

ADATVÉDELMI TAJÉKOZTATÓ

A Tiszaújváros Városi Rendelőintézet (3580 Tiszaújváros, Bethlen Gábor út 11-13.), továbbiakban „Adatkezelő” vagy „Rendelőintézet”) elhivatott abban, hogy a személyes adatok kezelése során a legnagyobb körültekintéssel járjon el. Ennek megfelelően az Rendelőintézet az általa végzett tevékenységek, a rá vonatkozó jogszabályi kötelezettségek és a pácienseivel, partnereivel fennálló jogviszonyok természetének figyelembe vételével alakította ki - a jogszabályi előírások szerinti - személyes adatok védelmét célzó adatkezelési, adatfeldolgozási, adattörlési szabályozását és belső rendszerét.

Az alábbi tájékoztató részletes leírást tartalmaz arra vonatkozóan, hogy az Rendelőintézet hogyan és milyen célból kezeli az Ön (továbbiakban: „Érintett”) személyes adatait és arra, hogy milyen jogok illetik meg Önt az Rendelőintézet által kezelt adatai vonatkozásában.

1. Az adatkezelő

Az adatkezelő neve és elérhetősége:

Tiszaújváros Városi Rendelőintézet, 3580 Tiszaújváros, Bethlen Gábor út 11-13.;

Tel.: +36-49-544-600;

E-mail: rendelo@tujvaros.hu

Közös adatkezelő: nincs.

Az adatkezelő képviselője: dr. habil Papp Miklós PhD főigazgató

Adatvédelmi tisztviselőnek a neve és elérhetősége: Biró Gergely, ITSecure Kft. 1012 Budapest, Logodi u 54., Tel.: +36-1-799-1212;

E-mail: dpo@itsecure.hu

2. Az adatkezelés jogalapja, célja, adatok kezelésének időtartama

A Tiszaújváros Városi Rendelőintézet adatkezelési tevékenységének alapvető célja és rendeltetése, a költségvetési szerv Alapító Okirata és a vonatkozó hatályos jogszabályi rendelkezések szerint, az egészségügyi közfeladat ellátásának biztosítása, valamint a jogszabályi rendelkezésekben foglalt kötelezettségeinek (kiemelten: egészségügyi szolgáltatás biztosítása, és az ezzel kapcsolatos egészségügyi dokumentáció kezelése, humán erőforrás-gazdálkodás és dokumentáció kezelés, gazdálkodási tevékenység folytatása alapító okirata szerint, továbbá informatikai rendszerek működtetése a tevékenységének ellátása érdekében) teljesítése.

A Tiszaújváros Városi Rendelőintézet hatályos Alapító Okirata értelmében, az Rendelőintézet - mint költségvetési szerv - közfeladata: Az egészségügyről szóló 1997. évi CLIV. törvény alapján, ellátási területére kiterjedően a járó- és fekvőbetegek diagnosztikus és terápiás szakorvosi ellátása, rehabilitációja és követéses gondozása, továbbá a közfeladat ellátásával összefüggő gazdálkodási tevékenység folytatása.

A Rendelőintézet az Adatvédelmi szabályzatát az alábbiakban megjelölt jogszabályi rendelkezések és előírások alapján és érvényesülésével határozza meg:

- *Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (General Data Protection Regulation, a továbbiakban. **GDPR**)*
- *Az információs önrendelkezési jogról és az információszabadságról szóló **2011. évi CXII. törvény***
- *Az Egészségügyről szóló **1997. évi CLIV. törvény***
- *Az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló **1997. évi XLVII. törvény***
- *A kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény*
- *az államháztartás működési rendjéről szóló **2011. évi CXCV. törvény (Aht.) 61-62. és***
- *az államháztartásról szóló törvény végrehajtásáról szóló **368/2011. (XII. 31.) Korm. rendelet (Avr.),***
- *A számvitelről szóló **2000. évi C. törvény***
- *A Munka Törvénykönyvéről szóló **2012. évi I. törvény (Mt.)***
- *A közalkalmazottak jogállásáról szóló **1992. évi XXXIII. törvény (Kjt.)***
- *az egészségügyi szolgálati jogviszonyról szóló **2020. C. törvény,***
- *Az egészségügyi tevékenység végzésének egyes kérdéseiről szóló **2003. évi LXXXIV. törvény***
- *A kötelező egészségbiztosítás ellátásairól szóló **1997. évi LXXXIII. törvény.***
- ***39/2016. (XII. 21.) EMMI rendelet** az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról (EESZT)*
- *a költségvetési szervek belső kontrollrendszeréről és belső ellenőrzéséről szóló **370/2011. (XII. 31.) Korm. rendelet (Bkr.) 2-10. §-a***
- *a kormányzati stratégiai irányításról szóló **38/2012. (III. 12.) Korm. rendelet***
- *1996. évi XX. törvény a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról*
- *2012. évi LXII. törvény a közadatok újrahasznosításáról*
- *2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről*
- *2007. évi CI. törvény a döntés-előkészítéshez szükséges adatok hozzáférhetőségének biztosításáról*
- *1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során*
- *86/1996. (VI. 14.) Korm. rendelet a biztonsági okmányok védelmének rendjéről*
- *38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról*
- *337/2008. (XII.30.) Korm. rendelet az egészségügyi ellátórendszer fejlesztéséről szóló 2006. évi CXXXII. törvény végrehajtásáról*
- *335/2007. (XII. 13.) Korm. rendelet a döntés-előkészítéshez szükséges adatok hozzáférhetőségének biztosításáról szóló 2007. évi CI. törvény végrehajtásáról*
- *305/2005. Korm. rendelet a közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról*
- *62/1997. (XII.21.) NM rendelet az egészségügyi és hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről*
- *Az egészségügyi miniszter **1/2005. (EüK.1.) EüM** számon tette közzé **irányelvét** az egészségügyi intézmények keretében fekvőbeteg-ellátásban részt vevők részére szükséges **betegazonosító rendszer** működéséről.*
- *Az Rendelőintézet keretében működtetett betegazonosító rendszer részletes szabályait a betegazonosító karszalag Rendelőintézetben belüli alkalmazására vonatkozó speciális szabály, valamint az Rendelőintézet Házirendje tartalmazza.*

Az Rendelőintézet adatkezelési tevékenységének ellátása során alapvető feladata és kötelezettsége az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról (továbbiakban: GDPR), az Egészségügyről szóló 1997. évi CLIV. törvény (Eütv.), az informatikai önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.), valamint az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (Eüak.), továbbá az adatok védelmével összefüggő hatályos jogszabályok rendelkezéseinek, a Rendelőintézet működtetése keretében történő érvényre juttatása.

Rendelőintézetünk működése során általános és kivételt nem ismerő szabályként a személyes adatok kezelése során érvényesülnie kell azon alapelveknek, miszerint kizárólag olyan személyes adat kezelhető az arra jogosultak részéről, amely az adatkezelés céljának **megvalósulásához elengedhetetlen, a cél elérésére alkalmas, és kizárólag a cél megvalósulásához szükséges mértékben és ideig. Az adatkezelés során maradéktalanul és teljes- körűen biztosítani kell az adatok védelmét a véletlen vagy szándékos megsemmisítéssel, megváltoztatással, nyilvánosságra kerüléssel, vagy illetéktelen személyek hozzáféréseivel szemben.**

3. Az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése:

a) Alapellátás (központi orvosi ügyelet, védőnői szolgálat, iskola-és ifjúság-egészségügyi ellátás, otthoni hospice és otthoni szakápolás)

- **adatkezelési tevékenységeinek felsorolása:** Beteg előjegyzés, Beteg fogadás, Azonosítás, Regisztráció, Anamnézis felvétel, Állapotfelmérés, Gyógykezelés, Elbocsátás, visszarendelés, továbbutalás
- **az adatkezeléssel érintett személyes és egyéb szenitív adatok megjelölése:** Személyes adat (családi és utónév, születési családi és utónév, születési hely, születési idő, anyja születési családi és utóneve, lakcím, TAJ- szám, telefonszám), Egészségügyi adat, genetikai adat
- **az adatkezelés jogalapjának megjelölése:** Az egészségügyről szóló 1997. évi CLIV. törvény; Az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVIII. Törvény; 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során; 62/1997. (XII.21.) NM rendelet az egészségügyi és hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről; GDPR 6. cikk (1) e); GDPR 9. cikk (2) h)
- **az adatkezelés módja, folyamata:** elektronikus, papír alapú
- **folyamatgazda és adatkezelő:** előjegyzést adó személy, házi orvos, védőnői ellátás, ügyelet, asszisztens
- **adatfeldolgozók megjelölése:** előjegyzést adó személy, házi orvos, védőnői ellátás, ügyelet, asszisztens
- **a személyes adatok kezelése során felmerülő, lehetséges kockázatok meghatározása:** Nem megfelelő nyomon követhetőség, téves azonosítás, téves gyógykezelés, adminisztrációs hiba, jogalap nélküli adatkezelés, Informatikai hálózat hibája, tűzkár, vízkár, egészségügyi dokumentációhoz való jogosulatlan hozzáférése, stb.

b) Járóbeteg ellátás

- **adatkezelési tevékenységeinek felsorolása:** Beteg előjegyzés, Beteg fogadás, Azonosítás, Regisztráció, Anamnézis felvétel, Állapotfelmérés, Gyógykezelés, Elbocsátás, visszarendelés, továbbutalás
- **az adatkezeléssel érintett személyes és egyéb szenitív adatok megjelölése:** Személyes adat

(családi és utónév, születési családi és utónév, születési hely, születési idő, anyja születési családi és utóneve, lakcím, TAJ- szám), Egészségügyi adat, genetikai adat

- **az adatkezelés jogalapjának megjelölése:** Az egészségügyről szóló 1997. évi CLIV. törvény; Az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVIII. Törvény; 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során; 62/1997. (XII.21.) NM rendelet az egészségügyi és hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről; 1/2005. (EüK.I.) EüM irányelv a betegazonosító rendszer működéséről; GDPR 6. cikk (1) e); GDPR 9. cikk (2) h)
- **az adatkezelés módja, folyamata:** elektronikus, papír alapú
- **folyamatgazda és adatkezelő:** előjegyzést adó személy, kezelőorvos, asszisztens
- **adatfeldolgozók megjelölése:** előjegyzést adó személy, kezelőorvos, asszisztens
- **a személyes adatok kezelése során felmerülő, lehetséges kockázatok meghatározása:** Nem megfelelő nyomon követhetőség, téves azonosítás, téves gyógykezelés, adminisztrációs hiba, jogalap nélküli adatkezelés, Informatikai hálózat hibája, tűzkár, vízkár, egészségügyi dokumentációhoz való jogosulatlan hozzáférés stb.

c) Fekvőbeteg ellátás

- **adatkezelési tevékenységeinek felsorolása:** Beteg előjegyzés, Anamnézis felvétel, Fizikális vizsgálat, Betegdokumentáció készítése, Beteg vizsgálat, Gyógykezelés, Beavatkozások (), Műtétes beteg kivizsgálása, Műtéti program tervezése, Műtét kivitelezése, Műtéti anyagfelhasználás, Vérkészítmények alkalmazása, Betegazonosítás átadás-átvételkor (betegszállításkor), Postoperatív ellátás, Beteg áthelyezés, tovább utalás, a beteg elbocsátása, zárójelentés készítés,
- **az adatkezeléssel érintett személyes és egyéb szenzitív adatok megjelölése:** Személyes adat (családi és utónév, születési családi és utónév, születési hely, születési idő, anyja születési családi és utóneve, lakcím, TAJ- szám), Hozzá tartozói adatok (hozzátartozó neve, elérhetősége, lakcím, telefonszám), Egészségügyi adat, genetikai adat
- **az adatkezelés jogalapjának megjelölése:** Az egészségügyről szóló 1997. évi CLIV. törvény; Az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVIII. Törvény; 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során; 62/1997. (XII.21.) NM rendelet az egészségügyi és hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről; 1/2005. (EüK.I.) EüM irányelv a betegazonosító rendszer működéséről, GDPR 6. cikk (1) e); GDPR 9. cikk (2) h)
- **az adatkezelés módja, folyamata:** elektronikus, papír alapú
- **folyamatgazda és adatkezelő:** előjegyzést adó személy, felvételt végző orvos, kezelőorvos, ápoló, adminisztrátor, asszisztensek, operáló orvos, műtősnők, műtőssegédek, vérellátó
- **adatfeldolgozók megjelölése:** előjegyzést adó személy, felvételt végző orvos, kezelőorvos, ápoló,
- **a személyes adatok kezelése során felmerülő, lehetséges kockázatok meghatározása:** Nem megfelelő nyomon követhetőség, téves azonosítás, téves gyógykezelés, adminisztrációs hiba, jogalap nélküli adatkezelés, Informatikai hálózat hibája, tűzkár, vízkár, egészségügyi dokumentációhoz való jogosulatlan hozzáférése stb.

d) Képképző diagnosztika

- **adatkezelési tevékenységeinek felsorolása:** Vizsgálatkérés, Vizsgálati képanyag készítése, Leletezés, Leletközlés
- **az adatkezeléssel érintett személyes és egyéb szenzitív adatok megjelölése:** Személyes adat (családi és utónév, születési családi és utónév, születési hely, születési idő, anyja születési családi és utóneve, lakcím, TAJ- szám), egészségügyi adat
- **az adatkezelés jogalapjának megjelölése:** Az egészségügyről szóló 1997. évi CLIV. törvény; Az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVIII. Törvény; 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során; 62/1997. (XII.21.) NM rendelet az egészségügyi és hozzájuk kapcsolódó személyes adatok

kezelésének egyes kérdéseiről, GDPR 6. cikk (1) e); GDPR 9. cikk (2) h)

- **az adatkezelés módja, folyamata:** elektronikus, papír alapú
- **folyamatgazda és adatkezelő:** kezelőorvos, asszisztens
- **adatfeldolgozók megjelölése:** kezelőorvos, asszisztens
- **a személyes adatok kezelése során felmerülő, lehetséges kockázatok meghatározása:** Nem megfelelő nyomon követhetőség, téves azonosítás, téves gyógykezelés, adminisztrációs hiba, jogalap nélküli adatkezelés, Informatikai hálózat hibája, tűzkár, vízkár

e) Központi laboratórium

- **adatkezelési tevékenységeinek felsorolása:** Vizsgálatkérés, Mintavétel, Leletezés, Leletközlés
- **az adatkezeléssel érintett személyes és egyéb szenzitív adatok megjelölése:** Személyes adat (családi és utónév, születési családi és utónév, születési hely, születési idő, anyja születési családi és utóneve, lakcím, TAJ- szám), egészségügyi adat, genetikai adat
- **az adatkezelés jogalapjának megjelölése:** Az egészségügyről szóló 1997. évi CLIV. törvény; Az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVIII. Törvény; 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során; 62/1997. (XII.21.) NM rendelet az egészségügyi és hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről; 1/2005. (EüK.I.) EüM irányelv a betegazonosító rendszer működéséről, GDPR 6. cikk (1) e); GDPR 9. cikk (2) h)
- **az adatkezelés módja, folyamata:** elektronikus, papír alapú
- **folyamatgazda és adatkezelő:** kezelőorvos, asszisztens, labor asszisztensek
- **adatfeldolgozók megjelölése:** kezelőorvos, asszisztens, labor asszisztensek
- **a személyes adatok kezelése során felmerülő, lehetséges kockázatok meghatározása:** Nem megfelelő nyomon követhetőség, téves azonosítás, téves gyógykezelés, adminisztrációs hiba, jogalap nélküli adatkezelés, Informatikai hálózat hibája, tűzkár, vízkár, egészségügyi dokumentációhoz való jogosulatlan hozzáférése stb.

f) Humán erőforrás gazdálkodás

- **adatkezelési tevékenységeinek felsorolása:** állaspályázatok kezelése, kinevezés/ kinevezés módosítás, fenntartás, megszüntetés ügyintézése, illetménnyel/számfejtéssel kapcsolatos feladatok, szabadság megállapítása, lmi-kártérítési felelősség megállapítás, egészségügyi tevékenységre irányuló egyéb szerződések (szabadfoglalkozás, személyes közreműködés), munkáltatói igazolásokkal kapcsolatos feladatok, statisztikai adatszolgáltatások, rezidens oktatással kapcsolatos adatok kezelése, továbbítása,
- **az adatkezeléssel érintett személyes és egyéb szenzitív adatok megjelölése:** pályázat elbíráláshoz szükséges személyi adatok, továbbá végzettségre, szakképesítésre, szakmai gyakorlatra vonatkozó adatok, büntetlen előélet igazolása, szerződő felek szerződéskötéshez személyes adatai, végzettségre, szakképzettségre vonatkozó adatok, előző munkaviszonyok, működési nyilvántartás adatai, kamarai tagságra, távollétre vonatkozó adatok, munkaidő nyilvántartás adatai, munkabérré és egyéb juttatásokra vonatkozó adatok, szerződő felek illetve személyes közreműködő szerződéskötéshez személyes adatai, végzettségre, szakképzettségre vonatkozó adatok, érintett munkavállalók személyes, továbbá munkaviszonyra és bérezésre vonatkozó adatai, munkavállalók személye, végzettségre, szakképzettségre, továbbá munka viszonyra vonatkozó adatai, rezidensek és tutorok személyes, illetve munkaidő adatai, szakmai felelősség biztosítás adatai, munkaköri egészségi alkalmasság igazolása.
- **az adatkezelés jogalapjának megjelölése:** 1992. évi XXXIII. tv. a közalkalmazottak jogállásáról, 356/2008. (XII. 31.) Korm. rendelet a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény egészségügyi intézményekben történő végrehajtásáról, az egészségügyi szolgálati jogviszonyról szóló

2020. C. törvény, 2012. évi I. törvény a munka törvénykönyvéről, 2006. évi XCVII. tv. az egészségügyben működő szakmai kamarákról, 1997. évi CLIV. törvény az egészségügyről, 1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről, 1995. évi CXVII. tv. a személyi jövedelemadóról, 2003. évi LXXXIV. tv. az egészségügyi tevékenység végzésének egyes kérdéseiről, 2016. évi CLV. tv. a hivatalos statisztikáról, 96/2003.(VII.15.) Komi. Rendelet az egészségügyi szolgáltatás gyakorlásának általános feltételeiről, valamint a működési engedélyezési eljárásról, 162/2015. (VI. 30.) Komi, rendelet az egészségügyi felsőfokú szakirányú szakképzési rendszerről, a Rezidens Támogatási Program ösztöndíjairól, valamint a fiatal szakorvosok támogatásáról, jogszabály alapján kötelező adatkezelés vagy hozzájárulás, GDPR 6. cikk (1) a) és c)

- **az adatkezelés módja, folyamata:** elektronikus, papír alapú
- **folyamatgazda és adatkezelő:** munkaügyi előadó, bíráló bizottság tagjai, érintett munkáltatói jogkör gyakorló, jelentő munkatársak, , orvosigazgató, egészségügyi ügyvitel szervező, gazdasági igazgató, intézeti vezető asszisztens és helyettesei
- **adatfeldolgozók megjelölése:** munkaügyi előadó, bíráló bizottság tagjai, érintett munkáltatói jogkör gyakorló, jelentő munkatársak, , orvosigazgató, egészségügyi ügyvitel szervező, gazdasági igazgató, intézeti vezető asszisztens és helyettesei.
- **a személyes adatok kezelése során felmerülő, lehetséges kockázatok meghatározása:** szükségtelenül felvett adatok kezelése, adminisztrációs hiba, pályázat lejárt utáni jogalap nélküli adatkezelés, hibás adatszolgáltatás, adminisztrációs hiba, informatikai hálózat hibája, jogalap nélküli adatkezelés, tűzkár, vízkár, , munkaügyi dokumentációban, illetve személyi anyagban szereplő adat jogosulatlan megismerése

g) Pénzügyi tevékenység

- **adatkezelési tevékenységeinek felsorolása:** jogi személyiséggel rendelkező társaságok azonosító adatainak kezelése, természetes személyek azonosító adatainak kezelése, Intézményi dolgozók személyes adatainak kezelése, Letét kezelés, beteg dokumentációk kezelése, intézményi dokumentációk kezelése, szállítói számlák kezelése
- **az adatkezeléssel érintett személyes és egyéb szenzitív adatok megjelölése:** cégjegyzék szám, adószám, pénzforgalmi jelzőszám, tulajdonosok személyes adatai, székhely-, telephelyadatok, szerződés tárgya, összege, Term. személyek - családi vezeték és utónév, születési adatok, adóazonosító jele, TAJ szám, anyja neve, lakcíme, személyi igazolvány száma, Intézményi dolgozók családi-, vezeték-, és utónév, születési adatok, adóazonosító jele, TAJ szám, anyja neve, lakcíme, személyi igazolvány száma, bankszámla száma, törzsszáma, bérjegyzéke, kifizetett járandóság összege, ápoltak, betegek letéti értékei, leletek, vizsgálatkérő lapok, Vezetői aláírási címpéldányok (MÁK), főkönyvi adatok, bevételi és kiadási adatok, adatszolgáltatási dokumentációk, bevallási dokumentációk, A beérkező számlák 2018. április 1.től digitalizálásra kerülnek. Mindenki számára látható lesz, a számla minden adata, aki elektronikus aláírásra jogosult. az adatkezelés jogalapjának megjelölése: 2011.évi CXII. Trv. Információs önrendelkezési jog, Mt. 2012.évi I. trv. 10§ (1) és (3)., 1997. évi XLVII. Törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről, 4/2013 (1.11) komi, rendelet államháztartási számvitelről, jogszabály alapján kötelező adatkezelés, belső szabályozás, hozzájárulás
- **az adatkezelés módja, folyamata:** elektronikus, papír alapú
- **folyamatgazda és adatkezelő:** betegellátó osztályok, munkaügy, gazdasági csoport, főigazgatói titkárság,
- **adatfeldolgozók megjelölése:** munkaügy, gazdasági csoport betegellátó osztályok, főigazgatói titkárság,
- **a személyes adatok kezelése során felmerülő, lehetséges kockázatok meghatározása:** adminisztrációs hiba, hibás adatkezelés, jogalap nélküli adatkezelés, informatikai hálózat hibája, tűzkár, vízkár, CT-Ecostat hiba, adatok jogalap nélküli továbbítása, GIRO hiba, iratok elvesztése, jogosulatlan számára hozzáférhetővé tétele

h) Informatikai tevékenység

- **adatkezelési tevékenységeinek felsorolása:** Medikai rendszerekkel kapcsolatos hozzáférések kezelése, automatikus adattovábbítás (pl. EESZT), Humánpolitikai rendszerekkel kapcsolatos hozzáférések kezelése, Gazdasági rendszerrel kapcsolatos hozzáférések kezelése, Iratkezelő rendszerrel kapcsolatos hozzáférések kezelése, Kamerarendszerek üzemeltetése, Szállítókkal kapcsolatos adatok kezelése,
- **az adatkezeléssel érintett személyes és egyéb szenzitív adatok megjelölése:** Hozzáféréshez szükséges személyes adatok kezelése (Családi és utónév, pecsétszám, szakképzettség), Hozzáféréshez szükséges személyes adatok kezelése (Családi és utónév, adószám, vagy diákigazolvány szám, e-mail cím, kártyaszám), Hozzáféréshez szükséges személyes adatok kezelése (Családi és utónév, munkahelye, beosztása, kártyaszám), Kamerafelvételek kezelése, esemény esetén a szükséges kimentés elvégzése, Megrendelések, szerződések kezelése, szállítók nyilvántartása
- **az adatkezelés jogalapjának megjelölése:** MT/KJT., Info TV., MT 52./KJT., KJT 1992. XXXIII. tv., Eü. és személyes adatok kezeléséről és védelméről szóló 1997. XLVII. tv., Személyes hozzájárulás, , GDPR 6. cikk (1) a) és c)
- **az adatkezelés módja, folyamata:** elektronikus, papír alapú
- **folyamatgazda és adatkezelő:** Informatikus
- **adatfeldolgozók megjelölése:**

Cég név	Program	Program szerepe
Asseco Central Europe Magyarország Zrt.	MedWorks	Labor rendszer
BÉKER-SOFT International Kft.	Fónix	Tüdőszűrő HIS
SW Controll Group Kft	Kristály	Foglalkozás egészségügyi rendszer
Vitarex Stúdió Kft..	Stefánia	Védőnői nyilvántartó rendszer
Homeo-praxis Bt.	Sámán	Sámán 2000 – Házi orvosi és Házi Gyermekorvosi
Flexys Kft	Flexys	Gyógyászati rendszer
COMPUTREND Zrt.	Ecostat	Gazdálkodási rendszer
	Eiktat	Központi iktatórendszer
GIRO Zrt.	Electra terminál	Központ giro utalási rendszer
OTP Zrt.	Banki utalás	

- **a személyes adatok kezelése során felmerülő, lehetséges kockázatok meghatározása:** jogalap nélküli adatkezelés, Informatikai hálózat hibája, tűzkár, vízkár, informatikai rendszer sérülékenységei

i) Finanszírozási és kontrolling tevékenység

- **adatkezelési tevékenységeinek felsorolása:** Más egészségügyi intézetekkel történő egyeztetés átfedések miatt, Más egészségügyi intézet által küldött számlák ellenőrzése, szerződések kezelése, véleményezése, Teljesítményjelentések fogadása közreműködőktől, Teljesítményjelentések készítése, Elszámoláson alapuló nemzetközi szerződés alapján történő ellátás jelentése, Vállalkozó orvosok teljesítésének ügyintézése, Járó és fekvőbeteg kódolás, Működési engedély, Határozatok,
- Humánpolitikai adatok kezelése (HENYÍR), Eszköz árának visszaigénylésével kapcsolatos adatok kezelése, Hatósággal történő levelezés, Klinikai vizsgálati szerződések, módosítások ügyintézése, Klinikai vizsgálati szerződések, módosítások ügyintézése, Klinikai vizsgálatokkal kapcsolatosan beérkező teljesítésigazolások ügyintézése, Rendelőintézetben belüli adatszolgáltatás, Fizetős beteg felvétele, Táppénz jelentés, NEAK TAJ kérés, Várólista felület kezelése, OBP adatszolgáltatás kezelése, Tétéles eszközök, gyógyszerek jelentése, EU-s betegekkel kapcsolatos adatkezelés
- **az adatkezeléssel érintett személyes és egyéb szenzitív adatok megjelölése:** természetes személyazonosító adat és egészségügyi adat: TAJ, név, szül dátum, a vizsgálat megnevezése, dátum,WHO kód, összeg, kérő osztály kódja, orvos pecsét száma, külső intézet neve, címe, adószám, bankszámlaszám szolgáltatás megnevezése, összeg, intézetünk név, cím, adószáma, Üzleti adatok, székhely, kapcsolattartó, cégjegyzék száma, cégbíróság neve adószám, bankszámla szám, statisztika számjel, Rendelő azonosító, ellátást végző orvos kódja, beutaló orvos munkahelyének azonosítója, beutaló orvos pecsét száma, beutalást megalapozó ellátást igazoló adat, állampolgárság, személyazonosító jel (TAJ- szám), beteg születési dátuma, lakcím irányítószáma és az ellátásra vonatkozó egészségügyi adat, Nyomtatvány azonosító, munkahely azonosító, ellátási forma azonosító, ellátás azonosító, biztosítási azonosító, neme, beteg születési dátuma, vezetéknév, utónév, külföldi biztosító országkód, külföldi biztosító azonosító száma, biztosítási kártya azonosító száma, külföldi biztosító neve, külföldi biztosító címe, Cégnév, székhely, adószám, kórház neve, címe, finanszírozásra/elszámolásra vonatkozó teljesítmény adatok (pontszám, pont/Ft érték, számla összege), Rendelőintézet gazdálkodási adatai, béradatok, szerződéses adatok: bevételi adatok, költség adatok, főkönyvi könyvelés adatai, naturális adatok, Beteg neve, Születési idő, hely, Anyja neve, Beteg lakcíme, Társadalombiztosítási azonosító jel, Útlevelszám, Állampolgárság, Beutaló orvos pecsét számmal, Beutaló munkahely, Kezelő orvos pecsét számmal, Diagnózis, Beavatkozás, Önkéntes/nem önkéntes ellátás, Beteg életelőzménye, (anamnézis), Beteg panaszai, bekerülésének körülménye, Betegnek adott gyógyszerek, egyéb terápia, Vizsgálati leletek, Rendelőintézetben belül hol történt az ellátása korábban. Kapacitás adatok (szervezeti egység kód, megnevezés, szakma neve, szakmakódja, ellátási forma, progresszivitási szint, ügyelet/készenlét, engedély státusza, TEK adatok, szakorvosi-nem szakorvosi óraszám, szerződött ágyszám, rendelési idő), Humánpolitikai adatok (HENYÍR), Egészségügyi szolgáltató 6 jegyű ÁNTSZ azonosítója, Szervezeti egység 9 jegyű ÁNTSZ azonosítója, Szervezeti egység megnevezése, Szervezeti egység típusa, Alkalmazás kezdete, Alkalmazás vége, Alap-nyilvántartási szám, EEICH nyilvántartás típusa, Név, Szerződés szám, Munkakör, Munkarend, Képesítés, Foglalkoztatás jellege, Foglalkoztatási jogviszony típusa, FEOR szám, FEOR név, Közreműködő/személyes közreműködő "KSH" száma, Közreműködő/személyes közreműködő szolgáltató neve, Vezető beosztású munkakör, Nyugdíjas foglalkoztatás, Helyettesítés, A tevékenységet felügyelet alatt végzi, A felügyeletet ellátó személy, alapnyilvántartás száma, A felügyeletet ellátó személy EEKH nyilvántartás típusa, Szervezeti egységben végzett heti óraszám, Önként vállalt többletmunka havi óraszám, Heti óraszám összesen, Tartós távollét oka, Tartós távollét vége, Beültetendő eszköz, Visszaigényelhető összeg, Eszköz forgalmazó adatai, Beteg neve, Születési idő, hely, Anyja neve, Beteg lakcíme, Társadalombiztosítási azonosító jel, Állampolgárság, Beutaló orvos pecsét számmal, Beutaló munkahely, Kezelő orvos pecsét számmal, Diagnózis, Beavatkozás, Önkéntes/nem önkéntes ellátás, Beteg életelőzménye (anamnézis), Beteg panaszai, bekerülésének körülménye, Betegnek adott gyógyszerek, egyéb terápia, Vizsgálati leletek, Rendelőintézetben belül hol történt az ellátása korábban. Dolgozók végzettségét igazoló okirat, Beteg nevét TAJ számát tartalmazó statisztikák, EMMI OTFHÁT Ellenőrzési jegyzőkönyvek, NEAK ellenőrzési jegyzőkönyvek, Mok/MESZK kártya másolatok, Végzettséget igazoló okiratok, Munkaköri leírások, Alkalmassági vizsgálat érvényességének igazolása, cégnév, cím, adószám, vizitdíjak, egyéb szerződéses összegek, beteg neve, születés, TAJ szám, finanszírozási adatok (HBCs, súlyszám,

esetszám, betegszám, NEAK által kifizetett összegek), természetes személyazonosító adat (név, születési idő, személyt azonosító okirat adatai, anyja neve) és egészségügyi adat, felvétel módja, tp. jellege, BNO kód, tp. megszűnés módja, OENO kód, elhunyt személyes adatai, a halál helye, ideje, oka, **halottvizsgálatot végző orvos** neve, pecsétszáma, a szállítás időpontja, munkáltatói adatok név, pecsétszáma, szakvizsga, dátum, szervezeti egység, felírási jogosultságok, Eu-s igazolvány, útlevel/ személyigazolvány/ jogosítvány és azokon szereplő adatok

- **az adatkezelés jogalapjának megjelölése:** jogszabály alapján kötelező adatkezelés, belső szabályozás, Az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVIII. Törvény Rendelőintézeti adatvédelmi szabályzat, Fenntartói kontrolling szabályzat, Az Egészségügyről szóló 1997. évi CLIV. Törvény, "az egészségügyi szolgáltatás gyakorlásának általános feltételeiről, valamint a működési engedélyezési eljárásról" szóló 96/2003.(VII.15.) Korm. Rendelet, Szabályzat Az emberi felhasználásra kerülő vizsgálati készítmények klinikai vizsgálatáról valamint a vizsgálatok végzésének intézeti feltételeiről, Korm. rendelet a várólista alapján nyújtható ellátások részletes szabályairól, 43/1999. (III. 3.) Korm. Rendelet, GDPR 6. cikk (1) c)
- **az adatkezelés módja, folyamata:** elektronikus, papír alapú
- **folymatgazda és adatkezelő:** Beteg kezelésében részt vevő szervezeti egység, Műtő, Betegellátó osztály, EMMI OTFHÁT, NEAK
- **adatfeldolgozók megjelölése:** Beteg kezelésében részt vevő szervezeti egység, Műtő, Betegellátó osztály, EMMI OTFHÁT, NEAK
- **a személyes adatok kezelése során felmerülő, lehetséges kockázatok meghatározása:** jogalap nélküli adatkezelés, adminisztrációs hiba, tűzkár, vízkár, adatvesztés az informatikai rendszerben,

j) Betegfelvétel és betegdokumentáció kezelése

- **adatkezelési tevékenységeinek felsorolása:** betegfelvételi tevékenység, betegelőjegyzés, dokumentáció kikérés teljesítése, egészségügyi dokumentáció archiválása,
- **az adatkezeléssel érintett személyes és egyéb szenzitív adatok megjelölése:** családi és utónév, születési családi és utónév, születési hely, születési ideje, anyja születési családi és utóneve, lakcím, TAJ- szám, törzsszám, diagnózis, hozzátartozó név, cím, telefonszám, külföldi esetén: Eu kártya, Büntett megnevezése, cselekvőképesség,
- **az adatkezelés jogalapjának megjelölése:** 1997. évi XLVII. Törvény
- az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről, 1997. évi CLIV. Törvény az egészségügyről, Egészségbiztosítási ellátásról szóló 1997.évi LXXXIII. Törvény, PTK jogállási tv. éti. tevékenységről (2013. V.), Levéltári törvény, GDPR 6. cikk (1) e)
- **az adatkezelés módja, folyamata:** elektronikus, papír alapú
- **folymatgazda és adatkezelő:** **Betegirányító, szakrendelések** Főigazgatóság
- **adatfeldolgozók megjelölése:** Főigazgatóság, **Betegirányító,-szakrendelések**
- **a személyes adatok kezelése során felmerülő, lehetséges kockázatok meghatározása:** adminisztrációs hiba, jogalap nélküli adatkezelés, téves azonosítás, Informatikaihálózat hibája, tűzkár, vízkár, iratok elvesztése, jogosulatlan számára hozzáférhetővé válása

k) Irattár

- **adatkezelési tevékenységeinek felsorolása:** Egészségügyi dokumentáció nyilvántartása 2013- ig, betegellátással kapcsolatos iratok, irattározása, Igazgatási és jogi iratok irattározása, Gazdasági ügyek iratainak irattározása, Humánpolitikai, munka és társadalombiztosítási ügyek, bérelszámolás iratainak irattározása, Szakmai, tudományos kutatással kapcsolatos ügyek iratainak irattározása, Foglalkozás- egészségügy iratainak irattározása
- **az adatkezeléssel érintett személyes és egyéb szenzitív adatok megjelölése:** Egészségügyi adat, személyazonosító adat (a családi és utónév, leánykori név, a nem, a születési hely és idő, az anya leánykori családi és utóneve, a lakóhely, a tartózkodási hely, a társadalombiztosítási azonosító jel), Minősített adat, egészségügyi adat, személyazonosító adat (a családi és utónév, leánykori név, a nem, a születési hely és idő, az anya leánykori családi és utóneve, a lakóhely, a tartózkodási hely), Cégszámok (név, székhely), pénzügyi adatok, munkaviszonyra vonatkozó adatok
- **az adatkezelés jogalapjának megjelölése:** Az "Egészségügyről" szóló 1997. évi CLIV. Törvény, Az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVIII. Törvény, Köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. Törvény, GDPR 6. cikk (1) e)
- **az adatkezelés módja, folyamata:** papír alapú **folyamatgazda és adatkezelő:** **titkársági munkatárs**
- **adatfeldolgozók megjelölése:** **titkársági munkatárs**
- **a személyes adatok kezelése során felmerülő, lehetséges kockázatok meghatározása:** adminisztrációs hiba, jogalap nélküli adatkezelés, tűzkár, vízkár, kártevők

l) Jogi tevékenység

- **adatkezelési tevékenységeinek felsorolása:** szerződésekkel kapcsolatos ügyintézés, peres ügyintézés, panaszkezelés,
- **az adatkezeléssel érintett személyes és egyéb szenzitív adatok megjelölése:** Intézményi dolgozók személyes adatai, szerződő felek szerződéskötéshez, szerződés teljesítése érdekében szükséges személyes adatai (név, születési név, lakcím, adóazonosító jel, anyja neve, bankszámlaszám, elérhetőség (telefon vagy fax), nyilvántartási szám egyéni vállalkozók esetén) , szerződő felek szerződéskötéshez, szerződés teljesítése érdekében szükséges személyes adatai (működési engedély száma, egészségügyi alkalmasság ideje, bizonyítvány száma, megnevezése) , peres iratokban rögzített személyes adatok (peres felek neve, lakcíme, elérhetősége, peres iratokban szereplő egyéb személyes adata, így különösen: szociális helyzetére, egészségügyi állapotára vonatkozó személyes adatok) , biztosítói ügyintézés (név, születési név, lakcím, elérhetőség, adóazonosító jel), biztosítói ügyintézésrel összefüggő egészségügyi személyes adatok , panaszkezeléshez szükséges dokumentumokban rögzített személyes adatok (név, születési név, anyja neve, lakcím, adóazonosító jel, a panaszban megadott további személyes adatok, így különösen egészségügyi személyes adatok), eseti megkeresések kapcsán szükséges személyes adatok (név, születési név, lakcím, adóazonosító jel, anyja neve, az esettel összefüggésben előadott bármely személyes adat
- **az adatkezelés jogalapjának megjelölése;** az információs önrendelkezési jogról és az információszabadságról szóló 2012. évi CXII. Törvény/Az Európai Parlament és Tanács (EU) 2016/679. rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), A közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény/az egészségügyi tevékenység végzésének egyes kérdéseiről szóló 2003. évi LXXXIV. Törvény, az egészségügyi szolgáltatás gyakorlásának általános feltételeiről, valamint a működési engedélyezési eljárásról szóló 96/2003. (VII. 15.) Korm. Rendelet, A Polgári Perrendtartásról szóló 1952. évi törvény/A polgári per rendtartásról szóló 2016. évi CXXX. törvény/Az államháztartásról szóló 2011. évi CXCV. törvény/Az államháztartásról szóló törvény végrehajtásáról szóló 368/2011. (XII. 31.) Korm. rendelet, az információs önrendelkezési jogról és az információ szabadságról szóló 2012. évi

CXII. Törvény/Az Európai Parlament és Tanács (EU) 2016/679. rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), Az egészségügyről szóló 1997. évi CLIV. törvény/az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről 1997. évi XLVII. törvény, GDPR 6. cikk (1) e)

- **az adatkezelés módja, folyamata:** elektronikus, papír alapú
- **folyamatgazda és adatkezelő:** **Intézeti jogász** Főigazgatói Titkárság
- **adatfeldolgozók megjelölése,** **intézeti jogász** Főigazgatói Titkárság
- **a személyes adatok kezelése során felmerülő, lehetséges kockázatok meghatározása:** adminisztrációs hiba, jogalap nélküli adatkezelés, adatok jogalap nélküli továbbítása, Iratok elvesztése, jogosulatlan személyek számára hozzáférhetővé tétele, Szükségtelenül felvett adatok kezelése, adminisztrációs hiba, Informatikai hálózat hibája, tűzkár, vízkár

4. Adatokhoz való hozzáférés, adattovábbítás

A Rendelőintézet az adatkezelés céljának megfelelő informatikai támogatást alakított ki, amely biztosítja, hogy a személyes adatokhoz csak azon személyek férhessenek hozzá, akiknek ezen adatok kezelése szükséges.

Ezen túlmenően, amennyiben arra az adatkezelés jogalapja alapján szükség van, a Rendelőintézet az általa kezelt adatokat jogosult, illetve köteles az arra jogosult számára továbbítani vagy hozzáférhetővé tenni.

Az Rendelőintézet az általa kezelt személyes adatokat átadhatja a Rendelőintézet szerződéses jogviszonyban álló szolgáltatók (futárszolgálat) részére, ezen személyek feladatainak teljesítéséhez szükséges mértékben és időtartamra, de legfeljebb a fentiekben meghatározott adatkezeléssel azonos mértékben és időtartamra.

Az Rendelőintézet jogosult a birtokában lévő adatok teljes időtartama alatt az adatkezelési tevékenység ellátásába adatfeldolgozót bevonni.

Adattovábbításra a következő esetekben kerülhet sor (egészségügyi ellátóhálózaton belül, illetve kívül):

- más egészségügyi szolgáltatók további ellátás érdekében;
- hatósági, illetve bírósági adatszolgáltatási kötelezettség teljesítése érdekében;
- a jogszabályokban előírt adatszolgáltatási esetekben;
- megkötött szerződés teljesítése vagy a szerződéssel összefüggésben vállalt kötelezettségek teljesítése, illetve ezek ellenőrzése érdekében, ha adott terméket, szolgáltatást a Rendelőintézet valamely más partnerrel közösen biztosítja.

Az adattovábbítások címzettjeiről a Rendelőintézet az érintett személy kérésére információt szolgáltat:

- fenntartói jogokat gyakorló szervek
- társadalombiztosítás terhére végzett egészségügyi ellátás ellátó hálózata (társkórházak)
- társadalombiztosító
- egészségügyi finanszírozó
- adóhatóság
- OTH
- Bíróságok
- Rendőrség
- egyéb hatóságok
- szakképzés

- tudományos kutatások
- statisztikai adatfeldolgozás
- epidemiológiai jelentések
- jogszabályi kötelezettségen alapuló, egészségügyi ellátással összefüggő jelentések (EESZT, illetve rákregiszter, szívinfarktus regiszter, stroke regiszter, stb., várólista jelentés, **implantátum regiszter** stb.)

Az Rendelőintézet biztosítja, hogy a fentiekben meghatározott személyek az adatkezelést a mindenkor hatályos adatvédelmi szabályok és a titokvédelemre vonatkozó törvényi rendelkezések betartása mellett kezeljék.

5. A különböző adatkategóriák törlésére előírányzott határidők:

- egészségügyi dokumentáció megőrzése **az egészségügyi dokumentációt az adatfelvételtől számított 30 évig, a zárójelentést legalább 50 évig kell megőrizni, vényt 5 évig.**
- képalkotó diagnosztikai eljárások felvételeiről készült leletet 30 évig kell megőrizni; a képalkotó diagnosztikai eljárással – 2012. január 1-jét követően - készült felvételt annak készítésétől számított 10 évig kell megőrizni.
- humán erőforrás gazdálkodással és a társadalombiztosítás ellátásaival összefüggő személyes adatok megőrzési ideje 50 év
- pályázatok megőrzési ideje = a pályázat elbírálásának időpontja, azt követően a pályázatokat meg kell semmisíteni (kivéve: amennyiben a pályázó írásban kifejezetten hozzájárul az intézet részére, a pályázat további megőrzéséhez)
- pénzügyi/gazdálkodási adatok (Áht. és Számvetési törvény szerint) = minden szigorú számadású nyomtatványt és pénzügyi dokumentumot (beszámoló, főkönyvi kivonat, számlák) = 8 év (egységesen, a papír alapú és elektronikus dokumentációt egyaránt))
- finanszírozással kapcsolatos dokumentáció 50 év (a zárójelentés megőrzéséhez igazodóan).
- klinikai vizsgálatokkal kapcsolatos dokumentáció = a vizsgálat lezárásától számított 15 év;

6. Ha lehetséges, a 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

Az **adatkezelő és az adatfeldolgozó** a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével **megfelelő technikai és szervezési intézkedéseket hajt végre** annak érdekében, **hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja**, ideértve, többek között, adott esetben:

- a személyes adatok álnevesítését és titkosítását;
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

A megfelelő szintű adatbiztonság megvalósítása érdekében, az alkalmazandó technikai és szervezési intézkedéseket az Rendelőintézet Informatikai Biztonsági Szabályzata tartalmazza, mely követelményeket és előírásokat az adatfeldolgozóknak minden esetben alkalmazni kell. Az adatfeldolgozók ezen előírásoktól kizárólag szigorúbb és az adatbiztonság megvalósítása érdekében hatékonyabb előírásokat alkalmazhatnak, melyekről az adatkezelőt tájékoztatni kötelesek.

A biztonság megfelelő szintjének meghatározásakor kifejezetten **figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáféréséből** erednek.

A kockázatfelméréseket az Intézmény - és szervezeti egységei - a hatályos kockázatkezelési szabályzatának megfelelően folyamatosan végzi el.

A lehetséges technikai és szervezési intézkedések

a) Személyes adatok álnevesítése és titkosítása

A személyes adatokat oly módon kell elkülöníteni a kezelt adatoktól, hogy a kezelt adatokat a külön, biztonságosan tárolt többletinformáció nélkül ne lehessen azonosított vagy azonosítható személyhez rendelni. Szimmetrikus és aszimmetrikus kulcsokkal kell titkosítani a személyes adatokat.

b) A rendszerek és szolgáltatások bizalmas jellege, integritása, rendelkezésre állása és ellenálló képessége

Az alábbi intézkedésekkel kerül biztosításra a személyes adatok bizalmas jellege és az integritás:

A hozzáférés ellenőrzése:

Az épületek - lehetőség szerint - biztonsági besorolásuk alapján, jól felépített beléptetési koncepcióban meghatározott beléptető rendszerrel kerüljenek felszerelésre. Lehetőség szerint minden épületben kártyaolvasós beléptetési rendszert tartalmazó ellenőrzési intézkedések kerüljenek alkalmazásra. Biztonsági besorolástól függően az ingatlanok, épületek, illetve konkrét területek biztonságáról további intézkedésekkel is lehet gondoskodni. Ilyen intézkedések például a különleges hozzáférési profilok, a biometria, a személyi azonosító kódok (PIN) bevitelére szolgáló billentyűzetek, a DES hardverkulcsok, a külön belépési kódok, a videokamerás megfigyelőrendszerek és az élőerős őrzés. Mindenki egyedileg kap hozzáférési jogosultságot, az Informatika által meghatározott feltételek alapján. Ezen intézkedéseket a harmadik személyekre is vonatkoztatni kell.

A rendszerhozzáférés ellenőrzése:

Az adatkezelő rendszerekhez kizárólag azok a hitelesített felhasználók férhetnek hozzá, akik a feladatkörük alapján erre felhatalmazást kaptak, lehetőleg a következő biztonság-technikai intézkedések alkalmazása mellett: Az adatok titkosítása, (legalább 8 karakterből álló, rendszeres időközönként automatikusan lejáró) egyéni jelszó hozzárendelése, PKI- rejtjelzett munkavállalói azonosító kártyák, inaktivitás esetére jelszóval védett képernyővédők, behatolásjelző rendszerek és behatolás megelőző rendszerek, rendszeresen frissített vírusvédők és kémprogram-szűrők a hálózaton, valamint az egyes számítógépeken és mobil eszközökön.

Az adatokhoz való hozzáférés ellenőrzése:

A személyes adatokhoz hozzáférési jogosultság feladatkörök szerinti engedélyezési rendszer szerint adható. Olyan felhasználó-kezelő rendszert kell lehetőség szerint kialakítani, amely a felhasználói adatbázishoz hozzárendeli a megfelelő jogosultságokat és amelyből az adatkezelő rendszerek a hálózaton keresztül központilag kérhetnek le adatokat. Ezenkívül az adatok titkosítása megakadályozza a személyes adatokhoz való jogosulatlan hozzáférést. A hozzáférési jogosultságok kiosztása mindig az adott szervezeti egység vezetőjének kérése alapján történik, főigazgatói jóváhagyással.

Az adattovábbítás ellenőrzése:

Lehetőség szerint zárt hálózatok felállításával és adattitkosítási eljárásokkal kell védeni az elektronikus kommunikációs csatornákat. Az adathordozók fizikai szállítása olyan ellenőrizhető szállítási folyamatok segítségével történik lehetőség szerint, amelyek megakadályozzák az adatokhoz való jogosulatlan hozzáférést, illetve a logikai veszteséget. Az adathordozókat az adatvédelmi rendelkezéseknek megfelelően

kell kivonni a forgalomból.

A következő intézkedésekkel gondoskodunk a rendszerek és szolgáltatások állandó rendelkezésre állásáról és megbízható működéséről:

A rendszerek és szolgáltatások rendelkezésre állása és ellenálló képessége akként kerül biztosításra, hogy a kulcsfontosságú informatikai és hálózati elemek lehetőség szerint elszigetelésre kerülnek, gondoskodni kell megfelelő biztonsági mentésről és redundanciáról, redundáns villamosenergia-rendszerek alkalmazásáról, és rendszeresen tesztelésre kerülnek a rendszerek és szolgáltatások.

c) A személyes adatok rendelkezésre állása és elérése incidensek esetén

Lehetőség szerint a következő intézkedésekkel kell helyreállítani a személyes adatok rendelkezésre állását és elérhetőségét váratlan fizikai vagy technikai incidens esetén:

A működtetett biztonság-technikai rendszerekben kerülnek tárolásra a személyes adatok, a redundáns rendszerek pedig a biztonsági jelölés szerint kerülnek integrálásra. Szünetmentes áramellátással (pl. szünetmentes tápegységgel, akkumulátorokkal, generátorokkal) kerülnek biztosításra az adatközpontok áramellátása. Az adatbázisokat vagy adatközpontokat különböző fizikai helyszíneken tükörképszerűen kerülnek elhelyezésre.

Lehetőség szerint álljon rendelkezésre átfogó, írásbeli vészhelyzeti terv. A vészhelyzet esetén követendő eljárások és rendszerek kerüljenek lehetőség szerint rendszeres időközönként felülvizsgálatra.

d) Az adatkezelés biztonsága érdekében végzett ellenőrzése

Kockázatkezelésen alapuló ellenőrzési eljárások kerülnek alkalmazásra, figyelembe véve az illetékes Információ biztonsági Hivatal alapvető informatikai védelmi katalógusait, valamint az ISO/IEC 27001 szabvány előírásait, amelyek szerint az adatkezelés biztonsága érdekében a technikai és szervezési intézkedések hatékonyságát rendszeresen felül kell vizsgálni, fel kell mérni és értékelni kell. Ezzel biztosítható a lényeges információk, alkalmazások (köztük a minőség- és biztonságvizsgálati módszerek), az üzemi környezet (pl. a káros hatások kiszűrésére végzett hálózatmonitorozás) védelme és a védelmi koncepciók műszaki kivitelezése (pl. sebezhetőségi elemzésekkel). A gyenge pontok szisztematikus felderítésével és elhárításával folyamatosan ellenőrzi és fejleszti a védelmi intézkedéseket.

e) Személyügyi intézkedések

Írásbeli utasítások/szabályzatok kerülnek kiadásra és a személyes adatokhoz hozzáférő foglalkoztatottak rendszeres képzésben részesülnek annak érdekében, hogy a személyes adatok kezelése kizárólag a GDPR és a vonatkozó hatályos jogszabályok, többek között az azokban foglalt technikai és szervezési intézkedések szerint történjen.

7. Az Érintett jogai és azok érvényesítési lehetőségei

A vonatkozó jogszabályok alapján az alábbiak kérelmezhetők a Rendelőintézettől:

- Érintett tájékoztatása a személyes adatai kezeléséről;
- az Érintett személyes adatainak helyesbítése;
- az Érintett személyes adatainak, a kötelező adatkezelés kivételével, törlése;
- az adatok hordozásának igénylése (hozzájárulás-szerződés jogalap, automatizált adatkezelés esetén);
- tiltakozás a jogosulatlan adatkezelés, illetve adattovábbítás ellen (közfeladat ellátása érdekében történő adatkezelés esetén);
- az adatkezelés korlátozásának kezdeményezése;
- jogorvoslat kezdeményezése.

A személyes adatok kezelésével kapcsolatban jogsérelem esetén az alábbi jogorvoslati lehetőségeket biztosítja a Rendelőintézet az Érintett részére:

- Tájékoztatást kérhet személyes adatai kezeléséről, valamint kérheti személyes adatainak helyesbítését. Kérelmére a Rendelőintézet, tájékoztatást ad az általa kezelt adatairól, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevééről, címéről (székhelyéről) és az adatkezeléssel összefüggő tevékenységéről, továbbá arról, hogy kik és milyen célból kapják vagy kapták meg az adatokat. A tájékoztatás a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban, ha jogszabály ennél rövidebb határidőt nem állapít meg, legfeljebb egy hónapon belül (indokolt esetben további két hónap hosszabbítással) írásban, közérthető formában kerül átadásra.
- Az Érintett személyes adata törlésre kerül:
 - ha kezelése jogellenes,
 - ha az Érintett azt kéri (kivéve ha az adatkezelés jogszabály kötelező rendelkezésén alapul),
 - ha az adatkezelés célja megszűnt,
 - ha az hiányos vagy téves, és ez az állapot jogszerűen nem orvosolható, feltéve, hogy a törlést törvény nem zárja ki,
 - ha az adatok tárolásának törvényben meghatározott határideje lejárt,
 - ha azt a bíróság vagy azt a Nemzeti Adatvédelmi és Információszabadság Hatóság elrendelte.

A helyesbítésről és a törlésről a Táraság értesítést küld. Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti.

Tiltakozhat személyes adatának kezelése ellen, ha

- a személyes adatok kezelése vagy továbbítása kizárólag az adatkezelő közfeladata ellátásának teljesítéséhez vagy az adatkezelő, az adatátvevő vagy harmadik személy jogos érdekének érvényesítéséhez szükséges;
- a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik; valamint
- a tiltakozás jogának gyakorlását egyébként törvény lehetővé teszi.

Rendelőintézet, mint adatkezelő – az adatkezelés egyidejű felfüggesztésével – a tiltakozást a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb, ha jogszabály ennél rövidebb határidőt nem állapít meg, egy hónapon belül megvizsgálja, és annak eredményéről a kérelmezőt írásban tájékoztatja. Amennyiben a Rendelőintézet a tiltakozás megalapozottságát megállapítja, az adatkezelést – beleértve a további adatfelvételt és adattovábbítást is – megszünteti, és az adatokat zárolja, valamint a tiltakozásról, illetőleg az annak alapján tett intézkedésekről értesíti mindazokat, akik részére a tiltakozással érintett személyes adatot korábban esetleg továbbította, és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében.

Amennyiben a Rendelőintézet döntésével nem ért egyet, illetve ha a Rendelőintézet a GDPR-ban előírt határidőt elmulasztja, a döntés közlésétől, illetve a határidő utolsó napjától számított 30 (harminc) napon belül bírósághoz fordulhat.

8. Nemzeti Adatvédelmi és Információszabadság Hatóság (Felügyeleti hatóság)

Az Érintett személyes adatainak kezelésével kapcsolatban panaszt tehet az Adatvédelmi Felügyeleti Hatóságnál (Nemzeti Adatvédelmi és Információszabadság Hatóság, 1125 Budapest, Szilágyi Erzsébet fasor 22/c, postacím: 1530 Budapest, Pf.: 5. e-mail: ugyfelszolgalat@naih.hu).

9. Hatályba lépés, módosítás

A jelen tájékoztató 2018. november 5. napján lép hatályba azzal, hogy a Rendelőintézet jogosult a benne foglaltakat egyoldalúan módosítani.

