezetni az Adatkezelési Nyilvántartásban.

8.5. Adatkezelés megszüntetésével kapcsolatos feladatok

99. Amennyiben a kezelt adatokra a továbbiakban nincs szükség (az adatkezelési cél megvalósult), vagy jogszabályi változások miatt, vagy az adatvédelmi felügyeleti hatóság vagy bíróság döntése értelmében az adatok kezelését meg kell szüntetni, az adatkezelési megbízott – az adatvédelmi tisztviselő és rajta keresztül a Jogász és az Informatikus véleményének kikérése után – javaslatot tesz a döntésre jogosultnak:

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

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

100. A 99. pontban meghatározott esetben

a/ megfelelően alkalmazni kell a 83-95. pont rendelkezéseit,

b/ az Adatkezelési Nyilvántartásból az adatkezelést vagy az egyes adatfajtákat törölni kell,

c/ az adatokat – a 99. 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.

8.6. Az érdekmérlegelési teszt elvégzésének módszertana

101. 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.

102. Az érdekmérlegelési tesztet az adatkezelési megbízott végzi el. Az érdekmérlegelési tesztet írásban kell elvégezni. Az elkészült dokumentumot – a 89-91. 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 95. pont rendelkezéseit jelen esetben is alkalmazni kell.

103. 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.

104. Az érdekmérlegelési teszt részei:

a/ a tervezett adatkezelés leírása és az annak keretében kezelni tervezett személyes adatok meghatározása,

b/ az adatkezelő vagy azon harmadik fél jogos érdekének azonosítása, akinek az adatkezelés érdekében áll (Miért szükséges az adatkezelés?),

c/ az érintett érdekeinek, jogainak azonosítása (Arányban van-e az adatkezelés az érintett magánszférájának korlátozásával?),

d/ az adatkezelő (vagy harmadik fél) és az érintettek érdekeinek összevetése,

e/ az adatkezelés biztosítékainak leírása,

f/ az érdekmérlegelési teszt eredménye.

8.7. Az adatvédelmi hatásvizsgálat elvégzésének módszertana

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

106. A hatásvizsgálat elvégzésének szükségességéről az adatkezelési megbízott szükség esetén kikéri az adatvédelmi tisztviselő véleményét.

107. A hatásvizsgálat elvégzését az adatkezelési megbízott koordinálja a 87. 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, úgy meg kell indokolnia és dokumentumokkal igazolnia a mellőzés okait. A 95. pont rendelkezéseit jelen esetben is alkalmazni kell. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

108. 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.

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

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

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

a/ az adatkezelésért felelős szervezeti egységet és a tervezett adatfeldolgozó megjelölését;

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

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

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

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

f/ az adatkezelés folyamatának a leírását.

112. 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.

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

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

a/ a 111-113. 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.

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

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

9. AZ ÉRINTETTI JOGOK GYAKORLÁSÁNAK ELŐSEGÍTÉSE

9.1. Az adatkezelési tevékenység nyilvánossága

117. Az Intézmény honlapján közzé kell tenni:

a/ az Intézmény adatvédelmi politikáját;

b/ az Intézmény általános adatkezelési tájékoztatóját;

c/ az Intézmény egyes adatkezelési tevékenységeihez kapcsolódó (különös) adatkezelési tájékoztatók, ide nem értve a munkavállalók, egyéb jogviszonyban foglalkoztatottak adatainak kezelésére vonatkozó tájékoztatókat;

d/ közös adatkezelés esetén a közös adatkezelésben résztvevők közötti megállapodás lényegét, ha azt a különös adatkezelési tájékoztatók nem tartalmazzák;

e/ tájékoztatást arról, hogy az érintett kihez fordulhat az adatkezelést érintő kérdéseivel, panaszaival (az adatkezelő és az adatvédelmi tisztviselő elérhetősége, az adatvédelmi felügyeleti hatóság elérhetősége).

118. 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).

119. Az Intézmény vezetői gondoskodnak arról, hogy az Intézmény általános adatkezelési tájékoztatóján kívül az adott szervezeti egységek tevékenységi körébe tartozó adatkezelésekről szóló (különös) adatkezelési tájékoztatók kinyomtatott formában is rendelkezésre álljanak. Az Intézmény kezelésében lévő közérdekű adatok közzétételéről, illetve rendelkezésre bocsátásáról külön szabályzat rendelkezik.

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

120. Az Intézmény vezetői az adatkezelési megbízott 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 gondnokság alatt álló érintettel.

9.3. Gondokság alatt álló személyek személyes adatainak kezelése hozzájáruló nyilatkozat alapján

121. Az Intézmény vezetői az adatkezelési megbízott 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.

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

123. 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.

9.4. Hozzátartozók tájékoztatása

124. Az Intézmény vezetői az adatkezelési megbízott 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.

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

10. AZ ÉRINTETTŐL SZÁRMAZÓ KÉRELMEK, PANASZOK MEGVÁLASZOLÁSÁNAK RENDJE

10.1. Az adatvédelmi bejelentések típusai

126. 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 kezelt adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja – adathordozhatósághoz való jog (GDPR 20. cikk);

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

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

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

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

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

10.2. Az adatvédelmi beadványok kezelésének eljárásrendje

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

128. Az Intézményhez érkező, „Az adatvédelmi bejelentések típusai" pontban meghatározott beadványokat az Intézmény panaszkezelési 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/ Az adatvédelmi bejelentések típusai 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 Jogász bármely beadvány esetén kérheti az adatvédelmi tisztviselő véleményét a tekintetben, hogy a beadvány a 126. pontban meghatározott tárgyú-e, illetve, hogy az érintett kérte-e az adatkezelés korlátozását [zárolás, GDPR 18. cikk – lsd. Az adatvédelmi bejelentések típusai pont e/ alpont], és kérés esetén az adatvédelmi tisztviselő – az Informatikus 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 „Az adatvédelmi bejelentések típusai" pontban meghatározott tárgyú beadvány egyértelműen megalapozatlan vagy túlzó-e,

e/ az érintettnek saját adatairól szóbeli tájékoztatás csak egyértelmű azonosítás után lehetséges. Amennyiben a beadványozó nem azonosítható vagy kétség merül fel a beadványozó

személyazonosságát illetően, meg kell megkísérelni a beadványozó személyének azonosítását, beleértve a személyes megjelenés igénylését. Ilyen esetekben a GDPR 12. cikk (3) bekezdése szerinti határidő a beadványozó sikeres azonosításakor kezdődik;

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

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

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

i/ elektronikus úton egészségügyi adat csak a beadványozó kifejezett kérésére és csak oly módon küldhető, ha előzőleg a beadványozó figyelmét felhívták a kockázatokra és a beadványozó ezek után megerősíti a szándékát, egyúttal tudomásul véve az 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 „Az adatvédelmi bejelentések típusai" 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.

2. Az adatvédelmi beadványokról olyan ügyiratnyilvántartást kell vezetni, amely segítségével bármikor egyértelműen azonosíthatók Az adatvédelmi bejelentések típusai 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.

11. AZ ADATBIZTONSÁGI INTÉZKEDÉSEK (TECHNIKAI ÉS SZERVEZÉSI INTÉZKEDÉSEK) MEGHATÁROZÁSA ÉS VÉGREHAJTÁSA - A SZERVEZET ADATVÉDELMI RENDSZERE

Az Intézmény jelen szabályzatban határozza meg az adatvédelmi előírások megvalósításához szükséges feladat- és hatásköröket.

129. 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.

130. Az Intézmény működése során betartandó adatbiztonsági szabályokat (GDPR 32. cikk) külön szabályzatok tartalmazzák.

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

132. Az adatvédelmi tisztviselő Szabályzat szerinti feladatainak ellátásához szükséges mértékben a főigazgató köteles kijelölni az adatkezelési feladatokért felelős egy vagy több személyt („adatkezelési megbízottja"), aki e tevékenysége ellátása során közvetlenül az adatvédelmi tisztviselővel tartja a kapcsolatot, neki köteles jelenteni.

133. Az egyes szervezeti egységek vezetőinek és munkatársainak az adatkezeléssel összefüggő kötelezettségeit, az adatvédelmi előírások megtartásához fűződő személyi felelősségét az adatkezelési megbízott nem helyettesíti, hanem azt támogatja, koordinálja.

134. A szervezeti egység vezetője felelős a vezetése alá tartozó szervezeti egységnél az adatkezelésre vonatkozó jogszabályok és a Szabályzatban foglaltak betartásáért.

135. A Szabályzatban előírtak betartatásáért az Intézmény minden munkatársa felelős.

136. Mindenki köteles gondoskodni arról, hogy jogosulatlan személyek ne tekinthessenek be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető. Az adatbiztonság elveinek egy adatkezelés bevezetésének vagy személyes adatkezelést és/vagy - feldolgozást eredményező módosításának előkészítése során történő érvényesítése az Informatikus feladata, aki(ke)t az adatkezelési tevékenységet támogató nyilvántartási rendszerek kifejlesztésének, módosításának folyamatába kötelezően be kell vonni. Az adatbiztonsági intézkedések mindennapi működésben történő betartására az Intézmény minden alkalmazottja, valamint az Intézmény informatikai rendszereihez hozzáférő személy köteles.

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

12.1. Közös adatkezelés

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

138. A közös adatkezelésről szóló megállapodásban meg kell határozni különösen

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

b/ azt, hogy a közös adatkezelésben érintett egyes adatkezelők

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

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

- az adatvédelmi incidens tudomásra jutása esetén a másik adatkezelő adatvédelmi tisztviselőjét (adatvédelmi tisztviselő hiányában a kijelölt kapcsolattartót) haladéktalanul kötelesek értesíteni az adatvédelmi rendellenességről vagy incidensről,
- egymással kötelesek együttműködni az adatvédelmi rendellenesség vagy incidens okának kiderítésében és következményeinek felszámolásában,

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

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.

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

140. Amennyiben a közös adatkezelésben érintett másik adatkezelő harmadik országbeli adatkezelő, először abban a kérdésben kell dönteni – a 15. 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.

141. Amennyiben döntés születik a közös adatkezelés bevezetéséről, az illetékes adatkezelési megbízott, az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő és egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a Jogász közreműködésével, továbbá az Informatikus 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.

142. 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.

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

12.2. Adatfeldolgozói szerződések

144. Amennyiben harmadik országbeli adatfeldolgozó igénybevétele merül fel, először abban a kérdésben kell dönteni – a 15. 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.

145. Adatfeldolgozó igénybevétele esetén az adatfeldolgozóval kötendő szerződésnek tartalmaznia kell a GDPR 28. cikk (1)-(4) bekezdésében foglalt tartalmi elemeket a 146. pontban foglalt kiegészítések és pontosítások szerint.

148. 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 (aladatfeldolgozó) 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.

147. Az adatfeldolgozó igénybevételének szükségességét az adatkezelési megbízott az adatkezelés bevezetéséről való döntés előkészítése részeként vizsgálja meg. Ezt a szabályt kell alkalmazni akkor is, ha az adatfeldolgozó igénybevételéről az adatkezelés folyamán születik döntés.

148. Az adatbiztonsági intézkedések megfelelőségének megítélése az Informatikus 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.

149. 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 Jogász közreműködésével, továbbá Informatikus véleményének kikérésével előkészíti az adatfeldolgozóval kötendő szerződés tervezetét és azt felterjeszti a szerződés megkötésére jogosult személynek.

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

151. Az al-adatfeldolgozó igénybevétele esetén is megfelelően alkalmazni kell azzal, hogy az aladatfeldolgozó igénybevételére vonatkozó hozzájáruló nyilatkozatnak az adatfeldolgozói szerződés megkötésre jogosult személy általi kiadása előtt az adatkezelési megbízott kikéri az adatvédelmi tisztviselő és rajta keresztül a Jogász, továbbá az Informatikus véleményét is.

13. AZ ADATKEZELÉSI NYILVÁNTARTÁS

152. 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 adatok leírását,

e/ az adatok forrását,

f/ az adatok kezelésének időtartamát,

g/ a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló, valamint nemzetközi szervezethez történő adattovábbításokat is,

h/ az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét,

i/ az alkalmazott adatfeldolgozási technológia jellegét;

j/ az adatkezelő szervezeti egység megnevezését,

k/ az adatkezelésért felelős szervezeti egység vezetője, az adatokhoz hozzáférésre jogosult személyek köre (munkakör),

l/ az adatkezelés módszere (manuális, számítógépes, vegyes),

m/ adatbiztonsági intézkedések, archiválás módja, gyakorisága, adattörlés ideje.

n/ a kockázati besorolást.

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

154. Az adatvédelmi tisztviselő az Adatkezelési Nyilvántartásba való betekintést – a Hatóság képviselőin kívül – az Intézmény érintett szakterületei részére megigényli.

155. Az adatkezelési megbízott az új adatkezelés bevezetését az adatkezelés megkezdése előtt 5 munkanappal bejelenti az adatvédelmi tisztviselőnek, aki azt adatkezelési nyilvántartásba bejegyzi.

156. Az adatkezelési nyilvántartásba bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelési megbízott 5 munkanapon belül köteles bejelenteni az adatvédelmi tisztviselőnek, aki ennek megfelelően módosítja az adatkezelési nyilvántartás adatait.

157. Az Adatkezelési Nyilvántartással összefüggésben az adatvédelmi tisztviselő:

- 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;

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

- a Jogásszal együttműködve figyelemmel kíséri az adatkezelést érintő jogszabályok változását és a szükséges módosításokra felhívja az adatkezelési megbízottak figyelmét;

- az adatvédelmi felügyeleti hatóság megkeresésére adatot szolgáltat az Adatkezelési Nyilvántartásból.

14. AZ ADATVÉDELMI INCIDENSEK KEZELÉSE

14.1. Az adatvédelmi incidens minősítése

158. Adatvédelmi incidens csak akkor következik be, ha az adatbiztonsági intézkedések – akár vétlen, akár szándékos – megsértésének következtében bekövetkezik a személyes adatok véletlen

vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés:

a/ *súlyos incidens*: olyan incidens (pl. adatvesztés, adatsérülés), mely valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve (pl.: a jogosulatlan hozzáféréssel érintett adatok esete; az olyan adatsérülés, adatvesztés, amelynél az adatok naplózott állományból nem állíthatóak helyre). Magas kockázatúnak minősül az az eset, amely fizikai, vagyoni vagy nem vagyoni károkat okozhat az érintetteknek, pl. az érintetteknek a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, pénzügyi veszteséget, jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok integritásának, illetve bizalmas jellegének sérülését eredményezheti,

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

159. 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.

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

14.2. Az adatvédelmi incidens bejelentése

161. Az Intézmény irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező azon természetes személy (a munkavégzésre irányuló jogviszony jellegétől függetlenül), 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 közvetlen vezetőjének és az adatvédelmi tisztviselőnek az petegisz@petegisz.hu e-mail címen, vagy az intraneten erre a célra létrehozott űrlapot (1. melléklet) kitölteni. Az előbbieken túli egyéb bejelentő az Intézmény elektronikus elérhetőségén vagy az Intézmény honlapján elérhető űrlap kitöltésével jelentheti be az adatvédelmi incidenst.

162. 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 – írásban is meg kell erősíteni. Ilyen esetben a szóbeli közlés időpontját külön fel kell tüntetni.

163. 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.

164. 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 Intézményt, illetve az Intézmény adatvédelmi tisztviselőjét meghatározott elérhetőségen, köteles haladéktalanul, de legkésőbb az észlelést követő 24 órán belül értesíteni írásban és telefonon is. A szerződésnek tartalmaznia kell továbbá a közös adatkezelő, illetve az adatfeldolgozó kötelezettségeit adatvédelmi incidens bejelentésében és kivizsgálásában.

14.3. Incidensprotokoll általában

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

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

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

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

d/ ha az Intézmény – a mindenkor hatályos információbiztonsági szabályzatában, továbbá az üzletmenet-folytonossági és katasztrófa tervben foglaltakkal összhangban – nem rendelkezik automatizált módszerrel az adott sérülés (incidens) elhárítására, akkor azt manuális módon kell azonnal elkezdeni;

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

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

14.4. Az adatvédelmi incidens kivizsgálása

167. Adatvédelmi incidens (papíralapú és nem papíralapú adatokra vonatkozóak egyaránt) felmerülése esetén az Intézmény adatvédelmi tisztviselője a Jogász és az Informatikus, továbbá szükség esetén az adott szakterületért felelős szervezeti egység kijelölt munkatársának (a továbbiakban együtt: incidensvizsgáló bizottság) közreműködésével megvizsgálja, és 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.

168. 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.

169. Az adatvédelmi incidensről az adatvédelmi tisztviselő értesíti az Intézmény főigazgatóját.

170. 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.

171. 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 információbiztonsági szabályzatában, illetve az üzletmenet-folytonossági és katasztrófa tervben foglaltak szerint kell folytatni.

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

a/ az Intézmény főigazgatóját;

b/ a Jogászt

c/ informatikai rendszert is érintő incidens esetén az Informatikust

d/ a szakmailag illetékes szervezeti egység vezetőjét.

173. 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 meghatározott egyéb személyeket.

174. Az adatvédelmi incidens részletes vizsgálatának szükségességéről az incidensvizsgáló bizottság dönt. A részletes vizsgálatot a vizsgálat megkezdése után a lehető leghamarabb le kell zárni.

175. A vizsgálat során elsősorban az alábbi módszerek alkalmazhatóak:

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

b/ írásbeli tájékoztatás kérése az érintett szervezeti egységektől,

c/ dokumentumok vizsgálata,

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

176. 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.

177. 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.

178. A részletes vizsgálatról szóló jelentést a 172. pont a/-d/ alpontjában említett vezetőknek kell megküldeni.

179. 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.

180. 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.

181. 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.

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

14.5. Az érintett tájékoztatása a súlyos adatvédelmi incidensről

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

184. 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.

185. 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.

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

14.6. Az adatvédelmi incidens bejelentése a Hatóságnak

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

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

189. 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.

190. Ha nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később (pl. a 181. pont szerinti jóváhagyás után haladéktalanul) részletekben is közölhetők.

14.7. Az adatvédelmi és egyéb incidensek nyilvántartása

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

192. A nyilvántartásban rögzíteni kell:

a/ az incidensben érintett személyes adatok körét; és számát,

b/ az adatvédelmi incidenssel érintettek körét, és számát,

c/ az adatvédelmi incidens tudomásszerzés időpontját,

d/ az adatvédelmi incidens körülményeit, hatásait,

e/ az adatvédelmi incidens elhárítására megtett intézkedéseket,

f/ az adatvédelmi incidenssel kapcsolatban adott tájékoztatások adatait.

193. 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 minimálisan 10 évig őrzi meg, illetéktelenek számára hozzá nem férhető zárt helyen.

15. HARMADIK ORSZÁGBA IRÁNYULÓ ADATTOVÁBBÍTÁS KÜLÖNÖS SZABÁLYAI

194. Amennyiben személyes adatnak harmadik országba történő továbbításának szükségessége merül fel, az érintett szervezeti egység köteles az adatvédelmi tisztviselő véleményét kérni az adattovábbítás megengedhetőségéről, illetve az adattovábbítás lehetséges módjáról, figyelembe véve a GDPR szabályait és az aktuális országbesorolást.

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

16. BELSŐ ADATVÉDELMI ELLENŐRZÉSI ELJÁRÁS

196. 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.

197. Az adatvédelmi tisztviselő éves ellenőrzési tervet készít. Az éves ellenőrzési tervnek az ellenőrzés alá vont szervezeti egység nevét és az ellenőrzés várható időpontját, továbbá az ellenőrzés tárgykörét kell tartalmaznia. Az éves ellenőrzési terveket úgy kell elkészíteni, hogy négyéves időtartam alatt lehetőség szerint minden szervezeti egység ellenőrzésére sor kerüljön. Az éves ellenőrzési tervet legkésőbb adott év március 5. napjáig kell elkészíteni és az Intézmény főigazgatója részére bemutatni.

198. Az éves ellenőrzési tervet az Intézmény főigazgatója hagyja jóvá.

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

200. 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.

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

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

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

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

205. Az adott ellenőrzéssel kapcsolatban az Intézmény főigazgatója külön tájékoztatást kérhet az adatvédelmi tisztviselőtől, egyébként az adatvédelmi tisztviselő évente egy alkalommal, legkésőbb a tárgyévet követő év március 5. napjáig összefoglaló jelentést készít az Intézmény adatvédelmi helyzetéről, beleértve az általa a tárgyévben lefolytatott ellenőrzésekről, amelyet az Intézmény főigazgatója részére küld meg.

17. ZÁRÓ RENDELKEZÉSEK

206. Jelen Adatvédelmi szabályzat az aláírást követő napon lép hatályba.

207. Jelen szabályzatot legalább évente, vagy jogszabályi változásokat, illetve jelentős szervezeti változásokat követően át kell vizsgálni és aktualizálni kell.

208. A GDPR változása és/vagy a magyarországi vonatkozó jogszabályok változása esetén a szabályzat aktualizálását teljeskörűen és késedelem nélkül el kell végezni.

209. A Szabályzat rendelkezéseit az Intézmény többi szabályzatának előírásaival összhangban kell értelmezni. Amennyiben a személyes adatok védelmével kapcsolatosan ellentmondás áll fent jelen Szabályzat és a bármely más, jelen Szabályzat hatálybalépése előtt hatályba lépett szabályzat, utasítás előírásai között, úgy abban az esetben a Szabályzat rendelkezései az irányadóak.

210. Amennyiben ellentmondás áll fent jelen Szabályzat és a bármely más, jelen Szabályzat hatálybalépése után hatályba lépő szabályzat vagy utasítás előírásai között, úgy csak abban az

esetben nem e Szabályzat rendelkezései az irányadóak, ha a később hatályba lépő szabályzat vagy utasítás arról kifejezetten rendelkezik

Kelt, Polgár, 2024.05.26.

PÉTEGISZ
Járóbeteg Szakellátó Központ

……..
Dr. Pásztor Ibolya
főigazgató

Incidensbejelentő űrlap

Incidens neve: ……..

Incidens iktatószáma: …….

Határokon átnyúló incidens? Igen/Nem

Incidens leírása:

……

……

……

……..

Érintett adatkezelési tevékenység:

……..

Incidens jellege:

- személyes adatot tartalmazó eszköz (pl. laptop, pendrive) elvesztése/ellopása

- személyes adatot tartalmazó informatikai rendszer feltörése (hackertámadás)

- adathalászat

- rosszindulatú számítógépes programok (pl. zsarolóvírusok)

- személyes adat jogosulatlan megsemmisítése (elektronikus vagy papíralapú)

- személyes adatot tartalmazó papír alapú dokumentum nem megfelelő védelme illetéktelen hozzáférés ellen (pl. dokumentált beléptető rendszer hiánya vagy gyenge ellenőrzése, ellenőrizetlen dokumentum-másolás)

- személyes adatot tartalmazó papír alapú dokumentum elvesztése

- személyes adatot tartalmazó papír alapú dokumentum ellopása (pl. gyenge vagy hiányos létesítményvédelem)

- személyes adatot tartalmazó papír alapú dokumentum tűzkár általi megsemmisülése

- személyes adatot tartalmazó papír alapú dokumentum vízkár általi megsemmisülése

- személyes adatot tartalmazó papír alapú dokumentum olvashatatlanná válása (penész, nyomtatott szöveg színvesztése)

- személyes adatok jogosulatlan megismerése (pl. nem megfelelően biztonságos informatikai rendszer, intézményi dokumentációk közötti, ellenőrizetlen átjárhatóság)

- személyes adatok téves címre való elküldése

- személyes adatot tartalmazó levél elvesztése vagy jogosulatlan felnyitása

- személyes adatok jogosulatlan nyilvánosságra hozatala (pl. honlapon történő megjelenés)

- személyes adatok jogosulatlan szóbeli közlése

- személyes adatok jogosulatlan megváltoztatása

- egyéb: …….

Incidens okai:

……...

……...

Érintett személyes adatok: ……..

Érintett személyes adatok becsült száma: …….

Érintettek: ……

Érintettek becsült száma: ……...

Az érintett tájékoztatása megtörtént?

- igen

- nem, de lesz tájékoztatás

- nem, de tudja az érintett

- nem, és nem is lesz tájékoztatás

Érintett tájékoztatásának időpontja: ……

Érintettek tájékoztatásának módja és tartalma:

……

……

……...

Incidens állapota:

- adatkezelőnek bejelentve (adatfeldolgozóként észlelt incidens)

- feldolgozás alatt

- lezárva

- lezárva (nem incidens)

Sérülés jellege:

- bizalmasság

- integritás (sértetlenség)

- rendelkezésre állás

Valószínűsíthető következmények:

- elhanyagolható (enyhe)

- jelentős (mérsékelt)

- korlátozott (enyhe)

- maximális (súlyos, katasztrofális)

Megjegyzés: …….

Kapcsolódó intézkedések:

- korábban alkalmazott intézkedések leírása

- következmények súlyossága

- megtett és/vagy tervezett intézkedések

Időpontok:

- incidens bekövetkezésének időpontja

- incidens megszűnésének időpontja

- tudomásszerzés időpontja

- észlelés módja

- hatósági bejelentés időpontja

- késedelmes tájékoztatás indokai

- hatósági azonosító

Kelt:……

……

Aláírás