SZEGEDI KISTÉRSÉG TÖBBCÉLÚ TÁRSULÁSA
Egyesített Szociális Intézmény

A SZEMÉLYES ADATOKRA VONATKOZÓ ADATVÉDELMI ÉS INFORMÁCIÓBIZTONSÁGI NYILVÁNOS SZABÁLYZAT

Az EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE (továbbiakban: GDPR) előírásainak alkalmazása céljából

v2. 2023. április

Dokumentum változáskövetés

Dátum	Verzió	A változás oka	A módosítást elvégezte
2019. július-augusztus hó	V1	Az EU Parlament és Tanács 2016/679. számú Rendelete (GDPR) és a 2011. évi CXII. törvény	RITEK Zrt.
2023. április hó	V2	a 2011. évi CXII. törvény 5. § (5) bekezdése által előírt 3 évenkénti dokumentáció felülvizsgálat	RITEK Zrt.

Tartalomjegyzék

I. A Szabályzat célja és hatálya.

1. **A Szabályzat célja**, hogy eleget tegyen a **Szegedi Kistérség Többcélú Társulása Egyesített Szociális Intézmény** (továbbiakban: Adatkezelő) a személyes adatok kezelése során irányadó adatvédelmi, adatkezelési és adatbiztonsági előírásoknak, a tevékenysége során:

   a) a 2016 / 679 Európai Parlament és a Tanács rendelete (továbbiakban: GDPR) és
   b) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infó tv.)

   által tartalmazott, személyes adatok védelméhez fűződő jog érvényesülésének biztosítása érdekében.

2. Az Adatkezelő területi hatálya kiterjed a mindenkor hatályos és az Alapító Okiratban szereplő központra és részlegekre, telephelyekre.

1. **Az adatkezelések céljai:** közfeladati tevékenységek nyújtása, különösen tanyagondnoki szolgáltatásra jogosult, Tartós Bentlakást Nyújtó Idősek Otthona szolgáltatásait igénylő, a területi védőnői ellátásról szóló 49/2004. (V. 21.) ESZCSM rendelet 3. § szerinti szolgáltatásokra jogosult, a Fogyatékosok Nappali Intézménye szolgáltatásait igénylő, életvezetési nehézségei miatt veszélyeztetett családok, a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény 41-43. §, hatálya alá tartozó gyermek, a Családok Átmeneti Otthonával kapcsolatba kerülő személy és gyermeke, a gyermekjóléti szolgálattal kapcsolatba kerülő gyermek, a 66/2012. (IV. 2.) Korm. rendelet szerinti Fogyasztó, 10 és 18 év közötti függőségi problémákkal küzdő fiatal, közterületen élő és éjjeli menedékhelyeken alvó, az idősek nappali ellátásának szolgáltatásaira jogosult személyek részére ellátás nyújtása.

2. Adatvédelmi tisztviselő neve, elérhetősége: RITEK Zrt., székhelye: 6724 Szeged, Huszár utca 1., e-mail címe: dpo@ritek.hu, telefonszáma: +36 62 421-247.

3. A Szabályzat 2023. május 01. napján lép hatályba.

4. A Szabályzat alanyi hatálya vonatkozik

a) a foglalkoztatásában, megbízásában álló természetes személyre,
b) az adatfeldolgozókra, továbbá
c) az érintettre, aki különösen – de nem kizárólagosan – lehet
   - 18 év alatti fiatal, gyermek,
   - a szülői felügyeletet gyakorló szülő által megbízott személy,
   - ügyfél, látogató,

- jogi személy kapcsolattartója

5. A Szabályzat tartalma nyilvános.

II. Az adatkezelés elvei

1. A törvényesség elve alapján: a személyes adatok kezelését jogszerűen, tisztességesen és átlátható módon kell végezni. Az Infó tv. megfogalmazásában: Személyes adat kizárólag egyértelműen meghatározott, jogszerű célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok gyűjtésének és kezelésének tisztességesnek és törvényesnek kell lennie.

2. A célhoz kötöttség elve alapján:
   a) a foglalkoztatottak kizárólag a munkaköri leírásukban meghatározott feladataik ellátása céljából, a részükre biztosított jogosultságok rendeltetésszerű használatával kezelhetnek személyes adatot;
   b) a konkrét, vagy az érintett által adott hozzájárulásban megfogalmazott célhoz nem köthető adatkezelés tilos;
   c) amennyiben az adatkezelés célja teljesült vagy megszűnt, az adatkezelésre irányadó jogszabályban meghatározott tárolási határidőt követően az adatot elektronikusan törölni, a papíralapú adathordozót pedig selejtezni kell.

3. A pontosság és korlátozott tárolhatóság elve alapján:
   a) amennyiben a foglalkoztatott tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos, vagy időszerűtlen, köteles azt helyesbíteni, vagy az adat helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni, és erről mindazokat értesíteni, akiknek az adat továbbításra került;
   b) a tárolásnak olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adat kezelése céljának eléréséhez szükséges ideig teszi lehetővé.

4. Az integritás és bizalmi jelleg elve alapján az adat kezelése során biztosítani kell, hogy:
   a) a személyes adat illetéktelen harmadik személy tudomására ne jusson (bizalmasság),
   b) az adat illetéktelen harmadik személy által ne legyen módosítható (sértetlenség),
   c) az adat elérhető legyen a feljogosított személyek, szervezetek számára (rendelkezésre állás).

5. Az adattakarékosság elve alapján: az Adatkezelő kizárólag annyi és olyan személyes adatot kezelhet, amely az érintett egyértelmű azonosításához és ügyének elintézéséhez minimálisan szüksége és arra alkalmas.

6. Az Infó tv. az adatvédelem fontosságával egészíti az alapelveket. *„Az adatkezelés során arra alkalmas műszaki vagy szervezési – így különösen az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisülésével vagy károsodásával szembeni védelmet kialakító – intézkedések alkalmazásával biztosítani kell a személyes adatok megfelelő biztonságát.”*

III. Az adatkezelés jogalapjai

A GDPR előírásai alapján a személyes adatok kezelésére lehetőség van a következő esetekben, ha az egyik tényállás teljesül:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;

b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;

c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;

d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Az Infó tv. a feltételek egy részét pontosítja:

Személyes adat akkor kezelhető, ha

a) azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben, különleges adatnak vagy bűnügyi személyes adatnak nem minősülő adat esetén – helyi önkormányzat rendelete közérdeken alapuló célból elrendeli,

b) az a) pontban meghatározottak hiányában az az adatkezelő törvényben meghatározott feladatainak ellátásához feltétlenül szükséges és az érintett a személyes adatok kezeléséhez kifejezetten hozzájárult,

c) az a) pontban meghatározottak hiányában az az érintett vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges és azzal arányos, vagy

d) az a) pontban meghatározottak hiányában a személyes adatot az érintett kifejezetten nyilvánosságra hozta és az az adatkezelés céljának megvalósulásához szükséges és azzal arányos.

IV. Az Adatkezelő nyilvántartásában levő, működésével kapcsolatos különleges adatok és azok továbbítása

1. TAJ száma, személyi igazolvány száma, Win-TSzG program törzsszám, étel allergia vagy diétás étkezési okok és az azt igazoló szakorvosi vélemény, szolgáltatás Igénybevétel kezdete/vége, jövedelmi adatok, Komplex minősítést végző I. fokú szakértői bizottság összefoglaló véleménye a megváltozott munkaképesség minősítéséről, illetve a megváltozott munkaképességű személyek ellátásainak megállapításához Bankszámla száma, Nyugdíj törzsszám, Fizetendő havi térítési díj,

2. a szülői felügyelet gyakorlására jogosult személy / törvényes képviselő adatai: neve, címe,

3. Oktatási intézményének megnevezése, Évfolyam, Háziorvos neve/elérhetősége, Közgyógyellátásban részesül-e, Gyógyszerei, a betegségek nemzetközi osztályozása szerinti kódja (BNO kód), egészségügyi adatok, Soron kívüli ellátásra vonatkozó igény, Állampolgársága, esetleges Gondnok neve, veszélyeztetettség típusa,

4. beilleszkedési nehézség, magatartási problémák, neveltetési körülmények, familiáris légkör, ellátás megkezdésének időpontja, ellátás megszüntetésének időpontja, ellátás megszüntetésének módja, ellátás megszüntetésének oka, a jogosultsági feltételek, munkaügyi státusz, Kezelési Igény Indikátor kitöltési adatok, adott esetben a büntetőügy száma, folyamatban lévő büntetőeljárás, korábbi büntetés(ek),

5. az Adatkezelő munkavállalói, közalkalmazottai, közfoglalkoztatottai esetében, születési idő, születési ország, állampolgárság, édesanyja neve, személyi ig. szám, adott esetben gépjármű törzskönyv másolat és gépjármű forgalmi engedély másolat, bankszámlaszám, a társadalombiztosítási azonosító jel, adóazonosító szám, családi adókedvezményhez szükséges adatok, magán-nyugdíjpénztár neve, állandó lakcím, tartózkodási hely, e-mail cím, telefonszám, közeli hozzátartozó adatai

6. A GDPR 4. cikk 10. pont szerinti harmadik fél részére történő adat átadás lehetséges:

Központi, regionális szervezet neve:	Elérhetőségek	Szervezet feladatai
Magyar Államkincstár Csongrád-Csanád Vármegyei Igazgatóság	6720 Szeged, Széchenyi tér 9., Telefon: +3662568168, honlap: http://tcs.allamkincstar.gov.hu/,	A KENYSZI, OSZIR (Országos Szociális Információs Rendszer), Szolgáltatói Nyilvántartási Rendszer (MŰKENG), Pénzbeli és Természetbeni Ellátások Rendszer (PTR) program biztosítása, szolgáltatások költségvetési feladatainak ellátása, bérszámfejtés, nyugellátási szolgáltatások költségvetési feladatainak ellátása
Csongrád-Csanád Vármegyei Kormányhivatal járási hivatalai	6722 Szeged, Rákóczi tér 1., Telefon: (62) 680-663, web: http://www.csmkh.hu/hu/szegedi-jarasi-hivatal	a feladat- és hatáskörébe tartozó szociális ellátásokra való jogosultság fennállásának elbírálása, az ellátás biztosítása, fenntartása és megszüntetése céljából nyilvántartást vezet (Szt. 18/A. §)
SZÁMADÓ Szoftver Kft.	1091 Budapest Üllői út 119., Telefon: +36 1 215-0256, E-mail: mail@szamado.hu	Win-Tszg (Területi Szociális Gondoskodó) programrendszer számviteli szolgáltatás nyújtása
GEKKOSOFT Kft.	8230 Balatonfüred, Csárda utca 15. 1. em. 2., e-mail: winidoki@winidoki.com, telefon: +36-70-621-7214,	WiniDoki-szoc.Extra rendszer üzemeltetése
Nemzeti Egészségbiztosítási Alapkezelő	1139 Budapest, Váci út 73/A, Web: http://www.oep.hu/	az egészségügyi szolgáltatások finanszírozására, gyógyszer, gyógyászati segédeszköz kiszolgáltatására, gyógyászati ellátás nyújtására és az ehhez kapcsolódó ártámogatás elszámolása, folyósítása
Állami Egészségügyi Ellátó Központ	1125 Budapest, Diós árok 3., Tel.: (+361) 356-1522, web: www.aeek.hu, mail: aeek@aeek.hu	A 27/2015. (II. 25.) Korm. rendelet 6. § (4)-(6) bekezdésein alapján az Elektronikus Egészségügyi Szolgáltatás Tér IT rendszer működtetője, melyhez 2017. november 1-jén a háziorvosi szolgálatok, járó- és fekvőbeteg-ellátó intézmények, és az összes gyógyszertár csatlakozott.
illetékes Kormányhivatal Jogi és Hatósági Főosztály Szociális, Igazságügyi és Gyámügyi Osztály, továbbá Népegészségügyi és Élelmiszerlánc-biztonsági Főosztály Népegészségügyi és Járványügyi Osztály	6722 Szeged, Rákóczi tér 1., Web: http://www.csmkh.hu/hu/ii-tevekenysegre-mukodesre-vonatkozo-adatok/kat/szocialis-igazsagugyi-es-gyamugyi-osztaly	másodfokú hatósági jogkört gyakorol gyermekvédelmi és közegészségügyi hatósági ügyekben, másodfokon eljár a települési önkormányzatok jegyzőinek, a járási gyámhivataloknak a gyermekvédelmi és gyámügyi hatósági ügyeiben, valamint meghatározott esetekben az ideiglenes hatályú elhelyezés tekintetében, illetve a gyermekvédelmi jelzőrendszer elégtelen működése esetén megteszi a szükséges intézkedéseket.

illetékes Járási Hivatal Hatósági Főosztály Gyámügyi és Igazságügyi Osztály, továbbá Népegészségügyi Osztály	6722 Szeged, Rákóczi tér 1., Szeged, Derkovits fasor 7-11., Email: kozeg.nefo@csongrad.gov.hu Telefon: 62/680-098, 06-70/338-21-08, Telefon: 62/681-716, Web: http://www.csmkh.hu/hu/szegedi-jarasi-hivatal/szegedi-jarasi-hivatal-hatosagi-foosztaly-1	hatósági jogkört gyakorol gyermekvédelmi hatósági ügyekben, első fokon engedélyezi, illetve ellenőrzi a gyermekjóléti és gyermekvédelmi szolgáltató tevékenységet végző szolgáltatók, intézmények, hálózatok működését.
Család- és Gyermekjóléti Központ	6723 Szeged, Sás u. 2., Telefon: 06-62-464-364, E-mail: szeged@csgyjk.ritek.hu	a gyermekvédelmi jelzőrendszer működtetésének a biztosítása
KSH	https://elektra.ksh.hu/asp/bejelentkezes.html	TEGYESZ Nyilvántartó Programban vezetett adatok, gyámhivatali határozatok feldolgozása
Szociális és Gyermekvédelmi Főigazgatóság	1132 Budapest, Visegrádi u. 49., Honlap: http://szocialisportal.hu, telefonszám: +36-1-769-1704, e-mail: info@szgyf.gov.hu	ellátja a szociális igazgatásról és szociális ellátásokról szóló 1993. évi. III. törvény és a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény szerinti fenntartói feladatokat
társintézmények, egészségügyi és szociális intézmények	illetékesség szerint	a gyermekvédelmi jelzőrendszer és egészségügyi ellátás működtetésének a biztosítása

7. Címzett III., Az Adatkezelő által igénybe vett Adatfeldolgozók:

Adatfeldolgozó Szervezet, vállalkozás neve	Elérhetőségei	Feladatai
RITEK Zrt.	székhelye: 6724 Szeged, Huszár utca 1., e-mail címe: dpo@ritek.hu, telefonszáma: +36 62 421-247	elektronikus levélszolgáltatás, tárhely biztosítás, informatikai rendszergazda

V. Az érintett adatkezeléssel kapcsolatos jogai

1. A GDPR alapján a következőek:

a) Tájékoztatás kéréshez, betekintéshez (hozzáféréshez) való jog. Az érintett az Adatkezelőtől kérheti, az adjon tájékoztatást, hogy róla milyen személyes adatot kezelnek, annak forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adattovábbítás jogalapjáról és címzettjéről.

b) A helyesbítéshez való jog. Az érintett helyesbítéshez való joga minden adatkezelési jogalap vonatkozásában megilleti. Az Adatkezelő a kérelmem esetén indokolatlan késedelem nélkül helyesbíti az érintettre vonatkozó pontatlanul kezelt személyes adatokat.

c) Adattörléshez (elfeledtetéshez) való jog. Az érintett kérheti, hogy az Adatkezelő törölje a személyes adatait. A törlési kérelmet az Adatkezelő különösen abban az esetben utasítja el, ha a jogszabály őt a személyes adatok tárolására és / vagy zárolásra kötelezi, pl. hatósági vagy bírósági eljárás során.

d) Zároláshoz való jog. Az érintett kérheti, hogy a személyes adatait az Adatkezelő zárolja, ami a tárolt személyes adatok megjelölését jelenti a jövőbeli kezelésük korlátozása céljából. A zárolás addig tart, amíg az érintett által megjelölt indok szükségessé teszi az adatok tárolását.

e) A tiltakozáshoz való jog. Az érintett írásban tiltakozhat az adatkezelés ellen. Így például, ha az Adatkezelő személyes adatot közvetlen üzletszerzés, ennek érdekében például a személyes adatára vonatkozó matematikai és statisztikai elemző eljárásokat alkalmazna, vagy közvélemény-kutatás vagy tudományos kutatás céljából továbbítaná, felhasználná.

f) Adathordozhatósághoz való jog. Az érintett jogosult kérni az Adatkezelőtől a személyes adatainak adatkezelők közötti, másik adatkezelőnek történő közvetlen továbbítását, ha ez technikailag megvalósítható és nem ütközik uniós vagy nemzeti jogszabály előírásába.

g) Önkéntes hozzájárulás esetén a visszavonáshoz való jog. Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét.

h) Az ügyfél hivatalos jogérvényesítése.

i) Az érintteti jogok gyakorlásának módja: az Érintett az Adatkezelőhöz és / vagy az adatvédelmi tisztviselőjéhez fordulhat (személyesen, telefonon, vagy e-mailen) adatvédelmi jogi kérdéseivel, valamint a gyakorolni kívánt jogai érvényesítésével kapcsolatosan.

j) Az adatbiztonsági követelmények teljesülése és az érintett jogainak védelme érdekében az Adatkezelő köteles meggyőződni az érintett és a hozzáférési jogával élni kívánó személy személyazonosságának egyezéséről, ennek érdekében a tájékoztatás, az adatokba történő betekintés, illetve azokról másolat kiadása is az érintett személyének azonosításához kötött.

k) Az Érintett által beküldött jogosulti igény, kérés esetén, az Adatkezelő köteles a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban egy hónapon belül, közérthető formában, az érintett erre irányuló kérelmére írásban megadni a válaszát.

2. Az Infó tv. előírásai szerinti érintetti jogok:

a) az adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően tájékoztatást kapjon (a továbbiakban: előzetes tájékozódáshoz való jog),

b) kérelmére személyes adatait és az azok kezelésével összefüggő információkat az adatkezelő a rendelkezésére bocsássa (a továbbiakban: hozzáféréshez való jog),

c) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatait az adatkezelő helyesbítse, illetve kiegészítse (a továbbiakban: helyesbítéshez való jog),

d) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatai kezelését az adatkezelő korlátozza (a továbbiakban: az adatkezelés korlátozásához való jog),

e) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatait az adatkezelő törölje (a továbbiakban: törléshez való jog).

3. Az érintett jogai érvényesülésének biztosítása az Infó tv. szerint:

a) az érintett részére az e törvényben meghatározott esetekben nyújtandó bármely értesítést és tájékoztatást könnyen hozzáférhető és olvasható formában, lényegre törő, világos és közérthetően megfogalmazott tartalommal teljesíti, és

b) az érintett által benyújtott, az őt megillető jogosultságok érvényesítésére irányuló kérelmet annak benyújtásától számított legrövidebb idő alatt, de

legfeljebb huszonöt napon belül elbírálja és döntéséről az érintettet írásban vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti.

4. Az adatkezelő a meghatározott jogok érvényesülésével kapcsolatban a meghatározott feladatait fő szabály szerint ingyenesen látja el.

VI. Információbiztonság az adatkezelésben

1. Az Adatkezelő információbiztonsági státusza: az Adatkezelő nem tartozik az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá, a védelmi intézkedésekről szóló döntést az Adatkezelő önállóan határozza meg.

2. Az Infó tv. előírásainak megfelelően az Adatkezelő műszaki és szervezési biztonsági intézkedésekkel köteles védeni a személyes adatok biztonságát, az Adatkezelő az érintettek alapvető jogainak érvényesülését az adatkezelés által fenyegető kockázatokhoz igazodó műszaki és szervezési intézkedéseket tesz, ideértve indokolt esetben az álnevesítés alkalmazását.

3. A meghatározott intézkedések kialakítása és végrehajtása során az adatkezelő és az adatfeldolgozó figyelembe veszi az adatkezelés összes körülményét, így különösen a tudomány és a technológia mindenkori állását, az intézkedések megvalósításának költségeit, az adatkezelés jellegét, hatókörét és céljait, továbbá az érintettek jogainak érvényesülésére az adatkezelés által jelentett változó valószínűségű és súlyosságú kockázatokat.

4. Az Adatkezelő a papír alapú iratok kezelése és az elektronikus adatok használata során az információbiztonsági előírásai alapján, megfelelően gondoskodik arról, hogy ne forduljon elő adatvédelmi incidens.

5. Az Adatkezelő az adatokat megfelelő intézkedésekkel védi
   a) a jogosulatlan hozzáférés,
   b) megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a
   c) véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó
   d) hozzáférhetetlenné válás ellen.

6. Az Adatkezelő az adatbiztonság feltételeinek érvényesítése érdekében gondoskodik az érintett munkatársak megfelelő felkészítéséről.

7. Az Adatkezelő az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel van a technika mindenkori fejlettségére. Az Adatkezelő több lehetséges adatkezelési megoldás közül azt választja, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene.

8. Az elektronikusan tárolt adatok esetében adatot csak a nyilvántartott hozzáférési jogosultsággal rendelkező adatkezelő kezelhet.

9. Az adatkezelőnek egyéni, titkos jelszóval kell bejelentkeznie a rendszerbe.

10. A rendszerben történt, jelszóval védett adatkezelésért az adatkezelő felel. Az esetleges visszaélések elkerülése érdekében az adatkezelő kötelezettsége, hogy egyéni jelszavak titkosságát biztosítsa.

11. Az adatkezelés befejeztével az adatkezelőnek a rendszerből ki kell lépnie.

12. Az Adatkezelő az adatokat megfelelő intézkedésekkel védi 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.

13. A rendszergazda jogosult az adatokról biztonsági és archiválási másolatok létrehozására, tárolására.

14. A védelmi intézkedések fő területei
    a) A jogosulatlan hozzáférés elleni védelem, ezen belül a szoftverek és a hardver eszközök védelme, a jogtalan hozzáférést, hálózati incidens megakadályozó fizikai védelmi intézkedések megvalósíthatóak.
    b) Az adatállomány helyreállítását biztosító intézkedések, ezen belül a rendszeres biztonsági mentések készítése, továbbá a másolatok elkülönített és biztonságos tárolása megtörténik.

15. Az elektronikus információs rendszer vírusvédelme biztosított.

16. Az egyes adatokat csak a nyilvántartottan és ehhez hozzáférési és egyéb jogosultsággal rendelkező személy kezelheti.

17. Az adatokhoz hozzáférő felhasználók elkülönített belépési névvel és egyéni, titkos jelszó használatával kezelhetik az elektronikus információs rendszeren levő személyes adatokat.

18. A Felhasználó kötelezettségei
    a) A számítástechnikai infrastruktúrát valamennyi Felhasználónak rendeltetésszerűen kell használnia.
    b) A Felhasználó köteles együttműködni a rendszergazdával.
    c) Az Adatkezelő előírja, hogy a Felhasználók megfelelő szintű jelszó titkosítást alkalmazzanak, továbbá a jelszavakat rendszeres és rövid időközönként cseréljék. A jelszó nem tartalmazhatja a Felhasználó családi nevét, felhasználónevét, sem egyéb Felhasználóhoz kapcsolódó információt.
    d) A Felhasználónak jeleznie kell a rendellenes működést és az egyéb általa veszélyesnek ítélt helyzeteket.
    e) A Felhasználó felelős, hogy az adatfájlokat, dokumentumokat és adatbázisokat az adathordozó sérülésének veszélye miatt, a szükséges feladatok elvégzése után, kötelezően és haladéktalanul szerverre mentse.
    f) A Felhasználó a rendelkezésére bocsátott, hordozható informatikai, irodatechnikai, multimédiás eszközt vagy adathordozót köteles megőrizni, az

illetéktelen hozzáféréstől személyes felügyelettel vagy az eszköz, adathordozó elzárásával megvédeni.

g) A Felhasználónak gondoskodni kell, hogy tulajdonában lévő mobil eszközök („okos telefonok", tabletek, laptopok) az elvárt funkcionalitással rendelkezzenek.

h) Abban az esetben, ha az „okos telefonon” az Adatkezelő tulajdonát képező adatok és dokumentumok tárolása történik, az eszközt olyan jelszóvédelemmel kell ellátni, amely egy meghatározott idő elteltével lezárja az eszközt.

i) A felhasználók kötelesek a munka megszakításakor vagy befejezésekor az elektronikus információs rendszerből kilépni, valamint biztosítaniuk kell a képernyőtakarást. A hálózatba beléptetett munkaállomást tilos kilépés, illetve lezárás nélkül elhagyni.

j) A Felhasználó felel a jogszabálykövető és biztonságos Internet használatért.

k) A Felhasználónak tilos más felhasználók erőforrásait illetéktelenül használni.

l) A Felhasználónak a laptopok, „okos telefonok" és más hordozható mobil eszközök esetében különös gonddal kell eljárnia az eszköz és az azon található adatok és dokumentumok védelme érdekében, ezek nyilvános helyen semmilyen körülmények között nem hagyhatók őrizetlenül, használatuk átruházása tilos.

m) Tilos a nem engedélyezett szoftverek, filmek, zenék és más szerzői jogvédelem alá eső anyagok letöltése, másolása.

n) Tilos a hálózati erőforrásokat védő technikai korlátozások feltörése, más Felhasználók jelszavaknak megszerzése.

o) Tilos a rendszer, és más Felhasználók adatait, fájljait — engedély nélkül - másolni, törölni vagy módosítani.

p) A munkaállomás illetéktelen hozzáférés elleni védettségéért, a munkaállomáson végzett minden tranzakcióért a bejelentkezéstől a kijelentkezésig a bejelentkezett Felhasználó a felelős. Ez a felelősség akkor is fennáll, ha a tranzakciókat jogosulatlan harmadik személy hajtotta végre, amennyiben erre jelen Szabályzat előírásainak Felhasználó általi be nem tartása miatt kerülhetett sor.

q) Amennyiben a munkaállomást több személy is használhatja, a Felhasználó a munkaállomást csak akkor hagyhatja el, ha minden futó programból, azonosított kapcsolatból és az operációs rendszerből is kijelentkezett.

r) A Felhasználó dokumentum nyomtatásakor köteles biztosítani, hogy az általa kinyomtatott irathoz illetéktelen személy ne férjen hozzá. Közös használatú hálózati nyomtató esetében a kinyomtatott iratot köteles a nyomtatóból eltávolítani, sikertelen nyomtatás esetén köteles meggyőződni — amennyiben szükséges, informatikus munkatárs segítségével — arról, hogy a nyomtató memóriájában nem maradt nyomtatandó dokumentum.

19. Valamennyi Felhasználónak tilos:

a) az általa használt eszközök biztonsági beállításait megváltoztatni,

b) a számítógép rendszerszintű beállításait módosítani (ide nem értve az irodai programok felhasználói beállításait),

c) a munkaállomására telepített aktív vírusvédelmet kikapcsolni,
d) belépési jelszavát (jelszavait), hardveres azonosító eszközét más személy rendelkezésére bocsátani, hozzáférhetővé tenni,
e) a számítógép-hálózatot fizikailag megbontani, számítástechnikai eszközöket lecsatlakoztatni, illetve bármilyen számítástechnikai eszközt rácsatlakoztatni a hálózatra a rendszergazda jóváhagyása nélkül,
f) a számítástechnikai eszközökből összeállított konfigurációkat megbontani, átalakítani,
g) bármilyen szoftvert installálni, Internetről letölteni, külső adathordozóról merevlemezre másolni a rendszergazda engedélye, illetve közreműködése nélkül, a munkaállomásokon nem az Adatkezelő által rendszeresített, vagy engedélyezett szoftvereket (szórakoztató szoftverek, játékok, egyéb segédprogramok) installálni és futtatni,
h) online játékokat használni,
i) bármilyen eszközt számítástechnikai eszközökbe szerelni és használni,
j) az általa használt adathordozó (pl. CD, DVD, Pendrive stb.) eszköz számítógépben hagyni a munkaállomásáról való távozás esetén,
k) ellenőrizetlen forrásból származó adatokat tartalmazó adathordozót az eszközökbe helyezni.
l) külső adathordozó esetében az adathordozót teljes vírusellenőrzést kell lefuttatni és csak a jóváhagyását követően lehet az adathordozót használni az eszközben,
m) más szerzői, iparjogvédelmi, egyéb szellemi tulajdonhoz fűződő, vagy egyéb személyhez fűződő jogát vagy jogos érdekét sértő dokumentumokat, tartalmakat (zenéket, filmeket stb.) az eszközökön tárolni, oda le-, illetve onnan a hálózatra feltölteni,
n) láncleveleket továbbítani, levélszemetet, továbbá azok mellékleteit, vagy linkjeit megnyitni, rendszer biztonságáért felelős személy külön engedélye nélkül — feliratkozni, kivéve a munkavégzéshez szükséges: az Adatkezelő által megrendelt, működtetett, vagy előfizetett szolgáltatásokat, belső információs rendszereket, adatfeldolgozó szervek/szervezetek által biztosított szolgáltatásokat, és a szolgáltatások levelező listáit.

20. A Felhasználó felelős az általa használt számítástechnikai infrastruktúráért, azok biztonságáért és az azokon tárolt adatokért, dokumentumokért.

21. Az Adatkezelő folyamatosan nyilvántartja és frissíti a hardver eszközök, valamint szerver rendszer használatához szükséges egyéni, felhasználói jogosultságok rendszerét.

22. A munkavállalók, és egyéb, az Adatkezelő érdekében eljáró személyek az általuk használt, vagy birtokukban lévő, személyes adatokat is tartalmazó adathordozókat, függetlenül az adatok rögzítésének módjától, kötelesek biztonságosan őrizni, és védeni a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

23. A papír alapú dokumentumokban szereplő személyes adatokat kizárólag az arra jogosult vezetők, döntéshozók és ügyintézők ismerik meg.

24. A személyes adatokhoz más nem férhet hozzá, a dokumentumokat az Adatkezelő zárható, száraz helyiségekben, külön elzárt szekrényekben, fiókokban tárolja.

25. Az iratokat kezelő ügyintéző az adatkezelésre szolgáló irodát akkor hagyja el, ha az iratokat vagy irodát bezárja.

VII. A szervezeti és adatvédelmi kockázattal kapcsolatos fogalmak, feladatok.

1. A kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;

2. A kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.

3. A kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása.

4. **A GDPR Praeambulum (77) bekezdése alapján, a kockázatok felmérését el kell végezni a személyes adatok kezelése során:**

   „ ... megfelelő intézkedéseknek az adatkezelő vagy adatfeldolgozó általi végrehajtásához, valamint a megfelelés általuk való bizonyításához - különösen ami az adatkezeléssel kapcsolatos kockázat beazonosítását, valamint a kockázat forrásának, jellegének, valószínűségének és súlyosságának a felmérését illeti -, továbbá a kockázat mérséklésével kapcsolatos bevált gyakorlatoknak” az ismerete szükséges

5. **A GDPR Praeambulum (78) bekezdése** kötelezettségi kapcsolatban van a fizikai, adminisztratív és logikai védelmi intézkedések megszervezésével és végrehajtásával:

   „A természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli az e rendelet követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát.”

6. A GDPR Praeambulum (83) bekezdése olyan előírásokat tartalmaz, amely átfedést jelent a **Bizalmasság-Sértetlenség-Rendelkezésre állás** követelményeivel és az adatvédelmi incidens megelőzési kötelezettségével:

   (83) A biztonság fenntartása és az e rendeletet sértő adatkezelés megelőzése érdekében az adatkezelő vagy az adatfeldolgozó értékeli az adatkezelés természetéből fakadó kockázatokat, és az e kockázatok csökkentését szolgáló intézkedéseket, például titkosítást alkalmaz. Ezek az intézkedések biztosítják a megfelelő szintű biztonságot - ideértve a bizalmas kezelést is -, figyelembe véve a tudomány és technológia állását, valamint a végrehajtás kockázatokkal és a védelmet igénylő személyes adatok jellegével összefüggő költségeit. Az adatbiztonsági kockázat felmérése során a személyes adatok kezelése jelentette olyan kockázatokat - mint például a továbbított, tárolt vagy más módon kezelt személyes adatok

véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés - mérlegelni kell, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek.

7. **A GDPR 32. cikk Az adatkezelés biztonsága** című tényállásában, az előbb ismertetett kötelezettségeket a következő előírásokkal erősíti meg:

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) a személyes adatok álnevesítését és titkosítását;
b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
c) 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;
d. az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

(2) 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 hozzáférésből erednek.

VIII. Eljárási kötelezettségek, lehetőségek az adatvédelmi incidens megelőzésekor, esetleges bekövetkezése esetén.

1. Az Adatkezelő tevékenysége során **köteles felvenni a kapcsolatot az Adatvédelmi tisztviselővel**, annak szakmai tájékoztatását kikérni.

2. Az Adatkezelő minden munkavállalója, megbízottja a Szabályzat megismerésével köteles eleget tenni, hogy a személyes adatok kezelése során az adatkezelőket **terheli a bizonyítási kötelezettség.**

3. Az Adatkezelőnek biztosítania kell a GDPR-ban foglalt 5. cikk (2) bekezdése alapján a következőt: „Az adatkezelő felelős az (1) bekezdésnek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („elszámoltathatóság”), ezért a szükséges kommunikáció minden lehetséges formáját **dokumentálhatóan rögzíteni kell**, hogy az Adatkezelő igazolni tudja az elvárható és kifejtett tevékenységének valódiságát.

4. Az Adatkezelő minden vezetője, munkavállalója köteles a vonatkozó jogi normák betartására, különösen a GDPR 33. cikkében foglaltakra:

   „(1) Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.
   (2) Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.
   (3) Az (1) bekezdésben említett bejelentésben legalább:
   ismertetni kell az adatvédelmi incidens jellegét, beleértve - ha lehetséges - az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
   közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
   ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
   ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

(4) Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.
(5) Az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést."

5. Az Adatkezelő bármely munkavállalója, megbízottja az Adatkezelő működésével összefüggő **adatvédelmi incidens lehetősége, veszélye, bekövetkezte** esetén ennek az ismeretéről haladéktalanul tájékoztatni köteles - lehetőleg írásban is - a vezetőjét.

6. Ezen túlmenően az említett személyek kötelesek az incidensnek nem minősülő, üzemzavart, részleges működőképességet vagy más szokatlan információbiztonsági eseményt jelezni a vezetőjük felé.

7. Az Adatkezelő Főigazgatója az Adatkezelő munkamegosztása alapján köteles gondoskodni a munkavállalók és megbízottak **incidenskezelési oktatásáról.**

8. **Az Főigazgató irányításával az Adatkezelő feladata, hogy az Adatvédelmi tisztviselő álláspontjának ismeretében:**
   a. az incidens-gyanús tényállás további kivizsgálása, az incidens elhatárolása az ideiglenes üzemzavartól,
   b. az incidens azonosítása,
   c. a veszélyeztetett személyes adatok körének vizsgálata,
   d. a tényállás kockázatának folyamatos mérése,
   e. a védelmi intézkedések meghatározása, végrehajtatása,
   f. a Nemzeti Adatvédelmi és Információszabadság Hatóság részére az incidens bejelentése (felügyeleti hatóság, NAIH) (postai cím: 1530 Budapest, Pf.: 5.; cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.; telefon:+36 (1) 391-1400; fax: +36 (1) 391-1410; e-mail: ugyfelszolgalat@naih.hu), az elektronikus bejelentés címe: **https://www.naih.hu/adatvedelmi-incidensbejelent--rendszer.html**,
   g. folyamatos kapcsolattartás a NAIH-al,
   h. szükség esetén az érintettek tájékoztatási kötelezettségének a megállapítása,
   i. adott esetben az érintettek értesítése, az érintettekkel való folyamatos kapcsolat biztosítása,

9. **Az Adatkezelőnek meg kell szerveznie, hogy**
   a. a biztonságot érintő összes eseményről tájékoztassák a felelős személyt vagy személyeket, akinek vagy akiknek a feladata az incidensek kezelése, az adatvédelmi incidens bekövetkeztének megállapítása és a kockázat felmérése,

b. tájékoztassák az Adatkezelő szervezet érintett részlegeit, telephelyeit az incidens beállásáról,
c. az incidens alakulásáról folyamatosan nyilvántartást vezessenek.

10. Az Adatkezelő köteles az **incidensről tájékoztatást nyújtani, riasztást kiadni az érintett:**
    a. közös adatkezelők tagjai, képviselői,
    b. adatfeldolgozók képviselői,
    részére

11. A NAIH részére szóló incidens bejelentésben legalább:
    a. ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
    b. közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
    c. ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
    d. ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

12. Ha az adatvédelmi incidens természetéből ez következik és nem lehetséges az incidenssel kapcsolatos információkat **egyidejűleg közölni a Hatóság felé**, akkor az Adatkezelőnek a GDPR 33. cikk (4) bekezdését kell alkalmazni, miszerint azok további indokolatlan késedelem nélkül később **részletekben is közölhetők a** Hatósággal.

13. Az Adatkezelő minden munkavállalója, megbízottja köteles együttműködni a NAIH-al.

14. Ha az Adatkezelő nem tesz bejelentést, azonban kiderül, hogy kellett volna, akkor a Hatóság bírságot szabhat ki a bejelentési kötelezettség elmulasztásáért.

15. Ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, akkor nem szükséges a NAIH-nak bejelentést tenni.

16. Az Iránymutatás szerint akkor tekinthető úgy, hogy az incidens az adatkezelő – **Adatkezelő - „tudomására" jutott**, amikor az adatkezelő észszerű bizonyossággal meggyőződött arról, hogy olyan biztonsági incidens történt, amelynek következtében a személyes adatok veszélybe kerültek.

17. A GDPR 34. cikk (1) bekezdése alapján az Adatkezelő köteles indokolatlan **késedelem nélkül tájékoztatni az érintetteteket** az adatvédelmi incidensről, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. *(„Ha az adatvédelmi incidens*

valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.")

18. **A GDPR (75)-(76) preambulum** bekezdései meghatározzák, hogy mi tekinthető kockázatnak a természetes személyek jogaira és szabadságaira nézve (például személyazonosság-lopás, személyazonossággal való visszaélés, diszkrimináció, pénzügyi veszteség, jóhírnév sérelme, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, gazdasági vagy szociális hátrány).

19. Az adatvédelmi incidensről szóló értesítés formájára és az arra alkalmazandó eljárásra vonatkozóan az Adatkezelőnek ésszerű és reális döntést kell hoznia.

20. Az érintetteket elvben közvetlenül kell tájékoztatni az adott incidensről, kivéve, ha ez aránytalan erőfeszítéssel járna. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

21. **Az érintettek időbeli tájékoztatása** a GDPR 86. Preambulumbekezdése szerint kell, hogy történjen, miszerint: „Az érintettet az adatkezelő indokolatlan késedelem nélkül tájékoztatja, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, annak érdekében, hogy megtehesse a szükséges óvintézkedéseket."

22. Az **érintettetek tájékoztatása kiterjed:**
    a. az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevére és elérhetőségére,
    b. az adatvédelmi incidensből eredő, valószínűsíthető következményekre,
    c. az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedésekre, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedésekre is.

23. Mérlegelni kell az incidens körülményei alapján, hogy a tájékoztatás az érintetteknek megküldhető például e-mail-en, sms-ben, weboldalon található hirdetéssel, postán vagy a nyomtatott sajtó útján. A körülményektől függően, javasolt lehet több csatornát is igénybe venni.

24. **Nem kell tájékoztatni az érintetteket, ha** a GDPR 34. cikk (3) bekezdése szerint, ha a következő feltételek bármelyike teljesül:
    a. az adatkezelő 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 adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az (1) bekezdésben említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
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.

25. Gondoskodni kell az incidens elhárításáról, majd **a megfelelő adatkezelés helyreállításáról.**

26. Az Adatkezelő **köteles a kockázatok és hatásuk felmérésére,** ennek során legalább a következő tényezők figyelembe vétele szükséges, mint például:
    a. az incidens típusa (bizalmassági, integritási vagy elérhetőségi);
    b. a személyes adatok jellege, érzékenysége és száma;
    c. mennyire könnyen azonosítható az adatvédelmi incidenssel érintett természetes személy;
    d. a természetes személyre nézve fennálló következmények valószínűsége és súlyossága;
    e. az Adatkezelő működésére, szolgáltatás ellátására milyen hatást gyakorol,
    f. az ügyfél kiszolgálást mennyiben korlátozza,
    g. kiszolgáltatott személyeket érint-e az incidens (például gyermekeket);
    h. pénzügyi kárral jár-e az incidens,
    i. az érintett személyek száma;
    j. más függőségi hatást okoz-e, az Adatkezelő más szolgáltatási ágait befolyásolja-e,
    k. jelentős többlet erőforrást, informatikai többlet szükségletet igényel-e.

27. **Az Adatkezelő Főigazgatója jogosult elsősorban:**
    a. az adatvédelmi incidens tényének megállapítására,
    b. az adatvédelmi incidens elhárításának a kihirdetésére, az incidens lezárására,
    c. az elektronikus és írott média, a közösségi hálózatok hivatalos tájékoztatására.

28. Az Adatkezelő kijelölt munkatársai kötelesek arra, hogy biztosítsák az **Adatkezelő incidens Nyilvántartásának a hiteles vezetését.**

29. A Nyilvántartásban az Adatkezelő erre kijelölt munkatársai nyilvántartják az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

30. A nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze a GDPR követelményeinek való megfelelést, az adatvédelmi incidens kezelését és megoldását, az ismételt előfordulás megakadályozására tett intézkedéseket.

IX. Fontosabb fogalmak.

különleges adat: a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;
adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

biometrikus adat: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;

bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés

okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;

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

elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok);

megelőzés: a fenyegetés hatása bekövetkezésének elkerülése;

MTPD (Maximum Tolerable Period of Disruption): Maximálisan tolerálható megszakadási időtartam, az a legnagyobb idő intervallum, ameddig a szervezet tolerálni képes az általa nyújtandó szolgáltatás kiesését;

nyilvántartási rendszer: a személyes adatok bármely módon - centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint - tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

reagálás: a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;

rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

rendkívüli esemény: minden olyan esemény, amely az Adatkezelő és Adatkezelői tevékenységének folyamatosságát támogató informatikai rendszerek folyamatos, üzemzavar mentes működőképességét veszélyezteti, vagy akadályozza;

részleges működőképesség: az az állapot, amikor az informatikai architektúra valamely elemének meghibásodása miatt az informatikai rendszerek bizonyos funkciói, vagy egésze jelentős ideig működésképtelenné válnak;

sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét,

bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

súlyos biztonsági esemény: olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;

teljes körű működésképtelenség: az az állapot, amikor az informatikai architektúra valamely elemének meghibásodása miatt az informatikai rendszerek még a minimális, erősen korlátozott rendszer funkciókat sem tudják ellátni, az ügyviteli folyamatok többségének informatikai támogatása megszűnik, és ennek helyreállítása jelentős időt vesz igénybe;

üzemzavar: az az állapot, amikor az informatikai rendszerek működésében rövid idejű zavar keletkezik, s így a rendszer néhány funkciójának átmeneti meghibásodása következik be, a zavar elhárítását az informatikai üzemeltető a napi rutinja alapján rövid idő alatt képes elvégezni;

védelmi feladatok: megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés

X. Általános tájékoztatás.

Az érintett kérelemére adott válasz felülvizsgálatának kezdeményezésére vonatkozó jogok:

1. Az érintteti jogok gyakorlásának módja: az Érintett az Adatkezelőhöz és / vagy az adatvédelmi tisztviselőjéhez fordulhat (személyesen, telefonon, vagy e-mailen) adatvédelmi jogi kérdéseivel, valamint a gyakorolni kívánt jogai érvényesítésével kapcsolatosan.

2. Az Érintett által beküldött jogosulti igény, kérés esetén, az Adatkezelő köteles a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban egy hónapon belül, közérthető formában, az érintett erre irányuló kérelmére írásban megadni a válaszát.

3. Ha az érintettnek nem sikerült a személyes adatával kapcsolatos tiltakozását, panaszát, kérelmét az Adatkezelőnél megnyugtató módon rendeznie és / vagy úgy ítéli meg, hogy személyes adatai kezelésével kapcsolatban jogsérelem következett be vagy annak közvetlen veszélye fennáll, jogainak érvényesítése érdekében:
   a) a Nemzeti Adatvédelmi és Információszabadság Hatóságnál jogosult bejelentést tenni és / vagy a Hatóság vizsgálatát kezdeményezheti az adatkezelő intézkedése jogszerűségének vizsgálata céljából,
   b) jogosult polgári peres eljárásban bírósághoz fordulni, amelynek elbírálása a Szegedi Törvényszék hatáskörébe tartozik. Az érintett választása szerint a per a lakóhelye szerinti törvényszék előtt is megindítható.

   A Nemzeti Adatvédelmi és Információszabadság Hatóság elérhetőségei:

Székhely:	1055 Budapest, Falk Miksa utca 9-11.
Postacím:	1363 Budapest, Pf. 9.
E-mail:	ugyfelszolgalat@naih.hu
Telefon:	+36 (1) 391 1400, +36 (30) 683-5969 és +36 (30) 549-6838
Ügyfélszolgálati idő:	hétfő - csütörtök 9:00 – 16:00 óra között, péntek: 9:00 – 14.00 óra között
Honlap:	www.naih.hu

S z e g e d, 2023. április

Zsótér Ágnes
Főigazgató