OSEI
SPORTKÓRHÁZ

ORSZÁGOS SPORTEGÉSZSÉGÜGYI INTÉZET
Dr. Soós Ágnes, főigazgató főorvos

1113 Budapest, Karolina út 27.
Levelezési cím: 1507 Bp. Pf. 202.
Tel.: (1) 488-6111 **E-mail:** foig@osei.hu

TÜV AUSTRIA
ZERTIFIZIERT
EN ISO 9001:2015
ZERTIFIKAT NR. 20 100 173002064
TÜV AUSTRIA CERT GMBH

6. számú szabályzat

Az Országos Sportegészségügyi Intézet adatvédelmi szabályzata

Készítette: Dr. Téglásy György Orvosigazgató
OSEI belső adatvédelmi felelős (BAF) .....

Ellenőrizte: Dr. Nagy Norbert
OSEI adatvédelmi tisztviselő (DPO) .....

Kiadás dátuma:2023. május 02.
Verzió/kiadás száma: 2/2

Jóváhagyta: .....
Dr. Soós Ágnes
Főigazgató főorvos

Felülvizsgálva. Érvényes.
A 2022. március 10.-én kiadott 2. 1. változat azonosítóval rendelkező Adatvédelmi szabályzat a 2.2. verzió hatálybalépésével érvényét veszti.
Jogfolytonossága a következő módosításig fenntartva. Hiteles 1-56. oldalig.
Budapest, 2023. május 02.

Jóváhagyta: .....
Dr. Soós Ágnes
Főigazgató főorvos

Tartalomjegyzék

1. A SZABÁLYZAT BEVEZETŐ RENDELKEZÉSEI

1. Alapelvek

1. Az Országos Sportegészségügyi Intézet (a továbbiakban: Intézmény) jelen Adatvédelmi Szabályzatban (a továbbiakban: Szabályzat) határozza meg a természetes személyek személyes adatainak kezelésével és védelmével kapcsolatos szabályokat, 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 az Alaptörvény VI.cikk, 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.), az uniós jog megsértését bejelentő személyek védelméről szóló 2019/1937/EU európai parlament és tanács irányelve (a továbbiakban: WBD), a panaszokról, a közérdekű bejelentésekről, valamint a visszaélések bejelentésével összefüggő szabályokról szóló 2013. évi XXV. törvény, az egészségügyről szóló 1997. évi CLIV. törvény (a továbbiakban: Eütv.), valamint az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (a továbbiakban: Eüak.) alkalmazandó rendelkezései, valamint az Intézményre irányadó egyéb jogszabályok rendelkezései szerint kezelni. Az Intézmény a személyes adatok kezelésével járó tevékenysége során érvényre juttatja a GDPR alapelveit, így különösen:
   a/ jogszerűség, tisztességes eljárás és átláthatóság elvei: 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/ elszámoltathatóság elve: az adatkezelő felelős az adatkezelési elveknek való megfelelésért, továbbá képesnek kell lennie a megfelelés igazolására

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

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

3. A Szabályzat hatálya alá tartozó személyek kötelesek az olyan tevékenységük során, amely szükségszerűen együtt jár személyes adatok kezelésével, az adott tevékenységre vonatkozó – a Szabályzat 9.1 számú mellékletében felsorolt – speciális szabályzatokban foglalt rendelkezések mellett a jelen Szabályzat rendelkezései szerint eljárni azzal, hogy amennyiben a speciális szabályzat a jelen Szabályzattal ellentétes rendelkezést tartalmaz, úgy jelen Szabályzat alkalmazandó.

2. Alapfogalmak

4. Jelen Szabályzat alkalmazása során a GDPR 4. cikkében és az Infotv. 3. § 3., 4., 6., 11., 12., 13., 16., 17., 21., 23-24. pontjában meghatározott fogalmakon kívül az alábbi fogalmakat kell alkalmazni:

a/ beteg [Eütv. 3.§ a) pont]: az egészségügyi ellátást igénybe vevő vagy abban részesülő személy;

b/ betegellátó [Eüak. 3.§ g) pont]: a kezelést végző orvos, az egészségügyi szakdolgozó, az érintett gyógykezelésével kapcsolatos tevékenységet végző egyéb személy, a gyógyszerész;

c/ egészségügyi ellátás [Eütv. 3. § c) pont]: a beteg adott egészségi állapotához kapcsolódó egészségügyi szolgáltatások összessége;

d/ gyógykezelés [Eüak. 3.§ c) pont]: minden olyan tevékenység, amely az egészség megőrzésére, továbbá a megbetegedések megelőzése, korai felismerése, megállapítása, gyógyítása, a megbetegedés következtében kialakult állapotromlás szinten tartása vagy javítása céljából az érintett közvetlen vizsgálatára, kezelésére, ápolására, orvosi rehabilitációjára, illetve mindezek érdekében az érintett vizsgálati anyagainak feldolgozására irányul, ideértve a gyógyszerek, gyógyászati segédeszközök, gyógyfürdőellátások kiszolgálását, a mentést és betegszállítást, valamint a szülészeti ellátást is.

e/ egészségügyi dokumentáció [Eüak. 3.§ e) pont]: a gyógykezelés / egészségügyi szolgáltatás során a betegellátó / egészségügyi dolgozó tudomására jutott egészségügyi és személyazonosító adatokat tartalmazó feljegyzés, nyilvántartás vagy bármilyen más módon rögzített adat, függetlenül annak hordozójától vagy formájától;

f/ kezelést végző orvos [Eüak. 3. § f) pont]: a beteg adott betegségével, illetve egészségi állapotával kapcsolatos vizsgálati és terápiás tervet meghatározó, valamint ezek

keretében beavatkozásokat végző orvos, aki a beteg gyógykezeléséért felelősséggel tartozik vagy abban közreműködő orvos (pl.: konzílium, telemedicina, stb.);

g/ közeli hozzátartozó [Eüak. 3.§ j) pont]: a házastárs, az egyeneságbeli rokon, az örökbe fogadott, a mostoha- és nevelt gyermek, az örökbe fogadó, a mostoha- és nevelőszülő, valamint a testvér és az élettárs;

h/ orvosi titok [Eüak. 3.§ d) pont]: a gyógykezelés során az adatkezelő tudomására jutott egészségügyi és személyes adat, továbbá a szükséges vagy folyamatban lévő, illetve befejezett gyógykezelésre vonatkozó, valamint a gyógykezeléssel kapcsolatban megismert egyéb adat. Az adatkezelőre vonatkozik az orvosi titoktartás, mely alól csak a beteg írásos hozzájárulása adhat felmentést, illetve a törvény alapján kötelező adattovábbítás jelent kivételt;

i/ sürgős szükség [Eüak. 3.§ k) pont]: az egészségi állapotában hirtelen bekövetkezett olyan változás, amelynek következtében azonnali egészségügyi ellátás hiányában az érintett közvetlen életveszélybe kerülne, illetve súlyos vagy maradandó egészségkárosodást szenvedne

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

k/ adatkezelési nyilvántartás: az adatvédelmi tisztviselő által üzemeltetett GDPR CERT rendszerben a GDPR 30. cikkében rögzített tartalmi elemekkel folyamatosan karbantartott nyilvántartás

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

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

n/ adatvédelmi hatásvizsgálat: olyan vizsgálat, amelyet az adatkezelő 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,

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

p/ belső adatvédelmi felelős: az adatvédelmi felelősök munkáját koordináló, az adatvédelmi tisztviselő tevékenységét a jelen Szabályzat szerint támogató munkavállaló;

q/ adatvédelmi felelős: az adatkezelésért felelős szervezeti egység azon, e feladatkör ellátására kijelölt munkavállalója, aki a jelen Szabályzatban, illetve az adatkezelést szabályozó más belső szabályozó dokumentumokban meghatározottak szerint a szervezeti egység feladat- és hatáskörébe tartozó adatkezelések tekintetében, gondoskodik az adatkezelőt terhelő feladatok elvégzéséről,

r/ adatvédelmi tisztviselő: a GDPR 39. cikkében meghatározott feladatokat az Intézmény részére szerződéses jogviszonyban ellátó természetes személy

s/ álnevesítés (pszeudonimizálás): a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni,

t/ 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,

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

v/ érdekmérlegelési teszt: 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,

w/ informatikai szakterület: az informatikai rendszerek üzemeltetéséért, az informatikai biztonság ellátásáért felelős szervezeti egység vagy egységek, ideértve az Intézmény elektronikus információs rendszer biztonságáért felelős személyét is,

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

y/ törlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása a továbbiakban már nem lehetséges.

z/ ügyvitel: az Intézmény tevékenységére vonatkozó jogszabályokban az Intézmény részére meghatározott közfeladatok ellátásával összefüggő eljárás.

aa/ belső bejelentés: jogsértésre vonatkozó információnak valamely magánszektorban vagy közszférában működő jogalanyon belül történő szóbeli vagy írásbeli közlése (WBD 5. cikk 4. pont)

3. A Szabályzat célja

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

6. A Szabályzat célja továbbá, hogy meghatározza azokat a szervezési és technikai intézkedéseket, amelyek kialakításával az Intézmény gondoskodik a személyes adatok

kezelése során a személyes adatok biztonságáról. Erre tekintettel a Szabályzat az Intézmény által folytatott adatkezelési tevékenységek során figyelembe veendő és követendő elveket, rendelkezéseket tartalmaz. Ezeket az előírásokat minden egyes adatkezelési folyamat, tevékenység során, annak teljes tartama alatt figyelembe kell venni.

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

4. A Szabályzat személyi hatálya

8. Jelen Szabályzat személyi hatálya kiterjed az Intézmény munkavállalóira, továbbá azon természetes személyekre (a továbbiakban: érintett), akik személyes adatait a jelen Szabályzat hatálya alá tartozó adatkezelések tartalmazzák, továbbá azon érintettekre, akik jogait vagy jogos érdekeit az adatkezelés érinti. Az Intézmény megbízásából személyes adatok kezelését vagy feldolgozását végzők esetén az erre a jogviszonyra az Intézmény által kötött szerződésben a GDPR 28. cikkének megfelelően rendelkezni kell arról, hogy az Intézmény által megbízott adatfeldolgozó a feladata ellátása során hogyan juttatja érvényre jelen Szabályzat rendelkezéseit.

5. A Szabályzat időbeli hatálya:

9. Jelen Szabályzat aláírásának napjától annak módosításáig vagy visszavonásig érvényes. A Szabályzat felülvizsgálatára háromévente került sor, mely idő lerövidül, amennyiben jogszabályi, szakmai, strukturális vagy egyéb változások szükségessé teszik a felülvizsgálatot.

6. A Szabályzat tárgyi hatálya

10. A Szabályzat tárgyi hatálya az Intézmény mindazon adatkezeléseire kiterjed – függetlenül attól, hogy az adatkezelés elektronikusan vagy papíralapon történik –, amelyek

    a/ az Intézmény önálló adatkezelői minőségében saját szervezeti egységeinek működtetése érdekében végrehajtott adatkezelési műveletekhez köthetők,
    b/ az Intézmény szerződéses partnereivel, hatóságokkal és felügyeleti szervekkel kapcsolatos adatkezelési műveletekhez köthetők,
    c/ az Intézmény által nyújtott egészségügyi szolgáltatáshoz köthetők.

2. AZ INTÉZMÉNY ADATVÉDELMI SZERVEZETI FELÉPÍTÉSE ÉS RENDSZERE

7. Adatvédelmi Szervezet

11. Az Intézmény a vonatkozó jogszabályok rendelkezései alapján belső adatvédelmi szervezetet alakít ki és működtet az alábbiak szerint:

12. A Főigazgató feladata:

a/ kijelöli és megbízza az adatvédelmi tisztviselőt (DPO), akit a Felügyeleti Hatóság nyilvántartásában regisztrál
b/ kijelöli és megbízza a rezidens belső adatvédelmi felelőst (BAF)
c/ kijelöli az intézeti és a szervezeti egység szintű adatvédelmi felelősöket (OAF)
d/ ellenőrzi az adatvédelmi tisztviselő (DPO) és a rezidens belső adatvédelmi felelős (BAF) tevékenységét
e/ elrendeli az Intézmény adatvédelmi szabályzatának elkészítését

13. Az Intézmény adatvédelmi tisztviselőjének (DPO) feladatai:

a/ adatvédelmi nyilvántartások vezetése a GDPR CERT rendszerben
b/ tájékoztat, szakmai tanácsot ad és ellenőrzi az adatvédelemmel kapcsolatos jogszabálynak való megfelelést, különös tekintettel az egészségügyi adatok kezelésére vonatkozó szabályokra
c/ közreműködik az Adatvédelmi Szabályzat és az Informatikai Biztonsági Szabályzat elkészítésében,
d/ a szervezeti egység szintű adatvédelmi rendszer felépítésének szakmai támogatása és ellenőrzése
e/ az osztályos adatvédelmi felelősök (OAF) szakmai felügyelete és oktatása, oktatási anyagok és tematika biztosítása
f/ tanácsot ad az adatvédelmi hatásvizsgálatra és az érdekmérlegelési tesztekre vonatkozóan, valamint aktívan közreműködik ezek elvégzése során
g/ kapcsolattartó pontként működik azon érintettek számára, akik személyes adataik kezelésével és jogaik gyakorlásával kapcsolatban keresik meg,
h/ együttműködik és kapcsolattartó pontként működik a Felügyeleti Hatóság felé az adatkezeléssel kapcsolatos ügyekben.
i/ adatvédelmi incidenssel során a tudomására jutástól számítva haladéktalanul, maximum 72 órán belül bejelentést tesz a Felügyeleti Hatóság (NAIH) felé
j/ javaslatot tesz az adatvédelem, illetve az adatbiztonság területén a kifejlesztett új technológiák és eszközök alkalmazása előtt.
k/ az adatvédelmi tevékenységgel kapcsolatos oktatásokat megszervezi és az oktatási anyagot évente legalább egy alkalommal minden szervezeti egységben frissíti az osztályos adatvédelmi felelősök (OAF) számára.

14. Az Intézmény belső adatvédelmi felelősének (BAF) feladatai:

Az Intézetben az Eszjtv. alapján foglalkoztatottak közül kerül kijelölésre a belső adatvédelmi felelős (BAF), az alábbiak feladatok ellátására:

a/ hatályos jogszabályok, szakmai anyagok ismerete, folyamatos követése, szakmai önképzés, a megszerzett információk alapján döntés előkészítés segítése
b/ az adatvédelmi tisztviselő munkájának támogatása
c/ az osztályos adatvédelmi felelősök munkájának támogatása és felügyelete
d/ aktív részvétel adatvédelmi incidensek azonosításában és kezelésében

15. Szervezeti egység szintű osztályos adatvédelmi felelősének (OAF) feladata:

Az Intézményben a szervezeti egységekben adatvédelmi felelősök lettek kijelölve, akinek a feladatai közé az alábbiak tartoznak:

a/ az új dolgozók adatkezelési tájékoztatása

b/ adatvédelmi incidens gyanújának rögzítése és haladéktalan továbbítása az adatvédelmi tisztviselő (DPO) és a belső adatvédelmi felelős (BAF) számára

c/ az érintettek megkereséseinek rögzítése és haladéktalan továbbítása az adatvédelmi tisztviselő (DPO) és a belső adatvédelmi felelős (BAF) számára

d/ a partnerek megkereséseinek rögzítése és haladéktalan továbbítása az adatvédelmi tisztviselő (DPO) és a belső adatvédelmi felelős (BAF) számára

e/ a közérdekű adatok megismerése iránti igények rögzítése és haladéktalan továbbítása az adatvédelmi tisztviselő (DPO) és a belső adatvédelmi felelős (BAF) számára

f/ a tudományos, történeti kutatások, statisztikai és edukációs adatok kezelésével kapcsolatos igények rögzítése és haladéktalan továbbítása az adatvédelmi tisztviselő (DPO) és a belső adatvédelmi felelős (BAF) számára

g/ a belső szabályozókban előírtaknak történő megfelelés ellenőrzése a napi munkavégzés során

h/ Az Intézmény dolgozóinak rendszeres, és a belépő dolgozóknak belépés előtt adatvédelmi oktatását az Intézmény szervezeti egység szintű adatvédelmi felelősei (OAF) végzik az adatvédelmi tisztviselő által kidolgozott és aktualizált oktatási tematika alapján melynek megtörténtét feljegyzésben rögzíti. A részvételt a dolgozók aláírással igazolják.

8. Illetékesség és felelősség

14. Az adatkezelés jogszerűsége érdekében az alábbi illetékességi és felelősségi köröket biztosítja az Intézmény:

Jelen Szabályzat **kidolgozásáért** felelős:	Főigazgató Adatvédelmi Tisztviselő (DPO) Belső Adatvédelmi Felelős (BAF)
Jelen Szabályzat **alkalmazásáért** felelős:	Belső Adatvédelmi Felelős (BAF) Adatvédelmi felelős (AF) A Szabályzat hatálya alá tartozó szervezeti egységek vezetői
Jelen Szabályzat **végrehajtásáért** felelős:	Belső Adatvédelmi Felelős (BAF) Adatvédelmi felelős (AF)
Jelen Szabályzat **ellenőrzéséért** felelős:	Főigazgató Adatvédelmi Tisztviselő (DPO)

9. Adatvédelmi Szabályzat

15. Jelen Szabályzatban az Intézmény általános adatvédelmi szabályai kerültek rögzítésre, a speciális adatvédelmi és adatbiztonsági szabályozás a szervezeti egységek osztályos működési rendjének adatvédelmi fejezetében és ezek mellékletében kerül kifejtére.

16. Az Intézmény elektronikus rendszert használ az adatvédelmi rendszer működtetésére és az adatvédelmi nyilvántartások vezetésére.

10. Szervezeti egység szintű osztályos működési rendek

17. Az Intézmény a speciális adatvédelmi és adatbiztonsági szabályokat a szervezeti egységek osztályos működési rendjének adatvédelmi fejezetében és ezek mellékletében kerül rögzítésre.

3. AZ INTÉZMÉNY ÖNÁLLÓ ADATKEZELŐI MINŐSÉGÉBEN SZERVEZETI EGYSÉGEINEK MŰKÖDTETÉSÉHEZ KAPCSOLÓDÓ ÁLTALÁNOS ADATVÉDELMI SZABÁLYOK

11. Az adatkezelés jogszerűségének biztosítása

18. Személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak. Kizárólag olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig. Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

19. Az Intézmény adatkezelői tevékenységét a jelen Szabályzatban foglalt okokból és célok elérése érdekében végzi. Az Intézmény mindenkori Főigazgatója határozza meg az Intézmény dolgozóinak adatkezeléssel kapcsolatos feladatait, tevékenységük célja, hogy törvényes és tisztességes módon, az adatkezelés minden szakaszában biztosítsák az adatok pontosságát, gondoskodjanak az érintett személyes adatainak védelméről jogosulatlan hozzáférés, megváltoztatás, továbbítás, törlés vagy megsemmisülés esetén.

12. Adatkezelés bevezetésével kapcsolatos feladatok

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

21. Adatkezelés bevezetése Főigazgatói utasítással történik. A Főigazgatói utasítás tartalmazza
a/ az adatkezelésért felelős szervezeti egységnek és egyéb szervezeti egységeknek az adatkezeléssel kapcsolatos feladatait, így különösen:
aa/ az adatok felvételének, módosításának, törlésének rendje,
ab/ adatszolgáltatási kötelezettségek meghatározása az adatok naprakészen tartása érdekében,
ac/ az adattovábbítás és az ahhoz való hozzáférés rendje;
b/ az adatkezelésre vonatkozó különös adatbiztonsági intézkedések meghatározása;
c/ mellékletként

ca/ a GDPR-nak, az Infotv-nek és egyéb alkalmazandó jogszabálynak megfelelő adatkezelési tájékoztatót,

cb/ hozzájáruláson alapuló adatkezelés esetén a hozzájáruló nyilatkozat mintáját.

22. Az adatkezelésért felelős szervezeti egység vezetőjét, az adatvédelmi tisztviselőt és a belső adatvédelmi felelőst az új adatkezelés bevezetésére vonatkozó igény megfogalmazásától kezdve be kell vonni az adatkezelés feltételeinek kidolgozása folyamatába.

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

24. Az adatkezelés feltételeinek kidolgozásában érintett szakterületek/szervezeti egységek adatvédelmi felelősei kötelesek egymással, a belső adatvédelmi felelőssel és az adatvédelmi tisztviselővel együttműködni. Az adatkezelés feltételeinek kidolgozásában érintett szakterületek/szervezeti egységek adatvédelmi felelősei tevékenységének koordinálásáról az adatvédelmi tisztviselő gondoskodik.

25. Az adatkezelés bevezetésével, az adatkezelés feltételeinek meghatározásával kapcsolatban

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

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

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

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

ad/ az aa/ pontban meghatározott feladat részeként az adatvédelmi tisztviselő véleményének kikérése után dokumentálja az adatvédelmi hatásvizsgálat el nem végzésének indokait vagy javaslatot tesz a döntésre jogosultnak adatvédelmi hatásvizsgálat elvégzésére [229-240. pont]; a döntésre jogosult erre vonatkozó pozitív döntése esetén – az informatikai fejlesztéseket, az informatikai architektúra tervezést, illetve az IT üzemeltetést végző szervezeti egységnél működő adatvédelmi felelős közreműködésével – elvégzi az adatvédelmi hatásvizsgálatot, elkészíti ennek dokumentumát, és kikéri róla az adatvédelmi tisztviselő, valamint – ha alkalmazható – az érintettek vagy képviselőik véleményét [GDPR 35. cikk (1)-(2) és (9) bek.];

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

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

ag/ az aa/ pontban meghatározott feladat részeként megszövegezi a hozzájáruló nyilatkozatot [GDPR 7. cikk (2) bek.], illetve, ha közös adatkezelés vagy adatfeldolgozó bevonása miatt szükséges, a megfelelő szerződéses rendelkezéseket;

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

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

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

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

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

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

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

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

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

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

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

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

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

26. A 225. 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.

27. A 225. 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.

28. Az adatvédelmi tisztviselő véleményének kikéréséhez olyan dokumentumot/leírást kell benyújtani, amely kellő részletességgel meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, illetve a 25. pontban meghatározott egyéb döntési javaslatokat.

29. Az adatvédelmi tisztviselő adatvédelmi jogi támogatást nyújt a belső adatvédelmi felelős által előkészített, megszövegezett, adatkezeléshez kapcsolódó dokumentumok elkészítésében és közreműködik azok véglegesítésében.

30. A végleges dokumentumok szakmai megfelelőségéért a dokumentum létrehozását kezdeményező belső adatvédelmi felelős, az adatvédelmi megfelelőségéért az adatvédelmi tisztviselő, az informatikai, információbiztonsági megfelelőségért pedig az informatikai szakterület a felelős. Abban az esetben, ha bármely terület eltér a megfogalmazott szakmai, adatvédelmi vagy információbiztonsági állásfoglalásoktól, az eltérésért, illetve a végleges dokumentumért az adatvédelmi tisztviselő vagy az információbiztonsági szakterület semmilyen felelősséggel nem tartozik.

31. Amennyiben az adatkezelés feltételei kidolgozásában részt vevő adatvédelmi felelősök között véleményeltérés van, illetve a Stratégiai Igazgató vagy az informatikai szakterület kifogást fogalmaz meg, az adatvédelmi tisztviselő – szükség esetén a belső adatvédelmi felelőssel, az adatvédelmi felelősökkel és a véleményezőkkel való konzultáció után – javaslatot tesz a lehetséges megoldásra.

32. 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.

13. Dokumentálási kötelezettség

33. 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 – adatkezelési nyilvántartást vezet a jelen szabályzat mellékletében nevesített adatkezelésekről a GDPR CERT rendszerben.

34. 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.

14. Adatkezelési Nyilvántartások

35. Adatkezelési tevékenységekről adatkezelési célonként az Intézmény adatkezelési nyilvántartást vezet a GDPR CERT rendszerben az Adatkezelési Tevékenységek Nyilvántartásában.

36. Adatkezelő az általános közzétételi lista III/3.,4., 6. közzétételi egységében közzéteendő adatait az Infotv. 37/C. § szerint a Nemzeti Adatvagyon Ügynökség (a továbbiakban: NAVÜ) által üzemeltetett Központi Információs Közadat-nyilvántartás felületre mutató linkkel teljesíti. Az Adatkezelő az így közzéteendő adatokat kéthavi rendszerességgel adatlapon továbbítja a NAVÜ számára.

15. Adatfeldolgozói szerződések

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

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

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

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

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

43. Az Adatkezelési Tevékenységek Nyilvántartásával összefüggésben az adatvédelmi tisztviselő:
    a/ biztosítja, hogy az adatkezelések bevezetését megelőző döntéselőkészítés során az érintett szakterületek az adatkezelési tevékenységek nyilvántartása adatait megismerhessék a felesleges, párhuzamos adatkezelések elkerülése, illetve az új adatkezelésnek a meglévő adatkezelésekhez való illeszkedése érdekében;

    b/ ellenőrzi az adatkezelések, közös adatkezelők, illetve adatfeldolgozók adatainak az Adatkezelési Tevékenységek Nyilvántartásába történő rögzítését és jelzi az adatkezelésért felelős szervezeti egység vezetőjének a hiányos, hibás vagy valószínűleg megváltozott adatokat, információkat;

    c/ a Jogi Irodával együttműködve figyelemmel kíséri az adatkezelést érintő jogszabályok változását és a szükséges módosításokra felhívja az adatvédelmi felelősök figyelmét;

    d/ a Felügyeleti Hatóság megkeresésére, vagy hatósági eljárása során adatot szolgáltat az Adatkezelési Tevékenységek Nyilvántartásából.

16. Az érintetti jogok gyakorlásának általános szabályai

44. Az Intézménynek elő kell segítenie az érintetti jogok gyakorlását.

45. Az Intézménynek az érintett részére a személyes adatok kezelésére vonatkozó valamennyi információt és minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell nyújtania, különösen a gyermekeknek címzett bármely információ esetében. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

46. Az Intézmény indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított 25 napon belül tájékoztatja az érintettet a jogai gyakorlására irányuló kérelme

nyomán hozott intézkedésekről. E határidő a GDPR-ban írt feltételekkel további két hónappal meghosszabbítható, amelyről az érintettet tájékoztatni kell.

47. Ha az adatkezelő nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely Felügyeleti Hatóságnál, és élhet bírósági jogorvoslati jogával.

48. Az Intézmény az információkat és az érintett jogairól szóló tájékoztatást és intézkedést díjmentesen biztosítja, azonban a GDPR-ban írt esetekben díj számítható fel.

49. A részletes szabályok a GDPR 12. cikke (Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések) alatt találhatók.

50. Az érintett jogosult arra, hogy az adatkezeléssel összefüggő tényekről és információkról az adatkezelés megkezdését megelőzően tájékoztatást kapjon. Ennek keretében az érintettet tájékoztatni kell [GDPR 13-14. cikk].

51. Az adatkezelő a fentiek szerinti tájékoztatást az alábbiak szerint adja meg:

    a/ a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül;

    b/ ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával; vagy

    c/ ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor.

52. Ha az adatkezelő a személyes adatokon a megszerzésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő célról és minden releváns kiegészítő információról.

53. Az előzőekben leírtakat nem kell alkalmazni, ha és amilyen mértékben:

    a/ az érintett már rendelkezik az információkkal;

    b/ a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne, különösen a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, a Rendelet 89. cikk (1) bekezdésében foglalt feltételek és garanciák figyelembevételével végzett adatkezelés esetében, vagy amennyiben a GDPR 14. cikk (1) bekezdésében említett kötelezettség valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezen adatkezelés céljainak elérését. Ilyen esetekben az adatkezelőnek megfelelő intézkedéseket kell hoznia – az információk nyilvánosan elérhetővé tételét is ideértve – az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében;

    c/ az adat megszerzését vagy közlését kifejezetten előírja az adatkezelőre alkalmazandó uniós vagy tagállami jog, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről rendelkezik; vagy

d/ a személyes adatoknak valamely uniós vagy tagállami jogban előírt szakmai titoktartási kötelezettség alapján, ideértve a jogszabályon alapuló titoktartási kötelezettséget is, bizalmasnak kell maradnia

54. Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz hozzáférést kapjon (GDPR 15. cikk).

55. Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a GDPR 46. cikk szerinti megfelelő garanciákról.

56. Az Intézménynek az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére kell bocsátania. Az érintett által kért további másolatokért az adatkezelő az adminisztratív költségeken alapuló, ésszerű mértékű díjat számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri. A másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait [GDPR 15. cikk].

57. Az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat.

58. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését is [GDPR 16. cikk].

59. Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje. [GDPR 17. cikk]:

60. Ha az Intézmény nyilvánosságra hozta a személyes adatot, és az előbbi pont értelmében azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, adatfeldolgozókat, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

61. Az előző két pont nem alkalmazandó, amennyiben az adatkezelés szükséges:

a/ a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;

b/ a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;

c/ a GDPR 9. cikk (2) bekezdése h) és i) pontjának, valamint a GDPR 9. cikk (3) bekezdésének megfelelően a népegészségügy területét érintő közérdek alapján;

d/ a GDPR 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben az

valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést; vagy

e/ jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez [GDPR 17. cikk[.

62. Az érintett jogosult arra, hogy az Intézmény korlátozza az adatkezelést, ha a jogszabályban meghatározott feltételek teljesülnek [GDPR 18. cikk].

63. Az érintett jogosult arra, hogy kérésére az Adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

a/ az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;

b/ az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;

c/ az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy

d/ az érintett a GDPR 21. cikk (1) bekezdése szerint tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

64. Az adatkezelő minden olyan címzettet tájékoztat valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről. a [GDPR 19. cikk]:

65. Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha

a/ az adatkezelés a GDPR 6. cikk (1) bekezdésének a) pontja vagy a GDPR 9. cikk (2) bekezdésének a) pontja szerinti hozzájáruláson, vagy a GDPR 6. cikk (1) bekezdésének b) pontja szerinti szerződésen alapul és

b/ az adatkezelés automatizált módon történik.

66. A fenti esetekben az érintett kérheti a személyes adatok adatkezelők közötti közvetlen továbbítását is.

67. Az Intézet – az egészségügyi szolgáltatásával összefüggő – adatkezelői tevékenysége Eütv.-ben foglalt jogi kötelezettségek alapján, a GDPR. 6. cikk (1) bekezdésének c), d) és e) alapján történik, valamint az adatkezelés nem automatizált formában történik, azért ezekben az esetekben az adathordozhatósághoz való jog nem illeti meg az érintettet.

68. Az adathordozhatóságra és továbbításra irányuló kéréseket Az Intézet Főigazgatójának címzett kérelemben kell megfogalmazni.

69. Az adathordozhatósághoz való jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges. E jog nem érintheti hátrányosan mások jogait és szabadságait. [GDPR 30. cikk]:

70. Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak [GDPR 6. cikk (1) bekezdés e) pont] közérdeken, közfeladat végrehajtásán, vagy jogos érdeken alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

71. Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

72. Ezen jogokra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

73. Az érintett a tiltakozáshoz való jogot műszaki előírásokon alapuló automatizált eszközökkel is gyakorolhatja.

74. Ha a személyes adatok kezelésére a GDPR 89. cikk (1) bekezdésének megfelelően tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozhasson a rá vonatkozó személyes adatok kezelése ellen, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség [GDPR 21. cikk].

75. Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené [GDPR 22. cikk].

76. Ez a jogosultság nem alkalmazandó abban az esetben, ha a döntés:

    a/ az érintett és az Intézmény közötti szerződés megkötése vagy teljesítése érdekében szükséges;

    b/ meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít; vagy

    c/ az érintett kifejezett hozzájárulásán alapul.

77. Az Intézmény köteles megfelelő intézkedéseket tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek legalább azt a jogát, hogy az adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

78. Az Intézményre vagy adatfeldolgozójára alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel korlátozhatja jogok és kötelezettségek (GDPR 12-22. cikk, 34. cikk, 5. cikk) hatályát, ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát.

79. Az Intézményre vagy adatfeldolgozójára alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel korlátozhatja a GDPR 12–22. cikkben és a 34. cikkben foglalt, valamint a 12–22. cikkben meghatározott jogokkal és kötelezettségekkel összhangban lévő rendelkezései tekintetében az 5. cikkben foglalt jogok és kötelezettségek hatályát, ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát, valamint az alábbiak védelméhez szükséges és arányos intézkedés egy demokratikus társadalomban:

a/ nemzetbiztonság;

b/ honvédelem;

c/ közbiztonság;

d/ bűncselekmények megelőzése, nyomozása, felderítése vagy a vádeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása, beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését;

e/ az Unió vagy valamely tagállam egyéb fontos, általános közérdekű célkitűzései, különösen az Unió vagy valamely tagállam fontos gazdasági vagy pénzügyi érdeke, beleértve a monetáris, a költségvetési és az adózási kérdéseket, a népegészségügyet és a szociális biztonságot;

f/ a bírói függetlenség és a bírósági eljárások védelme;

g/ a szabályozott foglalkozások esetében az etikai vétségek megelőzése, kivizsgálása, felderítése és az ezekkel kapcsolatos eljárások lefolytatása;

h/ az a)–e) és a g) pontban említett esetekben – akár alkalmanként – a közhatalmi feladatok ellátásához kapcsolódó ellenőrzési, vizsgálati vagy szabályozási tevékenység;

i/ az érintett védelme vagy mások jogainak és szabadságainak védelme;

j/ polgári jogi követelések érvényesítése.

80. Az előző bekezdésben említett jogalkotási intézkedések adott esetben részletes rendelkezéseket tartalmaznak legalább:

a/ az adatkezelés céljaira vagy az adatkezelés kategóriáira,

b/ a személyes adatok kategóriáira,

c/ a bevezetett korlátozások hatályára,

d/ a visszaélésre, illetve a jogosulatlan hozzáférésre vagy továbbítás megakadályozását célzó garanciákra,

e/ az Adatkezelő meghatározására vagy az Adatkezelők kategóriáinak meghatározására,

f/ az adattárolás időtartamára, valamint az alkalmazandó garanciákra, figyelembe véve az adatkezelés vagy az adatkezelési kategóriák jellegét, hatályát és céljait,

g/ az érintettek jogait és szabadságait érintő kockázatokra, és

h/ az érintettek arra vonatkozó jogára, hogy tájékoztatást kapjanak a korlátozásról, kivéve, ha ez hátrányosan befolyásolhatja a korlátozás célját [GDPR 23. cikk].

81. Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja, kivéve a jogi kötelezettség teljesítésére vonatkozó igényét. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét,

82. Az érintett jogosult arra, hogy panaszt tegyen a Felügyeleti Hatóságnál a **http://naih.hu** internetes oldalon közzétett elérhetőségeken – illetve a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállam Felügyeleti Hatóságnál –, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése jogsértő [GDPR 77. cikk].

83. Az egyéb közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben [GDPR 78. cikk].

84. Az egyéb közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden érintett jogosult a hatékony bírósági jogorvoslatra, ha a GDPR 55. vagy 56. cikk alapján illetékes felügyeleti hatóság nem foglalkozik a panasszal, vagy három hónapon belül nem tájékoztatja az érintettet a GDPR 77. cikk alapján benyújtott panasszal kapcsolatos eljárási fejleményekről vagy annak eredményéről.

85. A felügyeleti hatósággal szembeni eljárást a felügyeleti hatóság székhelye szerinti tagállam bírósága előtt kell megindítani.

86. Ha a felügyeleti hatóság olyan döntése ellen indítanak eljárást, amellyel kapcsolatban az egységességi mechanizmus keretében a Testület előzőleg véleményt bocsátott ki vagy döntést hozott, a felügyeleti hatóság köteles ezt a véleményt vagy döntést a bíróságnak megküldeni.

87. A rendelkezésre álló közigazgatási vagy nem bírósági útra tartozó jogorvoslatok – köztük a Felügyeleti Hatóságnál történő panasztételhez való jog – sérelme nélkül, minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak nem a GDPR rendelkezéseinek megfelelő kezelése következtében megsértették a GDPR szerinti jogait [GDPR 79. cikk].

88. Az adatkezelővel vagy az adatfeldolgozóval szembeni eljárást az adatkezelő vagy az adatfeldolgozó tevékenységi helye szerinti tagállam bírósága előtt kell megindítani. Az ilyen eljárás megindítható az érintett szokásos tartózkodási helye szerinti tagállam bírósága előtt is, kivéve, ha az adatkezelő vagy az adatfeldolgozó valamely tagállamnak a közhatalmi jogkörében eljáró közhatalmi szerve.

89. Minden olyan személy, aki az adatvédelmi rendelet megsértésének eredményeként vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért az adatkezelőtől vagy az adatfeldolgozótól kártérítésre jogosult.

90. Az adatfeldolgozó abban az esetben tartozik felelősséggel az adatkezelés által okozott károkért, ha nem tartotta be a jogszabályban meghatározott, kifejezetten az adatfeldolgozókat terhelő kötelezettségeket, vagy ha az adatkezelő jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el.

91. Ha több adatkezelő vagy több adatfeldolgozó vagy mind az adatkezelő mind az adatfeldolgozó érintett ugyanabban az adatkezelésben, és felelősséggel tartozik az adatkezelés által okozott károkért, minden egyes adatkezelő vagy adatfeldolgozó egyetemleges felelősséggel tartozik a teljes kárért. Az adatkezelő, illetve az adatfeldolgozó mentesül a felelősség alól, ha bizonyítja, hogy a kárt előidéző eseményért őt nem terheli felelősség.

17. Az adatkezelési tevékenység nyilvánossága

92. Az Intézmény a honlapján egy olyan, „Adatvédelem" nevű oldalt tart fenn, amely bármely oldalról közvetlenül elérhető. Az „Adatvédelem" oldalon közzé kell tenni:
    a/ az Intézmény adatvédelmi tisztviselőjének nevét és elérhetőségeit
    b/ az Intézmény előzetes adatkezelési tájékoztatóját;
    c/ tájékoztatást az e-Papír szolgáltatásról, az Intézmény Hivatali Kapu elérhetőségéről, valamint arról, hogy az Intézmény milyen típusú adatvédelmi beadványokat fogad az e-Papír szolgáltatás útján.

93. Az Intézmény honlapján el kell helyezni az internetes oldalra vonatkozó
    a/ impresszumot
    b/ jogi nyilatkozatot
    c/ adatkezelési tájékoztatót
    d/ süti tájékoztatót
    e/ egyéb releváns dokumentumot (pl. betegtájékoztatókat, formanyomtatványokat).

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

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

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

97. Az Intézmény szervezeti egységeinek vezetői az adatvédelmi felelősök közreműködésével gondoskodnak arról, hogy az Intézményben kezelt vagy az Intézménnyel más módon kapcsolatba kerülő gyermekek az adataik kezelésével kapcsolatos tájékoztatást a gyermek számára világos és elérhető módon megkapják. A tájékoztatás az alábbi módokon történhet:
    a/ a gyermek törvényes képviselője útján: a gyermeket érintő adatkezelésről a gyermekkel kapcsolatba lépő munkavállaló írásban tájékoztatja a gyermek törvényes képviselőjét, és írásban nyilatkoztatja arra vonatkozóan, hogy a tájékoztatást közli a gyermekkel;

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

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

98. Az Intézmény szervezeti egységeinek vezetői az adatvédelmi felelősök közreműködésével gondoskodnak arról, hogy az Intézményben kezelt korlátozottan cselekvőképes vagy cselekvőképtelen nagykorú személyek törvényes képviselői, illetve – állapotától függően – a korlátozottan cselekvőképes személy is megfelelő tájékoztatást kapjanak a személyes adatok kezeléséről. A törvényes képviselőt írásban nyilatkoztatni kell, hogy a tájékoztatást közli a gondnoksága alatt álló érintettel.

99. Az Intézmény szervezeti egységeinek vezetői az adatvédelmi felelősök 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.

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

101. 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.

102. Az Intézmény szervezeti egységeinek vezetői az adatvédelmi felelősök 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.

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

18. Közérdekű adatok megismerése iránti igényre vonatkozó általános szabályok

104. Az Intézmény az Infotv. 28-31.§ rendelkezéseinek megfelelően jár el a közérdekű adatok megismerése iránti igények esetében.

105. Az Intézmény adatvédelmi nyilvántartást vezet az Országos Kórházi Főigazgatóság által biztosított GDPR CERT elektronikus rendszerben a közérdekű adatok megismerése iránti igényekről.

106. Az Intézmény az elutasított közérdekű adatigénylésekről éves jelentést készít a Felügyeleti Hatóság számára, amelyben megjelöli az elutasítás pontos indokát és körülményeit.

19. Közérdekű archiválás, tudományos és történelmi kutatási, illetve statisztikai, vagy edukációs célú adatkezelésekre vonatkozó általános szabályok

107. A GDPR 9. cikk (2) bekezdés j) pontjában nevesített esetekben a GDPR 89. cikk (1) bekezdésével összhangban jár el az Intézmény.

108. Az Intézmény adatvédelmi nyilvántartást vezet az Országos Kórházi Főigazgatóság által biztosított GDPR CERT elektronikus rendszerben a közérdekű archiválás, tudományos és történelmi kutatási, illetve statisztikai, vagy edukációs célú adatkezelésekről.

20. Harmadik országba irányuló adattovábbítás általános szabályai

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

110. Az adatvédelmi tisztviselő – szükség esetén a Stratégiai Igazgató és az informatikai szakterület véleményének kikérése után – javaslatot tesz az adattovábbítás módjára, az adatátadás során alkalmazandó biztosítékok körére.

21. Általános adatbiztonsági intézkedések (technikai és szervezési intézkedések) meghatározása és végrehajtása

111. 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.

112. Az Intézmény működése során betartandó adatbiztonsági szabályokat (GDPR 32. cikk) külön szabályzatok tartalmazzák, így különösen a mindenkor hatályos
   a/ Informatikai Biztonsági Szabályzat,
   b/ Egészségügyi Vészhelyzeti Terv
   c/ Üzemeltetői Biztonsági Terv

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

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

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

115. *Az adatbiztonság elveinek egy adatkezelés bevezetésének vagy személyes adatkezelést és/vagy -feldolgozást eredményező módosításának előkészítése során az adatvédelmi* tisztviselőt és az informatikai szakterület vezetőjét kötelezően be kell vonni.

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

22. Adatkezelés megszüntetésével kapcsolatos feladatok

117. Amennyiben a kezelt adatokra a továbbiakban nincs szükség (az adatkezelési cél megvalósult vagy a kezelt adatokra vonatkozó megőrzési idő letelt), vagy jogszabályi változások miatt, vagy az adatvédelmi Felügyeleti Hatóság vagy bíróság döntése értelmében az adatok kezelését meg kell szüntetni, a belső adatvédelmi felelős – az adatvédelmi tisztviselő és rajta keresztül a Stratégiai Igazgató és az informatikai szakterület véleményének kikérése után – javaslatot tesz a döntésre jogosultnak:

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

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

23. Elektronikus megfigyelőrendszerekkel végzett adatkezelés

118. Adatkezelő elektronikus megfigyelő rendszereket alkalmaz székhelyén. Minden esetben rendelkeznie kell előzetes adatkezelési hatásvizsgálattal, illetve megfigyelési pontonként érdekmérlegelési tesztek alapján kerülhet meghatározásra a tárolási idő.

119. A tárolási időpontok lejárta után a rögzített anyagokat helyreállíthatatlan módon törölni kell. Amennyiben az adatok hatósági, vagy bírósági eljárásban felhasználásra kerülnek, akkor a felvételek megőrzésének időtartamára az adott eljárásra vonatkozó jogszabályi rendelkezések az irányadók.

120. Adatkezelő az elektronikus megfigyelőrendszerek működéséről előzetes és megfelelő adatkezelési tájékoztatást biztosít a helyszíneken kihelyezett tájékoztató táblák segítségével, illetve a https://osei.hu/adatvedelem oldalon elhelyezett dokumentumok segítségével.

121. Az elektronikus megfigyelpő rendszerek elhelyezése nem sértheti az emberi méltóságot, tehát képfelvétel nem rögzíthető munkaidő alatt wc, zuhanyzó, orvosi szoba, vagy váró, munkahelyi pihenőhelyiségben. A képfelvétel nem használható fel a foglalkoztatott magánéletének ellenőrzésére. A kamerák helyét és a megfigyelt terület leírását Adatlezelő adatvédelmi nyilvántartásban rögzítette.

122. A folyamatosan, valós időben közvetített képek megtekintésére kizárólag a Főigazgató, Orvosigazgató, Stratégiai Igazgató, Adatvédelmi tisztviselő és a Biztonsági Szolgálat munkatársai jogosultak.

123. Az elektronikus megfigyelőrendszerek által készített és rögzítésre került felvételeket kizárólag az előző 122. pontban nevesített személyek kezelhetik.

124. Az elektronikus megfigyelőrendszerek által készített és rögzítésre került felvételekről mentést kizárólag az előző 122. pontban felsorolt személyek készíthetnek.

125. Az elektronikus megfigyelőrendszerek által rögzített felvételeket Adatkezelő az adatvédelemre vonatkozó jogszabályok előírásainak megfelelően kezeli, azokat harmadik fél részére csak a törvényben meghatározott esetben (pl. rendőrség, bíróság, stb.) adja át. Az érintettek bármikor tájékoztatást kérhetnek a felvételek kezeléséről.

24. Belső bejelentések

126. Elektronikus megfigyelőrendszerekkel végzett adatkezelés A WBD 5. cikk 4. pont szerinti belső bejelentésre Adatkezelő a https://osei.hu/adatvedelem oldalon elérhető GDPR CERT rendszer folyamatos elérhetőségét biztosítja a foglalkoztatottak számára, illetve a visszaelesbejelento@osei.hu email címet.

4. AZ INTÉZMÉNY SZERZŐDÉSES PARTNEREIVEL, HATÓSÁGOKKAL ÉS FELÜGYELETI SZERVEKKEL KAPCSOLATOS ADATKEZELÉSEK ÁLTALÁNOS SZABÁLYAI

25. A közös adatkezelői megállapodások megkötésének és végrehajtása, ellenőrzésének szabályai

127. Közös adatkezelésnek minősül, ha az adatkezelés céljait és eszközeit az Intézmény egy vagy több másik adatkezelővel közösen határozza meg a GDPR 26. cikk értelmében.

128. A közös adatkezelésről szóló megállapodásban meg kell határozni különösen

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

b/ azt, hogy a közös adatkezelésben érintett egyes adatkezelők

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

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

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

bd/ az esetleges jogellenes adatkezelés következményeit milyen arányban viselik;

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

ca/ az adatvédelmi incidens tudomásra jutása esetén a másik adatkezelő adatvédelmi tisztviselőjét (adatvédelmi tisztviselő hiányában a kijelölt kapcsolattartót) haladéktalanul kötelesek értesíteni az adatvédelmi rendellenességről vagy incidensről,

cb/ egymással kötelesek együttműködni az adatvédelmi rendellenesség vagy incidens okának kiderítésében és következményeinek felszámolásában,

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

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

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

129. A közös adatkezelés szükségességét az adatvédelmi felelős az adatkezelés bevezetéséről való döntés előkészítése részeként vizsgálja meg.

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

131. Amennyiben döntés születik a közös adatkezelés bevezetéséről, a belső adatvédelmi felelős az adatvédelmi jogi megfelelőség biztosítása érdekében az adatvédelmi tisztviselő és a Stratégiai Igazgató közreműködésével, továbbá az informatikai szakterület véleményének kikérésével elkészíti 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.

132. 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.

133. A belső adatvédelmi felelős a közös adatkezelői megállapodás megkötését követően – az adatkezelések nyilvántartására vonatkozó szabályok szerint – e tényt és a további adatkezelő(k) adatait (név és cím, kapcsolattartó neve és elérhetősége) rögzíti az az Országos Kórházi Főigazgatóság által biztosított GDPR CERT elektronikus rendszerben.

26. Adatfeldolgozói szerződések megkötésének és végrehajtása ellenőrzésének szabályai

134. Adatfeldolgozó igénybevétele esetén az adatfeldolgozóval kötendő szerződésnek tartalmaznia kell a GDPR 28. cikk (1)-(4) bekezdésében foglalt tartalmi elemeket

135. Az adatfeldolgozóval kötendő szerződésben

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

b/ rögzíteni kell az adatfeldolgozónak az érintettől származó kérelmek, panaszok megválaszolásában való közreműködésének eljárásrendjét;

c/ rögzíteni kell az adatfeldolgozó kötelezettségeit adatvédelmi incidens észlelése esetén, így különösen

ca/ az adatvédelmi incidens tudomásra jutása esetén az Intézmény adatvédelmi tisztviselőjét haladéktalanul köteles értesíteni az adatvédelmi incidensről,

cb/ köteles együttműködni az Intézmény adatvédelmi tisztviselőjével és más közreműködő szervezeti egységgel az adatvédelmi incidens okának feltárásban és következményeinek felszámolásában,

cc/ köteles együttműködni az adatvédelmi incidens bejelentésének teljesítésében,

d/ rögzíteni kell az adatfeldolgozó kötelezettségét az adatvédelmi hatásvizsgálat elvégzésében, illetve a hatásvizsgálatban azonosított kockázatok alakulásának figyelemmel kísérésében, az adatkezeléssel járó kockázatok változásának jelzésében, illetve az adatvédelmi hatásvizsgálatok utóellenőrzésben.

136. Az adatfeldolgozó igénybevételének szükségességét az adatvédelmi felelős 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.

137. Az adatbiztonsági intézkedések technikai megfelelőségének megítélése az informatikai szakterület hatáskörébe tartozik, beleértve azt is, hogy az adatfeldolgozó által egy magatartási kódexhez vagy tanúsítási mechanizmushoz való csatlakozás elegendő garanciát jelent-e az adatbiztonsági szabályok megfelelőségére.

138. Amennyiben döntés születik az adatfeldolgozó igénybevételéről, a belső adatvédelmi felelős az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő és egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a Stratégiai Igazgató közreműködésével, továbbá az informatikai szakterület véleményének kikérésével előkészíti az adatfeldolgozóval kötendő szerződés tervezetét és azt felterjeszti a szerződés megkötésére az erre jogosult személynek.

139. Az adatvédelmi felelős az adatfeldolgozói szerződés megkötését követően – az adatkezelések nyilvántartására vonatkozó szabályok szerint – az adatfeldolgozó adatait (név és cím, kapcsolattartó neve és elérhetősége) rögzíti az az Országos Kórházi Főigazgatóság által biztosított GDPR CERT elektronikus rendszerben.

140. A 122.-127. pontok rendelkezéseit a további adatfeldolgozó igénybevétele esetén is megfelelően alkalmazni kell azzal, hogy a további adatfeldolgozó igénybevételére vonatkozó hozzájáruló nyilatkozatnak az adatfeldolgozói szerződés megkötésre jogosult személy általi kiadása előtt a belső adatvédelmi felelős kikéri az adatvédelmi tisztviselő és rajta keresztül a Stratégiai Igazgató, továbbá az informatikai szakterület véleményét is.

5. AZ INTÉZMÉNY EGÉSZSÉGÜGYI SZOLGÁLTATÁSÁHOZ KAPCSOLÓDÓ ADATKEZELÉSEK ÁLTALÁNOS SZABÁLYAI

27. Az egészségügyi szolgáltatás során kezelt személyes adatok

141. Az Intézmény jogszabályon és alapító okiratának rendelkezésein alapuló speciális ellátási kötelezettségéből fakadó egészségügyi szolgáltatás, azaz járó- és fekvőbeteg ellátás, valamint

az ellátásnak az egészségbiztosító/finanszírozó részére történő jelentése során kezel személyes és egészségügyi adatokat.

142. A Szabályzat célja az Intézmény közfeladatainak ellátása, működése során kezelt valamennyi személyes adat, illetve különleges személyes adat védelme kiemelten a betegellátás folyamataiban, a humánerőforrás gazdálkodás, a gazdasági tevékenység, a finanszírozási folyamatok és az iratkezelés során.

143. Az Intézmény a GDPR 6. cikk és GDPR 9. cikk szerinti jogalapokra hivatkozva pontosan meghatározott adatkezelési célok elérése érdekében kezel személyes adatokat. Az önkéntes hozzájáruláson alapuló adatkezelések esetében az érintettek e hozzájárulásukat az adatkezelés bármely szakában visszavonhatják, amennyiben a jogszabály, vagy a vonatkozó érdekmérlegelési tesztek alapján az Intézmény ezt megtagadhatja. Bizonyos esetekben a megadott adatok egy körének kezelését, tárolását, továbbítását jogszabályok teszik kötelezővé.

144. Az Intézménynél végzett adatkezelés célja az egészség megőrzésének, javításának, fenntartásának előmozdítása, a betegellátó eredményes gyógykezelési tevékenységének elősegítése, ideértve a szakfelügyeleti tevékenységet is, az érintett egészségi állapotának nyomon követése, a népegészségügyi, közegészségügyi és járványügyi érdekből szükségessé váló intézkedések megtétele, a létfontosságú rendszerek védelme, valamint a betegjogok érvényesítése.

28. Egészségügyi adatok kezelésének általános adatbiztonsági szabályai

145. Az Intézményben üzemelő klinikai programokkal csak az arra jogosult személy dolgozhat. Mivel a beteg személyi és ápolási adatai kiemelt védelmet élveznek, ezért biztosítani kell nem csak a programokkal dolgozó személyek azonosítását, de a számukra megengedett műveletek szabályozhatóságát is. Új dolgozó felvételekor a Munkahelyi vezető írásban közli az informatikai csoport megbízott munkatársával (Intézményi rendszergazda) a dolgozó nevét, beosztását, (orvos esetében - titulusát, orvosi pecsétszámát), munkakörét és a munkavégzés helyét. A fenti adatok alapján az Intézményi rendszergazda előállítja a felhasználói belépési jogosultságokat és hozzáférési listát a megadott munkahelyekhez.

146. A medikai rendszerben tárolt adatok védelméért az Intézmény adatvédelmi tisztviselője felelős. Betegdokumentációról kért másolatok nyilvántartása az erre kijelölt személy feladata. A medikai rendszerbe való belépés csak saját felhasználónévvel és jelszóval lehetséges, mely tevékenység minden esetben visszaellenőrizhető és nyomon követhető. A medikai rendszerben való jogosultságok szintjét az egyes foglalkoztatotti körök tekintetében jelen Szabályzat, valamint az Informatikai Biztonsági Szabályzat részletes előírásai tartalmazzák. Az adatok pontosságáért az adatokat származtató és rögzítő munkatárs a felelős. Az adatok bevitelekor az egészségügyi dokumentáció vezetésére vonatkozó szakmai előírások és protokollok rendelkezéseit maradéktalan be kell tartani.

147. Az adatkezelési rendszer működési megbízhatósága tekintetében biztosítani szükséges, hogy az abba adatot rögzítők megfelelő ismeretekkel és munkafegyelemmel rendelkezzenek, a rendszer megfelelőssége folyamatosan ellenőrizve legyen.

148. A számítástechnikai rendszert folyamatosan ellenőrizni és szükség szerint bővíteni kell. Az archív tárolás helyigényét, a rendezett tárolás feltételeit, a tűz – és fizikai megsemmisülés

elleni védelem műszaki feltételeit biztosítani és karbantartani kell. Jogszabályváltozás, vagy egyéb ok miatt szükségessé váló módosítás esetén az adatvédelmi és adatkezelési szabályzat módosítását, korszerűsítését, továbbá a karbantartást az adatvédelmi tisztviselő végzi.

149. Az egészségügyi dokumentáció osztályon való tárolása az illetéktelenek számára hozzáférhetetlen, az adatkezelő, illetve a betegellátó számára pedig hozzáférhető módon kell, hogy történjen. Archiválás esetén az adatkezelés folyamatának meg kell felelnie az Iratkezelési szabályzat előírásainak.

150. Minden munkatárs feladata az eltulajdonítás ellen az alábbi alapelvek betartása, illetve ezek elősegítése, továbbá az érintett munkatársak megfelelő tájékoztatása a jogszabályi háttérről és a jelen szabályzatról. Az ellátás alatti, illetve azzal kapcsolatos dokumentációt követően a dokumentumot olyan helyen kell tartani, ahol az zárható és ilyen esetben be is zárt.

151. A beteg szállítása, más telephelyen vagy rendelőben történő vizsgálata során a dokumentumot személy szerint a vizsgálatért, vagy beavatkozásért felelős, vagy az átvételt intéző egészségügyi dolgozónak kell átadni, borítékban vagy dossziéban. A beteggel kapcsolatos dokumentációk, adatok eltulajdonításának gyanúja esetén az adatvédelmi tisztviselőt kell értesíteni. Tényleges adat eltulajdonításakor jegyzőkönyvet kell felvenni és az adatvédelmi tisztviselőt tájékoztatni kell az eseményről, a jegyzőkönyv egy példányának eljuttatása mellett.

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

153. Az elektronikus iratkezelési szoftver hozzáférési jogosultságainak, az egyedi azonosítóknak, a helyettesítési jogoknak a kiosztásáról és jogszerűségéről a stratégiai Igazgató köteles gondoskodni az informatikai csoport bevonásával.

154. Az egészségügyi szolgálati jogviszonnyal rendelkező munkavállalók esetében az adatok kezelésével, védelmével kapcsolatos feladat-, hatás- és jogköreit a munkaköri leírás tartalmazza. Az Intézmény fokozott biztonsági fokozatba tartozik (betegadatok, személyes adatok és pénzügyi adatok kezelése), általános informatikai feldolgozást végez. Az Intézmény rendelkezik Informatikai Biztonsági Szabályzattal (IBSZ), mely alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát. Meghatározza az egyes folyamatok tekintetében az egyes szereplők kötelezettségeit, valamint az ellenőrzésre jogosultak körét. Az Intézmény rendelkezik a 2013. évi L. törvény 13. §-ában meghatározott feladatok ellátására elektronikus információs rendszer biztonságáért felelős személlyel (IBF).

155. Az egészségügyi dokumentációban az adatokat nem lehet törölni, a hibás adatok kijavítására is csak akképp kerülhet sor, hogy az eredetileg felvett adat is megmaradjon. Az egyes betegadatok kezelésével kapcsolatos részletes szabályokat jelen Szabályzat 5. számú fejezete tartalmazza. Az egészségügyi dokumentációt irattárba történő átadásakor tételesen /kórlap,

lázlap, ápolási lap, dekurzus, lelet, stb./ és lapszám szerint kell átvenni, mely kiadás és betekintés esetén is változatlanul előírás, mely segítségével az adatok megsemmisítése, elvesztése, megváltoztatása megakadályozható.

156. Az eredeti egészségügyi dokumentáció Intézményen kívüli kiadása nem megengedett – ettől az ügyészségi kikérés esetén lehet kizárólag eltérni. Hiányzó egészségügyi dokumentációról – ideértve az elvesztést, megsemmisülést – a Főigazgatót, az orvosigazgatót, valamint Az Intézmény adatvédelmi tisztviselőt a hiány észlelését követően haladéktalanul írásban tájékoztatni kell. Intézményből távozott beteg dokumentációját a távozás napján, különös méltánylást érdemlő, indokolt esetben legkésőbb a távozást követő 2 /két/ munkanapon belül le kell zárni az adatkezelési rendszer sérülése esetére.

157. Az Intézmény rendelkezik a mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi, ügyrendi intézkedések megtételéhez azon eszközökkel, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják. Az informatikai biztonsági feladatok elvégzése az Informatikai csoport felügyelete mellett zajlanak.

158. A gazdasági rendszerekben csak az arra jogosult személy dolgozhat. A programokhoz hozzáférési jog, kizárólag az adott terület vezetőjének előzetes engedélyével adható ki. Az Intézmény belső adatállományaihoz, valamint a géppark távmenedzseléséhez külső hozzáférést csak VPN kapcsolaton és nagyon indokolt esetben, csak a Főigazgató külön tájékoztatása utána az Informatikai vezető engedélyével lehetséges, függetlenül a hozzáférés fizikai voltától (Internet, betárcsázás, stb). A belső hálózat védelmét tűzfalrendszer használatával kell biztosítani; valamint az Internethez történő hozzáférés csak ezen a kapcsolaton keresztül valósulhat meg a belső hálózatot használó számítógépek esetén; a programnak rendelkeznie kell a belülről kifelé és a kívülről befelé irányuló adatforgalom típusonkénti és felhasználónkénti szabályozásának tulajdonságával, valamint szét kell tudnia választani a belső és külső adatforgalmat.

159. Az Intézmény minden számítógépén vírusellenőrző program telepítve van, ugyanígy a szerverek és a tűzfalrendszer vírusellenőrző programmal van ellátva. A vírustámadások veszélyének minimalizálása érdekében a vírusvédelmi rendszer napi többszöri frissítése biztosítva van. Az egyes felhasználók saját felhasználónévvel és jelszóval rendelkeznek, mely bizalmas kezelésére írásbeli nyilatkozattal vállalnak felelősséget. A jelszavakat vagy a jelszófájlokat a hálózaton nyílt, olvasható formában továbbítani tilos. A felhasználói jelszó szerkezeti szabályaival (bonyolultság) szemben támasztott követelményeket minden esetben az határozza meg, hogy milyen a kiszolgálón tárolt adatok érzékenységi besorolása és ebből következően a kiszolgáló informatikai biztonsági osztályba sorolása.

160. Az Intézmény hálózatára számítógépet, illetve egyéb gyengeáramú berendezést kizárólag az informatikai csoport munkatársai csatlakoztathatnak. A szabályzatnak megfelelően a nem használt végpontokat, illetve aktív eszköz portokat inaktív állapotba kell helyezni. Az egymástól jól elkülöníthető feladatokat ellátó gépeket külön hálózatba kell szervezni.

161. A számítógépes adatállományról naponta történik mentés. Az adatbázis szerverekről éjjel 1 és 3 óra között, elosztottan automatikus mentés történik külső adattárolóra. Az adattároló helye technikai és fizikai védelem alatt álló, önálló helység. A számítógépes hálózatban minden olyan programnak megfelelően dokumentáltnak kell lennie, mellyel a védett adat feldolgozása történik. A képernyős adatmegjelenítés titokvédelem szempontjából

adattovábbító eszköznek minősül, ezért minősített adat feldolgozása során a helységben csak a betekintésre jogosult tartózkodhat.

162. Az Intézményben biztosított az adatkezelési rendszerek tűzvédelmi szempontból történő védelme. Az adat tartalmú számítástechnikai berendezések Intézményből történő kiszállítása csak Főigazgatói engedéllyel lehetséges. A különleges védelmet igénylő informatikai eszközök helységébe csak az arra jogosult, ellenőrzött belépési renddel léphet be (riasztó berendezés). Az adatok védelmét a feldolgozás, adattovábbítás és tárolása során megfelelően biztosítani kell. A biztonsági okból előállított másolati adathordozókat az eredetitől területileg távol kell tartani.

163. A megsérült, elveszett adatok visszaállítását és annak mértékét – a lehetőségek felmérésével, indoklásával és mérlegelésével – a vezetőkkel egyeztetve az adatvédelmi tisztviselő rendeli el írásban. Amennyiben a visszaállítás – reális módon – nem valósítható meg, arról az adatvédelmi tisztviselő írásos feljegyzést készít, melyet az iktatási rendszerben „Adatvédelem" iktatási jelzéssel tartanak nyilván. A visszaállításról – amennyiben az méltányos és megoldható -, a mulasztásért felelős köteles gondoskodni. A méltányosság és a személyes felelősség eldöntése az adatvédelmi tisztviselő hatáskörébe tartozik.

164. Minden foglalkoztatott kötelezettsége az Intézmény által kiadott szabályzatok előírásainak betartása és betartatása. Betegellátás során, valamint azt követően gondoskodni kell a dokumentáció folyamatosan ellenőrizhető elhelyezéséről. Amennyiben az ellátott átszállításra kerül más telephelyre, vagy intézménybe, a betegdokumentációt zárt borítékban vagy dossziéban kell átadni – összhangban az Iratkezelési szabályzat előírásaival. Amennyiben felmerül az adatok eltulajdonításának gyanúja, azonnal, de legkésőbb a következő munkanapon értesíteni kell a Belső Adatvédelmi Felelőst; tényleges eltulajdonítás esetén jegyzőkönyv felvételét követően, annak egy példányát el kell juttatni hozzá. Az elektronikus medikai rendszerben rögzített adatokért Az Intézmény Informatikai vezetője felelős.

165. Az Intézmény adatvédelmi tisztviselője, a belső adatvédelmi felelős, valamint az Informatikai vezető a mindenkori Főigazgató megbízásából jogosult ellenőrizni a felhasználókat. Az adatkezelési rendszerbe minden felhasználó csak és kizárólag felhasználónév és jelszó segítségével léphet be, mely minden esetben rögzíthető és visszakereshető.

166. A személyazonosító adatok felvétele a Betegfelvételi ablakban történik, melyre az ellátás során az ellátásban részt vevők – elsősorban az adminisztrátorok, kezelőorvos – jogosult és köteles. Amennyiben az egészségügyi dokumentációban szereplő adat hibás, utólagos javítására csak akképp kerülhet sor, hogy az eredetileg felvett adat is megállapítható legyen,

167. Az adatokról, s egyben a keletkezett dokumentációról másolat kérhető, melynek részletes szabályait az Intézmény Iratkezelési szabályzata tartalmazza. Az egészségügyi dokumentáció részeként meg kell őrizni az alábbiakat: az egyes vizsgálatokról készült leletek, gyógykezelés és konzílium során keletkezett iratok, ápolási dokumentáció, képalkotó diagnosztikai eljárások felvételeiről készült leletek. A személyazonosító adatok a medikai rendszerbe a betegfelvétel során kerülnek be, mely folyamat alapja a hatósági szervek alapján kiadott, személyazonosságot, illetve jogosultságot igazoló okmányok bemutatása. A gyógykezelés során keletkezett adatok az ápolási és gyógyítási tevékenységben részt vevők által rögzített tények.

168. Személyes adatok csak és kizárólag hatósági igazolvány bemutatása alapján kerülhetnek be a rendszerbe. A felvett adatoknak hiteleseknek, pontosaknak, teljeseknek és időszerűeknek kell lenniük; azok felvétele és kezelése tisztességes, törvényes, pontos, teljes és időszerű kell, hogy legyen. A diagnózis és beavatkozás kódoknak az ellenőrzésére az ellátást végző orvos köteles, melyre az adatbevitellel egyidejűleg kell, hogy sor kerüljön, de legkésőbb az ellátott Intézményben történő távozásáig. Az Intézmény által használt medikai rendszer elektronikus alapon rögzíti az ellátottról, valamint a vele kapcsolatban felvett adatokat. Intézményünkben az azonosító adatok felvételét az adminisztrátorok és orvosírnokok végzik, míg az ellátásra és az egészségügyi adatokat az ellátást végző orvosok. Az egyes adatok adatkezelési rendszerbe történő bekerülése, illetve az adatkezelési rendszerből történő továbbításának részletes szabályait jelen Szabályzat további fejezetei, dokumentáció másolatának kikérése esetében pedig az Intézmény Iratkezelési szabályzat tartalmazza.

169. Az Intézményben működtetett számítástechnikai rendszert folyamatosan ellenőrizni és szükség szerint bővíteni kell. A rendszer működési műszaki megbízhatóságának alapja a működéssel kapcsolatos visszajelzések és problémák hatékony kezelése, melyért az mindenkori Főigazgató a felelős. Az archívum szükséges helyigényét, valamint a keletkezett dokumentumok tűz-, víz- és egyéb fizikai megsemmisülés elleni védelmét műszaki feltételekkel is biztosítani kell – összehangban az Iratkezelési szabályzat előírásaival.

170. Jelen Szabályzat egyben az Intézmény adatkezelési rendszerének szabályozása, mely összhangban a külső és belső kapcsolódó szabályozási előírásokkal, teljességében szabályozza az adatkezelés rendszerét. Jelen Szabályzat a kiadás időpontjában megvalósuló adatkezelési rendszer működésére vonatkozó szabályokatt tartalmazza, melynek folyamatos fejlesztése, módosítása, javítása, valamint a változó jogszabályi környezetnek való megfeleltetése a belső adatvédelmi felelős az adatvédelmi tisztviselő bevonásával.

171. Mindaddig jelen Szabályzat előírásait kell irányadónak tekinteni a gyakorlati tevékenység során, ameddig annak kihirdetett módosítására sor nem kerül. Az adatkezelők tekintetében attól függően, hogy milyen adatkezelési tevékenységet végeznek, tevékenységüket jelen Szabályzat további fejezeteiben meghatározottak szerint végzik. Amennyiben a kórlapok kódolása, adatfeldolgozás, dokumentumok archív tárolását megvalósító feladatokban a feldolgozást és a fejlesztést végző feladatkörök elválasztásra kerülnek, annak tényét dokumentálni szükséges.

172. Az Intézményben folyamatosan biztosítva van az adatkezelők képzése, továbbképzése és konzultációs lehetősége. Jelen Szabályzat hatályba lépését követően minden évben legalább egy alkalommal sor kerül adatvédelmi továbbképzésre.

173. Az Intézmény biztosítja minden szervezeti egység szintű osztályos adatvédelmi felelős számára, hogy a belső elektronikus rendszerébe, vagy az **adatvedelem@osei.hu** e-mail címre nem megfelelőség tapasztalása esetén jelentést küldenek. A jelentésekről az Intézmény belső adatvédelmi felelőse adatvédelmi nyilvántartást vezet az Országos Kórházi Főigazgatóság által biztosított GDPR CERT elektronikus rendszerben.

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

6. AZ ADATVÉDELMI INCIDENSEKRE VONATKOZÓ ÁLTALÁNOS SZABÁLYOK

29. Az adatvédelmi incidens minősítése

175. Adatvédelmi incidens csak akkor következik be, ha az adatbiztonság – akár vétlen, akár szándékos – sérülésével jár és bekövetkezik a személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés:

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

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

176. 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.

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

30. Az adatvédelmi incidens észlelése

178. Az a munkavállaló, aki az Intézmény által kezelt vagy feldolgozott személyes adatokkal kapcsolatban, vagy az Intézmény szerződéses partnere által kezelt vagy feldolgozott személyes adataival kapcsolatban adatvédelmi incidenst vagy annak gyanúját észleli, köteles azt haladéktalanul bejelenteni az adatvédelmi tisztviselőnek, a belső adatvédelmi felelősnek és a szervezeti egység vezetőjének az [adatvedelem@osei.hu] e-mail címen, vagy az intraneten erre a célra létrehozott űrlapot kitölteni. Az előbbieken túli egyéb bejelentő az

Intézmény elektronikus elérhetőségén vagy az Intézmény honlapján elérhető űrlap kitöltésével jelentheti be az adatvédelmi incidenst.

179. 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.

180. 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.

181. 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 a 167. pontban meghatározott email címen köteles haladéktalanul, de legkésőbb az észlelést követő 24 órán belül értesíteni. A szerződésnek tartalmaznia kell továbbá a közös adatkezelő, illetve az adatfeldolgozó kötelezettségeit adatvédelmi incidens bejelentésében és kivizsgálásában.

182. A nem papíralapon kezelt adattal kapcsolatos incidensek kezelésére az Intézmény mindenkor hatályos Informatikai Biztonsági Szabályzatban, továbbá az Egészségügyi Veszélyhelyzeti Tervben és az Üzemeltetői Biztonsági Szabályzatban 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.

183. Amennyiben a bejelentő nevének elhallgatását kéri, úgy az eljárás folyamatában biztosítani kell adatainak a zárt kezelését, amelyet csak irányítási jogköre alapján a Főigazgató és az adatvédelmi tisztviselő ismerhet meg.

184. A bejelentést tevő személlyel szemben nem alkalmazható semmiféle hátrányos elbánás, jelentéséért – kivéve a szándékosan valótlan tartalommal megtett jelentést – felelősségre nem vonható.

185. A bejelentőt – amennyiben bejelentése alapján az ügy feltárásra került – a szervezeti egység vezetője javaslatára a munkáltatói jogkör gyakorlója erkölcsi elismerésben (munkáltatói dicséret) részesítheti.

186. Külső ellenőrzési szerv által észlelt szabálytalanságra vonatkozó megállapításait az általa készített dokumentáció tartalmazza.

187. Amennyiben külső személy jelzi az adatvédelmet sértő eseményt, a bejelentést rögtzítő szervezeti egység vezetőjének és adatvédelmi felelősének érdemben kell megvizsgálnia és haladéktalanul értesítenie kell a belső adatvédelmi felelőst és az adatvédelmi tisztviselőt.

31. Az adatvédelmi incidens kivizsgálása

188. Adatvédelmi incidens (papíralapú és nem papíralapú adatokra vonatkozóak egyaránt) felmerülése esetén az Intézmény adatvédelmi tisztviselője a belső adatvédelmi felelős, a Stratégiai Igazgató és az informatikai csoport 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.

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

190. Az adatvédelmi incidensről az adatvédelmi tisztviselő értesíti az Intézmény Főigazgatóját és – szükség esetén – az Intézmény PR és sajtókapcsolatokért felelősét.

191. 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.

192. Ha a bejelentés előzetes megvizsgálása azzal az eredménnyel jár, hogy az adatvédelmi incidens nem érintett személyes adatokat, akkor a vizsgálatot le kell zárni.

193. 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 Főigazgatót az előzetes vizsgálat eredményéről, a GDPR 33. cikkében írt Felügyeleti Hatósági bejelentés esetleges szükségességéről, valamint arról, hogy szükséges-e az incidens részletes további vizsgálata.

194. 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 az incidensvizsgáló bizottság tagjait.

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

196. 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.

197. 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 a Főigazgatót és az érintett szervezeti egységek vezetőit.

198. 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.

199. A részletes vizsgálatról szóló jelentést az Intézmény Főigazgatójának kell megküldeni.

200. 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.

201. 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.

202. 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.

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

32. Az érintett tájékoztatása a súlyos adatvédelmi incidensről

204. Súlyos adatvédelmi incidens esetén az Intézmény – az érintettel kapcsolatban rendelkezésére álló elérhetőségeken, ennek hiányában vagy alkalmazásuk lehetetlensége

esetén (GDPR 34. cikk) az Intézmény honlapján közzétett közlemény útján – indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

205. 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.

206. 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.

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

33. Az adatvédelmi incidens hátrányainak megszüntetésére tett intézkedések

208. A munkatárs által önellenőrzéssel észlelt, illetőleg a belső kontrollrendszer keretében az előzetes, utólagos és vezetői ellenőrzés során kiszűrt, elrendelt javítással, helyesbítéssel megszüntethető hiba korrigálása nem igényel szabálytalansági eljárást.

209. A szabálytalanság megszüntetésére a hatáskörrel rendelkező Főigazgatónak kell intézkednie.

210. Nem kell új szabálytalansági eljárást lefolytatni ugyanolyan típusú szabálytalanság észlelésekor, ha már megkezdődött, de még nem zárult le az esettel megegyező, folyamatban lévő eljárás.

211. A szabálytalanság kivizsgálásában nem vehet részt, aki elfogult, akitől az ügy tárgyilagos megítélése nem várható el.

34. Az adatvédelmet sértő esemény megszüntetése

212. Az adatvédelmet sértő eseményt az Intézmény Főigazgatója – amennyiben az lehetséges – saját hatáskörben, az adatvédelmet sértő esemény észlelésétől számítva haladéltalanul, legfeljebb 3 napon belül köteles a megszűntetetés érdekében a szükséges intézkedést megtenni, majd az ügy tanulságairól tájékoztatást nyújt az érintett munkatársak részére, felhívja a figyelmüket az adatvédelmet sértő esemény elkerülésére.

213. Kiemelt jelentőségű adatvédelmet sértő esemény feltételezése esetén az eljárás kezdeményezése irányítási jogköre alapján a Főigazgató hatáskörébe tartozik. Az eljárás lefolytatása és a döntés meghozatalának megalapozása érdekében a Főigazgató közvetlenül kérheti az ügy megvizsgálását az erre a célra létrehozott incidenskezelési bizottságtól.

35. Jogkövetkezmények alkalmazása:

214. A jogkövetkezményekről való döntés kezdeményezése az adatvédelmet sértő esemény megszüntetésére hatáskörrel rendelkező Főigazgató feladata.

215. A jogkövetkezmény jellege szerint lehet:

a/ jogi jellegű (kártérítési eljárás megindítása, szabálysértési vagy büntetőeljárás kezdeményezése az arra feljogosított hatóságnál),

b/ munkajogi (figyelmeztetés, felmondással, azonnali hatállyal történő megszüntetése),

c/ pénzügyi jellegű (pénzbeli juttatás, kifizetés részben vagy egészben történő felfüggesztése, visszakövetelése, behajtása),

d/ szakmai jellegű (belső szabályozás módosítása, szigorításának kezdeményezése, betartásának fokozott ellenőrzése stb.).

216. Amennyiben büntető- vagy szabálysértési eljárás kezdeményezésének szükségessége merül fel, a szükséges intézkedések meghozatala az arra illetékes szervek értesítését is jelenti annak érdekében, hogy megalapozottság esetén az illetékes szerv a megfelelő eljárásokat megindítsa. Az eljárások megindításának kezdeményezésére a Főigazgató jogosult.

217. Ha nyilvánvalóvá vált, hogy az adatvédelmet sértő eseményt bejelentő rosszhiszeműen járt el és alaposan feltehető, hogy ezzel bűncselekményt vagy szabálysértést követett el, másnak kárt vagy egyéb jogsérelmet okozott, adatai az eljárás kezdeményezésére, valamint lefolytatására jogosult részére átadhatók.

36. Az adatvédelmi incidens bejelentése a Felügyeleti Hatóságnak

218. Az adatvédelmi incidensről elsősorban a Felügyeleti Hatóság által a **https://naih.hu/adatvedelmi-incidensbejelento-rendszer** internetes oldalon működtetett elektronikus adatvédelmi incidens bejelentő rendszeren - üzemzavar esetén a bejelentő űrlap elektronikus levél formájában történő elküldésével - kell a bejelentést megtennie az adatvédelmi tisztviselőnek, ennek akadályoztatása esetén levélpostai ajánlott tértivevényes levél útján a Felügyeleti Hatóság postacímére.

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

220. Az adatvédelmi incidensről szóló bejelentéshez a Felügyeleti Hatóság elektronikus űrlapját kell használni, különös tekintettel az alábbiakra:

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.

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

37. Az adatvédelmi incidensek nyilvántartása

222. Az adatvédelmi incidensekről az Intézmény az Országos Kórházi Főigazgatóság által biztosított GDPR CERT elektronikus rendszerben nyilvántartást vezet.

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

38. Az adatvédelmet sértő eseményekkel kapcsolatos intézkedések, eljárások nyomon követése

224. A Főigazgató feladata az adatvédelmet sértő eseményekkel kapcsolatos intézkedések, eljárások nyomon követése során:

a/ az elrendelt eljárások, a meghozott döntések, illetve a megindított eljárások figyelemmel kísérése,

b/ az eljárások során készített javaslatok, intézkedési tervek megvalósítása és a végrehajtás ellenőrzése,

c/ a feltárt adatvédelmet sértő esemény alapján a további bekövetkezési lehetőségek beazonosítása, szükség esetén a belső szabályzatok, illetve jogszabályok módosításának kezdeményezése,

d/ annak vizsgálata, hogy az ellenőrzési nyomvonalban rögzített eljárás az adott adatvédelmet sértő eseményt miért nem szűrte ki, indokolt esetben gondoskodni kell az ellenőrzési nyomvonal felülvizsgálatáról, helyesbítéséről.

225. Amennyiben az intézkedések végrehajtása során megállapítást nyer, hogy az alkalmazott intézkedések nem elég hatásosak, az adatvédelmet sértő esemény megszüntetéséért felelős vezető, kiemelt jelentőségű esetben az irányítási jogkörrel rendelkező Igazgató további intézkedést rendel el.

7. ADATKEZELÉS SORÁN ALKALMAZANDÓ MÓDSZERTANOK

39. Az érdekmérlegelési teszt elvégzésének módszertana

226. 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.

227. Az érdekmérlegelési tesztet a belső adatvédelmi felelőssel együttműködve a tervezett adatkezelésért felelős szervezeti egység adatvédelmi felelőse végzi el. Az érdekmérlegelési tesztet írásban kell elvégezni. Az elkészült dokumentumot 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.

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

229. Az érdekmérlegelési teszt részei:

a/ a tervezett adatkezelés leírása és az annak keretében kezelni tervezett személyes adatok (körének vagy típusának) meghatározása,
b/ szükségesség vizsgálata (Milyen alternatív megoldások léteznek?)
c/ az adatkezelő vagy azon harmadik fél jogos érdekének azonosítása, akinek az adatkezelés érdekében áll (Miért szükséges az adatkezelés?),
d/ az érintett érdekeinek, jogainak azonosítása (Arányban van-e az adatkezelés az érintett magánszférájának korlátozásával?),
e/ az adatkezelő (vagy harmadik fél) és az érintettek érdekeinek összevetése,
f/ a személyes adatok védelme biztosítékainak leírása, garanciák beépítése az adatkezelés folyamatába
g/ az érdekmérlegelési teszt eredménye.

40. Az adatvédelmi hatásvizsgálat elvégzésének módszertana

230. Ha az adatkezelés valamely, különösen új technológiákat alkalmazó típusa valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve az adatkezelést megelőzően adatvédelmi hatásvizsgálatot kell végezni. Olyan, egymással hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló kockázatokkal járnak,

egyetlen adatvédelmi hatásvizsgálat (továbbiakban: hatásvizsgálat) keretei között is értékelhetők.

231. A hatásvizsgálat elvégzésének szükségességéről a tervezett adatkezelésért felelős szervezeti egység adatvédelmi felelőse a belső adatvédelmi felelős útján szükség esetén kikéri az adatvédelmi tisztviselő véleményét.

232. A hatásvizsgálat elvégzését a tervezett adatkezelésért felelős szervezeti egység adatvédelmi felelőse koordinálja. 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 adatvédelmi felelős úgy ítéli meg, hogy az adatkezelés nem jár magas kockázattal a természetes személyek jogaira, úgy ezt meg kell indokolnia és – ha ez lehetséges – dokumentumokkal igazolnia a mellőzés okait. A 32. pont rendelkezéseit jelen esetben is alkalmazni kell. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

233. Adatvédelmi hatásvizsgálatot a GDPR 35. cikk (3) bekezdésében, illetve a Nemzeti Adatvédelmi és Információszabadság Hatóság által közzétett jegyzékben[1] szereplő adatkezelések, adatkezelési műveletek esetén kell végezni.

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

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

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

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

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

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

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

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

f/ az adatkezelés folyamatának a leírását.

237. 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.

[1] https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf

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

239. A hatásvizsgálat negyedik része tartalmazza a tervezett adatkezelés értékelését:
   a/ a 225. 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.

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

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

41. Belső adatvédelmi ellenőrzési eljárás elvégzésének módszertana

242. 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.

243. A belső adatvédelmi felelős és az adatvédelmi tisztviselő éves ellenőrzési tervet készítenek. Az éves ellenőrzési tervnek az ellenőrzés alá vont szervezeti egység nevét és az ellenőrzés várható időpontját, továbbá az ellenőrzés tárgykörét kell tartalmaznia. Az éves ellenőrzési terveket úgy kell elkészíteni, hogy négyéves időtartam alatt lehetőség szerint minden adatkezelésért felelős szervezeti egység ellenőrzésére sor kerüljön. Az éves ellenőrzési tervet legkésőbb adott év február 28. napjáig kell elkészíteni és az Intézmény Főigazgatója részére bemutatni.

244. Az éves ellenőrzési tervet az Intézmény Főigazgatója hagyja jóvá.

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

246. 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.

247. Az adatvédelmi tisztviselő az ellenőrzés megtörténtéről jegyzőkönyvet készít, melyet az ellenőrzött szervezeti egység vezetőjével mindketten aláírnak. A jegyzőkönyv az ellenőrzött szervezeti egység, valamint annak vezetője nevét, az ellenőrzés lefolytatásának tényét, annak időpontját és időtartamát, továbbá a 246. pont szerinti tevékenység során rögzített tényeket, megállapításokat, információkat tartalmazza.

248. Az adatvédelmi tisztviselő a lefolytatott ellenőrzésről vizsgálati jelentést készít, melynek mellékletét képezi az ellenőrzésről készült jegyzőkönyv. A vizsgálati jelentés tartalmazza az adott szervezeti egységnél vizsgált körülményeket, adatokat, valamint az adatvédelmi tisztviselő megállapításait. A vizsgálati jelentés tervezetére a szervezeti egység vezetője 10 napon belül észrevételt tehet. Az észrevételek közlésének elmaradását úgy kell tekinteni, hogy a szervezeti egység vezetője a vizsgálati jelentés megállapításait elfogadja.

249. Ha az adatvédelmi tisztviselő megállapítja, hogy az adatkezelés az ellenőrzés alá vont szervezeti egységnél nem a belső szabályzatoknak vagy jogszabályoknak megfelelően történik, javaslatot tesz a szabályszerű adatkezelés – meghatározott határidőn belüli – helyreállítására. Az adatvédelmi tisztviselő javaslata alapján megtett intézkedésekről a szervezeti egység vezetője tájékoztatja az adatvédelmi tisztviselőt. Az adatvédelmi tisztviselő a megtett intézkedéseket, illetve azok betartását bármikor jogosult ellenőrizni (utóellenőrzés). Az utóellenőrzésre a 245-248. pontban foglaltakat alkalmazni kell.

250. Az adatvédelmi tisztviselő rendkívüli ellenőrzést is lefolytathat, ha adatvédelmi szempontból indokolt, különösen, ha a személyesadat-kezeléssel érintettek száma jelentős. Rendkívüli ellenőrzésnek minősül az éves ellenőrzési tervben nem szereplő ellenőrzés. A rendkívüli ellenőrzést az Intézmény Főigazgatója előzetesen engedélyezi. A rendkívüli ellenőrzésre a 246-248. pont rendelkezéseit is alkalmazni kell.

251. Az adatvédelmi tisztviselő az adatvédelmi ellenőrzés (ideértve a 249. pont szerinti utóellenőrzést is) lefolytatását követően tájékoztatja az Intézmény Főigazgatóját az adatvédelmi ellenőrzés adatairól és eredményeiről. A Főigazgató tájékoztatása történhet szóban vagy a 248. pont szerinti, a vizsgált szervezeti egység vezetője által elfogadott vizsgálati jelentés megküldésével is. Az adatvédelmi tisztviselő jelen Szabályzat szerint az Intézmény adatvédelmi helyzetéről szóló éves jelentése tartalmazza az adott évben lefolytatott adatvédelmi ellenőrzésekkel és utóellenőrzésekkel kapcsolatos összegző információkat és megállapításokat is.

8. ZÁRÓ RENDELKEZÉSEK

252. Jelen Szabályzat a kiadásáról szóló Főigazgatói utasítás aláírását követő napon lép hatályba.

9. MELLÉKLETEK

9.1. <u>számú melléklet – Jelen Szabályzathoz kapcsolódó jogszabályok, belső szabályzatok, dokumentumok</u>

Jogszabályok
Magyarország Alaptörvénye VI. cikk (Alaptörvény)
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 (GDPR)
2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)
2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)
41/2015. (VII.15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről (Ibtvr.)
1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről, és a végrehajtására kiadott jogszabályok (Eüak.)
62/1997. (XII.21.) NM rendelet az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről (Eüakr.)
1997. évi CLIV. törvény az egészségügyről, és a végrehajtására kiadott jogszabályok (Eütv.)
2003. évi LXXXIV. törvény az egészségügyi tevékenység végzésének egyes kérdéseiről (Eütev.)
1997. évi LXXXIII. törvény kötelező egészségbiztosítás ellátásairól, és a végrehajtására kiadott jogszabályok (Ebtv.)
2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Lrtv.)
356/2008/. (XII. 31.) kormányrendelet a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény egészségügyi Intézményekben történő végrehajtásáról (Kjtvr.)
2019/1937/EU európai parlament és tanács irányelv az uniós jog megsértését bejelentő személyek védelméről szóló
2013. évi XXV. törvény a panaszokról, a közérdekű bejelentésekről, valamint a visszaélések bejelentésével összefüggő szabályokról
2020. évi C. törvény az egészségügyi szolgálati jogviszonyról (Eszjtv.)
528/2020. (XI.28.) Korm. rendelet az egészségügyi szolgálati jogviszonyról szóló 2020. évi C. törvény végrehajtásáról (Eszjtvr.)

Jogszabályok
39/2016. (XII. 21.) EMMI rendelet az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról (EESZTr.)
370/2011. (XII. 31.) kormányrendelet a költségvetési szervek belső kontrolrendszeréről és belső ellenőrzéséről (Bkr.)
1994. évi XXXIV. törvény a rendőrségről (Rtv.)
1995. CXXV. törvény a nemzetbiztonsági szolgálatokról (Nbtv.)
1995. évi LXVI. törvény a közokiratokról, a közlevéltárakról és a magánlevéltári anyag védelméről (Kltv.)
38/2012. (III.12.) kormányrendelet a kormányzati stratégiai irányításról
1996. évi XX. törvény a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról
2012. évi LXIII. törvény a közadatok újrahasznosításáról
2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről
2017. évi CI. törvény a döntés-előkészítéshez szükséges adatok hozzáférhetőségének biztosításáról
335/2007. (XII. 30.) kormányrendelet a döntés-előkészítéshez szükséges adatok hozzáférhetőségének biztosításáról szóló 2007. évi CI. törvény végrehajtásáról
1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során
86/1996. (VI. 14.) kormányrendelet a biztonsági okmányok védelmének rendjéről
38/2011. (III.22.) kormányrendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról
2006. évi CXXXII. törvény az egészségügyi ellátórendszer fejlesztéséről
337/2008. (XII. 30.) kormányrendelet az egészségügyi ellátórendszer fejlesztéséről szóló 2006. évi CXXXII. törvény végrehajtásáról
305/2005. (XII. 25.) kormányrendelet az közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról
1/2005. (EüK.1.) EüM számú irányelve az egészségügyi intézetek keretében fekvőbeteg ellátásban részt vevők részére szükséges betegazonosító rendszer működéséről
2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól
2011. évi CLXXXVII. törvény a szakképzésről

Jogszabályok
16/2010. (IV. 15.) EüM rendelet az egészségügyi felsőfokúszakirányú szakmai képzés részletes szabályairól
162/2015. (VI. 30.) Korm. rendelet az egészségügyi felsőfokú szakirányú szakképzési rendszerről, a Rezidens Támogatási Program ösztöndíjairól, valamint a fiatal szakorvosok támogatásáról
22/2012. (IX. 14.) EMMI rendelet az egészségügyi felsőfokú szakirányú képesítés megszerzéséről
230/2012. (VIII. 28.) Korm. rendelet a felsőoktatási szakképzésről és a felsőoktatási képzéshez kapcsolódó szakmai gyakorlat egyes kérdéseiről
2011. évi CCIV. törvény a nemzeti felsőoktatásról
2019. évi XIX. törvény a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény módosításáról
18/2005. (XII.27.) IHM rendelet a közzétételi listákon szereplő adatok közzétételéhez szükséges közzétételi mintákról
12/2001. (I. 31.) Kormányrendelet, a lakáscélú állami támogatásokról
1993. évi XCIII. törvény a munkavédelemről
60/2003. (X.20.) ESzCsM rendelet az egészségügyi szolgáltatások nyújtásához szükséges szakmai minimumfeltételekről
Belső szabályzatok, dokumentumok
Intézmény Szervezeti és Működési Szabályzata
Intézmény Informatikai Biztonsági Szabályzata
Intézmény közérdekű adatai szolgáltatásának, valamint közzétételének rendjéről szóló Főigazgatói Szabályzat
OKFŐ közérdekű, valamint közérdekből nyilvános adaok közzétételére vonatkozó eljárásrendről szóló Főigazgatói Utasítás
Intézmény Egészségügyi Válsághelyzeti Terve és az Üzemeltetői Biztonsági Terve
Intézmény szabályozó és igazoló dokumentumok készítéséről és közzétételéről szóló szabályzata
Intézmény Iratkezelési szabályzata
Intézmény szervezeti egység szintű osztályos működési rendjei (OMR)
MEES (2.0)

9.2. számú melléklet – GDPR CERT rendszerben vezetett adatkezelési nyilvántartások listája

Megnevezés
B01 Időpont foglalás – beutalóhoz kötött
B02 Időpont foglalás – beutalóhoz nem kötött
B03 Betegfelvétel
B04 Betegellátás
B05 Diagnosztikai tevékenység
B06 Beteg elbocsátás
B07 PACS rendszerben szereplő adatok Eüak. szerinti megőrzési időn túli tárolása
B09 Halálesetekhez kapcsolódó betegellátáson kívüli adminisztrációs tevékenység
B10 Foglalkozás egészségügyi vizsgálat
B11 Tételes finanszírozású gyógyszerek és eszközök nyilvántartása
B12 A pszichiátriai betegekkel kapcsolatos nyilvántartások
B13 Várólista és betegfogadási lista
B17 Beteg egészségügyi ellátásával kapcsolatos panaszok kivizsgálása
B18 Betegszállítás, mentés, halottszállítás
B19 Vényköteles gyógyszerek receptjeinek megőrzése
B26 Fertőző betegek nyilvántartása
B32 EÜ ellátásra vonatkozó egyezményt kötött államokból érkező személyek ellátása-"E" térítési kat.
B34 Gyógyszer támogatással történő rendeléssel összefüggő beteg nyilatkozat
B37 Fokozottan ellenőrzött szerek nyilvántartása
B39 Hozzátartozóval, illetve egyéb értesítendő személlyel kapcsolatos adatkezelés
B40 Személyazonosító karszalag fekvőbetegek számára
B43 COVID-os, karanténban lévő dolgozók nyilvántartása
B44 COVID-os betegek nyilvántartása
B16 Tudományos kutatás céljából történő adatbetekintés nyilvántartása
IT 2 Kamerás megfigyelő rendszer üzemeltetése
J1 A GDPR szerinti érintetti jogok gyakorlásával kapcsolatos intézkedések nyilvántartása
PÜ 2 Projekt dokumentáció

Megnevezés
PÜ 3 Projekt adminisztráció, ill. közpénzekből nyújtott uniós és nemzeti támogatásokkal kapcs. ak.
PÜ 8 Finanszírozással kapcsolatos adatkezelés
PÜ 12 Nagy értékű, országosan még nem elterjedt beavatkozások nyilvántartása
HR 01 Meghívásos eljárás (Eü. szolg. jogviszony betöltésére toborzás, kiválasztás)
HR 02 Toborzás, kiválasztás
HR 04 Eü. szolgálati törvény alapján történő foglalkoztatás
HR 05 Munka Törvénykönyve alapján történő foglalkoztatás
HR 07 Vállalkozási tevékenység formájában foglalkoztatott munkatársak
HR 08 Munkaerő kölcsönzéssel foglalkoztatott munkavállalókhoz kapcsolódó speciális adatkezelés
HR 09 További jogviszonnyal kapcsolatos adatkezelés
HR 10 Foglalkoztatási jogviszony megszűnése
HR 11 Orvosok működési nyilvántartása (HR)
HR 12 Bér- és adóügyek
HR 13 Egyes béren kívüli juttatások
HR 14 A munkába járással kapcsolatos költségtérítés
HR 15 Kiküldetési rendelvények és azok elszámolásával kapcsolatos dokumentumok nyilvántartása
HR 16 Dolgozói tartozások/Tartozásigazolás
HR 20 Munkaidő és távollét nyilvántartás
HR 21 Önként vállat többletmunka nyilvántartás
HR 23 Munkahelyi balesetek nyilvántartása
HR 24 Sugárterhelési nyilvántartás - a személyi dozimetriai adatok helyi nyilvántartása (dolgozók)
HR 25 Munkaruha, védőeszköz
HR 26 Rezidens képzés
HR 27 Továbbképzési kötelezettség nyilvántartása
HR 29 Tanulmányi szerződések nyilvántartása
HR 30 OKFŐI központi továbbképzések
HR 31 Közösségi szolgálat
HR 32 Tanulók szakmai gyakorlatai
HR 34 Teljesítményértékelés
HR 37 Aláírásminta nyilvántartás

Megnevezés
HR 45 Dolgozói e-mail fiókban tárolt, munkavégzéssel összefüggő levelezés
HR 46 Mobil telefon flottával kapcsolatos felhasználó nyilvántartás
HR 50 Egészségügyi szakember-képzés
IT 1 Az IT üzemeltetéshez kapcsolódó személyes adatok
IT 3 Iktatás és iratkezelés
IT 4 Honlapon süti (cookies) kezelés
IT 5 Kórházi számítógépes rendszerben tárolt felhasználói információk és logok megőrzése
IT 7 Távoli eléréssel rendelkező munkatársak nyilvántartása
IT 8 IT magánhasználati engedélyek
IT 9 Vezetékes telefonnal kapcsolatos felhasználó nyilvántartás
Betegjogi képviselő tevékenységével kapcsolatos nyilvántartás
J2 Peres eljárások
J3 Közérdekű adatigényléssel kapcsolatos nyilvántartás
M1 Behajtási engedélyek nyilvántartása
M2 Vagyonvédelmi intézkedések, talált tárgyak
B36 Egészségügyi szolgáltatásra nem jogosult és térítésköteles személy ellátása
PÜ 1 Számlák és az ahhoz kapcsolódó bizonylatok nyilvántartása
PÜ 4 Partnerekhez köthető magánszemélyek adatainak nyilvántartása
PÜ 5 Kintlevőségek nyilvántartása
PÜ 6 Egészségügyi dokumentációk másolási díjával kapcsolatos adatkezelés
PÜ 7 Beteg ingóságaival kapcsolatos letét
PÜ 10 Konzíliumi szolgáltatások
PÜ 11 Közbeszerzésekkel, illetve állami vagyonnal kapcsolatos adatkezelés
PÜ 9 Kontrolling, VIR elemzéshez fekvő- és járóbeteg ellátások teljesítményjelentéseinek kezelése

9.3. <u>számú melléklet – Tájékoztatás adatvédelmi incidensről (minta)</u>

_____ (személyes adat jogosultjának neve)

_____ (személyes adat jogosultjának címe)

<u>tárgy:</u> tájékoztatás adatvédelmi incidensről

Tisztelt _____!

Alulírott,_____ az Országos Sportegészségügyi Intézet (székhely: 1113 Budapest, Karolina út 27.) adatkezelő (a továbbiakban: **Intézet**) képviseletében eljárva ezennel tájékoztatom, hogy az Intézmény 20_____ . napján **adatvédelmi incidenst** szenvedett el. **Az adatvédelmi incidens Az Intézet által Önről kezelt személyes adatokat is érintette, így az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az Ön jogaira és szabadságaira.**

Az adatvédelmi incidens következményeinek megszüntetését és az adatbiztonság helyreállítását megkezdtük, és a **következő intézkedéseket már megtettük:** _____ (intézkedések felsorolása)

A továbbiakban a **következő intézkedések megtételét tervezzük**: _____ (intézkedések felsorolása)

Ezektől függetlenül javasoljuk, hogy az Ön személyes adatainak érintettsége okán a **következő valószínűsített követelményekre készüljön fel, és késedelem nélkül tegye meg a jogai és szabadságai védelme érdekében szükséges intézkedéseket: _____** (lehetséges következmények felsorolása)

Amennyiben további tájékoztatást kér az adatvédelmi incidens és lehetséges következménye tekintetében, **Intézetünk adatkezelési felelősét az alábbi elérhetőségen:**

Adatvédelmi tisztviselő:

név	Dr. Nagy Norbert
e-mail cím	norbert.nagy@infoszakerto.hu

Belső adatvédelmi felelős:

név	Dr. Téglásy György
telefonszám	06 1 488 6100
e-mail cím	adatvedelem@osei.hu

Budapest, 20 _____

Országos Sportegészségügyi Intézet

9.4. <u>számú melléklet – Helyesbítés iránti kérelem (minta)</u>

Tisztelt Adatkezelő!

Alulírott, _____ (név) személyes adatok jogosultja, Az Intézet, mint adatkezelő (a továbbiakban: **Adatkezelő**) részére a következő

k é r e l m e t

terjesztem elő.

Kérem a Tisztelt Adatkezelőt, hogy az Adatkezelő által kezelt és **pontatlan/hiányos személyes adataim** vonatkozásában a jelen nyilatkozatban meghatározottak szerint a személyes adataimat **helyesbítse, illetve egészítse ki** az alábbiak szerint:

Jelenleg kezelt pontatlan személyes adat	Helyesbített, kiegészített személyes adat

A helyesbítés, illetve kiegészítés igazolására szolgáló, a helyes személyes adatot tartalmazó dokumentum másolatot jelen nyilatkozatomhoz **csatolom**.

Kérem a Tisztelt Adatkezelőt, hogy fenti kérelmemet elbírálni szíveskedjen.

Kelt, _____ 20____ év _____ hó _____ nap

_____

Aláírás

9.5. <u>számú melléklet – Tiltakozásra vonatkozó kérelem (minta)</u>

Tisztelt Adatkezelő!

Alulírott, _____ (név) személyes adatok jogosultja, az Intézet, mint adatkezelő (a továbbiakban: **Adatkezelő**) részére nyilatkozom, hogy

t i l t a k o z o m

az adatkezelő adatkezelése ellen az alábbiak szerint:

Tiltakozással érintett személyes adat	Indok (Megfelelő jelölendő)
	a. Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítése. b. Közvetlen üzletszerzés.

Kérem a Tisztelt Adatkezelőt, hogy fenti kérelmemet elbírálni szíveskedjen, és a kért személyes adatot a fenti indokba megjelölt célból a továbbiakban ne kezelje.

Kelt, _____ 20____ év _____ hó _____ nap

_____

Aláírás

9.6. <u>számú melléklet – Adatkezelés korlátozására vonatkozó kérelem (minta)</u>

Tisztelt Adatkezelő!

Alulírott, _____ (név) személyes adatok jogosultja, Az Intézet, mint adatkezelő (a továbbiakban: **Adatkezelő**) részére a következő

k é r e l m e t

terjesztem elő.

Kérem a Tisztelt Adatkezelőt, hogy az Adatkezelő által kezelt alább részletezett **személyes adataimra vonatkozóan végzett adatkezelést korlátozza**:

Adatkezelés korlátozásával érintett személyes adat	**Indok (Megfelelő jelölendő)**
	a. Az érintett vitatja a személyes adat pontosságát. b. Az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését. c. Az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igényeinek előterjesztéséhez, érvényesítéséhez és védelméhez. d. Az érintett tiltakozik az adatkezelés ellen és az adatkezelő jogos indokai elsőbbségének megállapítása szükséges.

Kérem a Tisztelt Adatkezelőt, hogy fenti kérelmemet elbírálni szíveskedjen.

Kelt, _____ 20____ év _____ hó _____ nap

_____

Aláírás

9.7. <u>számú melléklet – Törlés iránti kérelem (minta)</u>

Tisztelt Adatkezelő!

Alulírott, _____ (név) személyes adatok jogosultja, Az Intézet, mint adatkezelő (a továbbiakban: **Adatkezelő**) részére a következő

k é r e l m e t

terjesztem elő.

Kérem a Tisztelt Adatkezelőt, hogy az Adatkezelő által kezelt alább részletezett **személyes adataimat késedelem nélkül valamennyi nyilvántartásából törölje**:

Törölni kért személyes adat	**Törlés indoka (Megfelelő jelölendő)**
	a.) a személyes adatra nincsen szükség abból a célból, amely az adatkezelés alapját képezte; b.) a személyes adatok jogosulja adatkezeléshez hozzájáruló nyilatkozatát visszavonta, és az adatkezelésnek nincs egyéb jogalapja; c.) bebizonyosodik, hogy a személyes adatokat az Intézmény jogellenesen kezelte; d.) jogszabályi kötelezettségnél fogva az Intézmény köteles a személyes adatok törlésére.

Kérem a Tisztelt Adatkezelőt, hogy fenti kérelmemet elbírálni szíveskedjen.

Kelt, _____ 20____ év _____ hó _____ nap

_____

Aláírás