Budapest Főváros XV. Kerületi Önkormányzat Göncz Árpád Szociális Intézmény

székhely: 1157 Budapest, Árendás köz 4-6.,
képviseli: Gráczer Irma Igazgató,
e-mail cím: igazgato@gaszixv.hu,
telefonszám: 06-1-307-6263, 06-1-306-3184.

ADATVÉDELMI SZABÁLYZAT

Adatkezelő: **Budapest Főváros XV. Kerületi Önkormányzat Göncz Árpád Szociális Intézmény** (székhely: 1157 Budapest, Árendás köz 4-6., képviseli: Gráczer Irma Igazgató, e-mail cím: igazgato@gaszixv.hu, tel.: 06-1-307-6263, 06-1-306-3184; adatvédelmi tisztviselő: Dr. Miklós Péter, dmp@dmp.hu). Érintett – az adott adatkezelés jogalapjához igazodóan – jogaival (hozzáférés, helyesbítés, törlés, elfeledtetés, korlátozás, tiltakozás, adathordozhatóság joga, hozzájárulás visszavonásának joga) az Adatkezelő elérhetőségére küldött kérelemmel élhet, továbbá panasszal fordulhat a hatósághoz (www.naih.hu, ugyfelszolgalat@naih.hu, 1363 Bp., Pf. 9.), és ha megítélése szerint megsértették jogait, fordulhat a lakóhelye szerint illetékes bírósághoz.

Belső Adatvédelmi Szabályozási Dokumentáció részei

Dokumentum neve	Elérhetősége
Adatvédelmi Szabályzat	Papír alapon: a székhely, telephelyek mindenkori címei Elektronikusan: Belső informatikai hálózat Weboldal
Szabályzat a közérdekű adatok megismerésére irányuló kérelmek intézésének, továbbá a kötelezően közzéteendő adatok nyilvánosságra hozatalának rendjéről	Papír alapon: a székhely, telephelyek mindenkori címei Elektronikusan: Belső informatikai hálózat Weboldal
Adatfeldolgozók, adattovábbítás címzettjeinek nyilvántartása	Papír alapon: 1157 Budapest, Árendás köz 4-6., Elektronikusan: Belső informatikai hálózat
Különböző tárgyú belső adatvédelmi utasítások	Papír alapon: 1157 Budapest, Árendás köz 4-6., és az idősek klubjainak és ellátások mindenkori címei Elektronikusan: Belső informatikai hálózat
Különböző tárgyú belső adatvédelmi utasítások tudomásul vételéről szóló Munkatársi nyilatkozatok	Papír alapon: (Munkatársak anyagaiban) 1157 Budapest, Árendás köz 4-6., és az idősek klubjainak és ellátások mindenkori címei Amennyiben az átadás-átvétel elektronikusan történt: Belső informatikai hálózat
Külső adatkezelési tájékoztatók Figyelem: a jelen dokumentum tartalmilag BELSŐ szabályozó irat (Információbiztonsági Politika, Adatvédelmi Szabályzat és Adatvédelmi Incidens Kezelési Szabályzat), amely a Munkatársak és a Partnerek kötelezettségeit rögzíti. A GDPR 13–14. cikke szerinti érintetti tájékoztatók ettől elkülönülő, közérthető dokumentumok, amelyeket szolgáltatásonként, cél–jogalap–megőrzés–címzett bontásban kell elkészíteni. Mivel az érintettek jelentős része idős, demens, értelmi fogyatékossággal élő vagy gyermekjóléti ügyfél, a GDPR 12. cikk (1) bekezdése	Papír alapon: 1157 Budapest, Árendás köz 4-6., és az idősek ellátásához tartozó klubbok, szolgáltatások és ellátások mindenkori címei Elektronikusan: http://gaszixv.hu/ Belső informatikai hálózat

szerinti közérthetőség követelménye fokozottan irányadó.	
Adatkezelői nyilvántartás (adatkezelések nyilvántartása)	Papír alapon: 1157 Budapest, Árendás köz 4-6., Elektronikusan: Belső informatikai hálózat
Kameraszabályzat és mellékletei	Papír alapon: 1157 Budapest, Árendás köz 4-6., és az idősek klubjainak és ellátások mindenkori címei Elektronikusan: Belső informatikai hálózat Kamera rendszer kizárólag a felügyelt kapcsolattartás esetén működik. Az Intézmény egyéb helyen nem használ kamerát.
Adatvédelmi incidens kezelési szabályzat	Papír alapon: 1157 Budapest, Árendás köz 4-6., és az idősek klubjainak és ellátások mindenkori címei Elektronikusan: Belső informatikai hálózat
Adatvédelmi incidensek nyilvántartása	Papír alapon: 1157 Budapest, Árendás köz 4-6., Elektronikusan: Belső informatikai hálózat
Közalkalmazotti ellenőrzési szabályzat	Papír alapon: 1157 Budapest, Árendás köz 4-6., és az idősek klubjainak és ellátások mindenkori címei Elektronikusan: Belső informatikai hálózat
Munkatársi adatvédelmi kisokos	Papír alapon: 1157 Budapest, Árendás köz 4-6., Elektronikusan: Belső informatikai hálózat
Belső adatvédelmi program	Papír alapon: 1157 Budapest, Árendás köz 4-6., Elektronikusan: Belső informatikai hálózat
Hozzájáruló nyilatkozatok	Papír alapon (ha papír alapon történik): 1157 Budapest, Árendás köz 4-6., a székhely, telephelyek mindenkori címei Elektronikusan: Belső informatikai hálózat
Adatvédelmi szervezet	Adatvédelmi Szabályzat

Munkaköri leírásokban megfogalmazott feladatok	Papír alapon: (Munkatársak anyagaiban) 1157 Budapest, Árendás köz 4-6., és az idősek klubjainak és ellátások mindenkori címei Elektronikusan: Belső informatikai hálózat
Adatfeldolgozási szerződés(ek)	Papír alapon: 1157 Budapest, Árendás köz 4-6., Elektronikusan (ha elektronikusan letárolásra kerül): Belső informatikai hálózat

Belső Adatbiztonsági Szabályozási Dokumentáció részei

Dokumentum neve	Elérhetősége
Belső Adatbiztonsági Szabályzat	Papír alapon: 1157 Budapest, Árendás köz 4-6., Elektronikusan: Belső informatikai hálózat
Informatikai felhasználói szabályzat	Papír alapon: 1157 Budapest, Árendás köz 4-6., Elektronikusan: Belső informatikai hálózat
Belső adatbiztonsági utasítások	Papír alapon: 1157 Budapest, Árendás köz 4-6., Elektronikusan: Belső informatikai hálózat
Iratkezelési szabályzat és mellékletei	Papír alapon: 1157 Budapest, Árendás köz 4-6., Elektronikusan: Belső informatikai hálózat
Távmunka szabályzat	Papír alapon: 1157 Budapest, Árendás köz 4-6., Elektronikusan: Belső informatikai hálózat

Budapest Főváros XV. Kerületi Önkormányzat
Göncz Árpád Szociális Intézmény

INFORMÁCIÓ BIZTONSÁGI POLITIKA

Hatályos: 2026. 09. 30. napjától

Adatkezelő: **Budapest Főváros XV. Kerületi Önkormányzat Göncz Árpád Szociális Intézmény** (székhely: 1157 Budapest, Árendás köz 4-6., képviseli: Grácz er Irma Igazgató, e-mail cím: igazgato@gaszixv.hu, tel.: 06-1-307-6263, 06-1-306-3184; adatvédelmi tisztviselő: Dr. Miklós Péter, dmp@dmp.hu). Érintett – az adott adatkezelés jogalapjához igazodóan – jogaival (hozzáférés, helyesbítés, törlés, elfeledtetés, korlátozás, tiltakozás, adathordozhatóság joga, hozzájárulás visszavonásának joga) az Adatkezelő elérhetőségére küldött kérelemmel élhet, továbbá panasszal fordulhat a hatósághoz (www.naih.hu, ugyfelszolgalat@naih.hu, 1363 Bp., Pf. 9.), és ha megítélése szerint megsértették jogait, fordulhat a lakóhelye szerint illetékes bírósághoz.

BEVEZETÉS

1. Az Információbiztonsági Politika (a továbbiakban: „*IBP*") az adatvédelmi és adatbiztonsági szabályozási dokumentáció legfelsőbb szintjén helyezkedik el és ily módon hatással van a teljes szabályozási strúktúrára.

2. Az IBP Ismerete és betartása minden Munkatárs és az Adatkezelő bármely informatikai rendszerében felhasználóként szereplő Partner számára kötelező.

I. FEJEZET
AZ IBP MEGFELELŐSÉGE, FELÜLVIZSGÁLATA

1. Az IBP-ben megfogalmazottaknak mindenkor összhangban vannak és megfelelnek a mindenkor hatályos vonatkozó jogszabályoknak. Amennyiben az Adatkezelőre vonatkozó jogszabály tartalmaz IBP hatókörébe tartozó rendelkezést, akkor annak betartása és betartatása minden esetben kötelező és közvetlenül alkalmazandó, kivéve, ha jelen IBP szigorúbb rendelkezést tartalmaz.

2. Az IBP karbantartása és folyamatos felülvizsgáltatása az Adatkezelő adatbiztonsági vezetésének feladata.

3. Az IBP rendszeres felülvizsgálata alapvető fontosságú. Az IBP-t jogszabályi, környezeti és jelentős feladatváltozás esetén, de legalább 2 (két) évente felül kell vizsgálni.

II. FEJEZET
BIZTONSÁGPOLITIKAI ALAPELVEK, CÉLKITŰZÉSEK, KÖVETELMÉNYEK

Az Adatkezelő az informatikai biztonság területén az alábbi alapelveket és védelmi célkitűzéseket kívánja következetesen érvényesíteni minden, a hatálya alá tartozó szervezeti egység, intézmény vonatkozásában a mindenkor hatályos jogszabályi követelményeknek és elvárásoknak megfelelően.

Alapelvek

1. **A védelem teljes körűségre vonatkozó alapelv**et a fizikai, a logikai és az adminisztratív védelem területén a következő dimenziókban kell érvényesíteni:
   a. az összes rendszerelemre,
   b. az informatikai és papír alapú nyilvántartási rendszerek architektúrájának minden rétegére, azaz így például a számítástechnikai infrastruktúra, mind az alkalmazások szintjén, mind a központi, mind a végponti informatikai eszközökre és környezetükre.

2. **A védelem zártságának alapelve**: A zárt védelem akkor biztosított, ha az összes valószínűsíthető fenyegetés elleni megelőző védelmi intézkedések megvalósításra kerültek, és azok szerves egységet alkotnak.

3. **A védelem kockázat arányosságának alapelve:** A védelem mértéke és költségei a felmért kockázatokkal arányos. Természetes célkitűzés a minimális védelmi költséggel elért maximális védelmi képesség.

4. **A védelem folytonosságának alapelve:** A kialakított védelmi képességeket a rendszerek teljes életciklusa alatt folytonosan biztosítani és fejleszteni kell.

Célkitűzések, követelmények

1. Alapvető célkitűzés a következőkben megfogalmazott követelmények maradéktalan teljesítése.

2. **Bizalmasság biztosítása** az Adatkezelő által rögzített, kezelt információkhoz való hozzáférés tekintetében, elsősorban a szervereken, továbbá a munkaállomásokon történő adathozzáférések és az adatkezeléseknél használt felhasznált adathordozók kezelése, nem elektronikus adathordozók kezelése, valamint a kommunikáció során. A bizalmasság így tehát az adatnak azon tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosult, és kizárólag a jogosultság szintjének megfelelően ismerheti meg, valamint rendelkezhet róla, ha a megismerési jogosultsággal rendelkezőnek van rendelkezéshez joga.

3. **Sértetlenség biztosítása** az Adatkezelő adatkezelése, adatfeldolgozása és kommunikációja során. Követelmény, hogy pontos és a valóságnak mindenben megfelelő információk kerüljenek az informatikai és papír alapú nyilvántartási rendszerekben rögzítésre, feldolgozásra, és ezen információ sértetlensége az adatkezelés során mindvégig biztosított legyen.

4. **Rendelkezésre állás biztosítása** az Adatkezelő által kezelt információk tekintetében. Követelmény a rögzített adatok vonatkozásában azok visszakereshetősége, melynek záloga az informatikai rendszerek funkcióinak és elérhetőségének folyamatos biztosítása.

5. **Működőképesség fenntartása** az Adatkezelő informatikai rendszereire és nem informatikai rendszerelemeire vonatkozóan, amely az adott informatikai eszköz vagy rendszer elvárt és igényelt üzemelési állapotban való fennmaradását jelenti. Ennek elérése céljából biztosítani kell a munkatársak megfelelő tudását, valamint a szükséges technikai feltételeket is.

6. **A fizikai és szervezeti védelem**, környezeti infrastruktúra területén az Adatkezelő vezetésének célkitűzése a következő: az Adatkezelő minden objektumának biztonságának szavatolása, az információ kezelését, feldolgozását végző helyiségek, valamint az egyes eszközök, az abban elhelyezett adattárolók és adathordozók fizikai védelmének biztosítása, papír formában, valamint elektronikusan kezelt és tárolt információk, tárgyi eszközök, vagy szolgáltatást végző személyek védelmének biztosítása a különböző eseményektől, mint tűz, víz, áramellátás kimaradása, külső támadások, betérés, informatikai, vagy egyéb úton keletkezett adatok és információk kezelése során az előírt fizikai informatikai biztonsági követelmények betartásának elősegítése, szállításra, karbantartásra vonatkozó fokozott biztonsági intézkedések bevezetése, személyi felelősségek egyértelmű meghatározása és elhatárolása.

Egyéb követelmények

1. A kialakított adatvédelmi és adatbiztonsági szabályozási dokumentáció egyik eleme sem mondhat ellent a mindenkor hatályos jogszabályoknak és a mindenkor hatályos IBP-nek.

2. A munkatársakkal, amennyiben ez szükséges, akkor szervezet oktatás keretében meg kell ismertetni a rájuk vonatkozó szabályokat és be kell tartatni velük a gyakorlati működésük során.

3. Az Adatkezelő informatikai kapcsolatainak kialakítására és biztosítására kizárólag, olyan technikai és adminisztratív intézkedések engedélyezhetők, illetve valósíthatók meg, amelyekkel a jogszabályi és egyéb előírásoknak megfelelően biztosított az informatikai rendszerek védelme. Ehhez kapcsolódik az, hogy az Adatkezelő informatikai rendszereit logikai, technikai és adminisztratív eszközökkel védeni kell a külső kapcsolatok, más szervezetek és az internet felől érkező támadásokkal szemben.

4. Az információk tárolására és egyéb módon történő kezelésére használt hardver és szoftver rendszereket, elemeket a külső környezeti hatásoktól folyamatosan védeni kell.

5. Az Adatkezelő munkatársai, felhasználói csak ellenőrzött körülmények között, a szükséges felhasználói jogosultságokkal férhetnek hozzá az említett rendszerekhez, szolgáltatásokhoz. Külső felek kizárólag szükség esetén, szerződésben vagy más dokumentumban szabályozott és folyamatosan az Adatkezelő által ellenőrzött körülmények között, kizárólag a legszükségesebb rendszerekhez és információkhoz férhetnek hozzá, a lehet legrövidebb ideig.

6. Rendelkezéseket kell kidolgozni a hardver és szoftver rendszerek kezelésére, valamint ezek megsemmisüléstől és illetéktelen hozzáféréstől történő védelmére.

7. Az elektronikus vagy papír alapú adatrögzítés során biztosítani kell a forrás dokumentumok, az adatbeviteli munkakörök és munkaállomások, rendszerek biztonságát, azonosíthatóságát, valamint a bevitt adat ellenőrzését és a hibás bemeneti adatok kezelését.

8. Biztosítani kell az információk rendszeres mentését, letárolását és visszaállítási teszteket kell dokumentáltan elvégezni.

9. Az Adatkezelő köteles kialakítani, fenntartani olyan információkezelésre szolgáló rendszereket, ideértve hardver és szoftver rendszereket is, és olyan célokat és terveket alkotni, valamint olyan nyilvántartásokat bevezetni, amelyek alapjai egy pontos és helyes szakmai kockázatelvű vizsgálatnak.

10. Az Adatkezelő feladata az informatikai biztonsági szervezet és rendszerek informatikai biztonsági tervezése és a tervek végrehajtása. Az Adatkezelő igénybe vehet informatikai biztonsági szakértőket annak érdekében, hogy a vonatkozó szabványok és ajánlások érvényre juthassanak.

11. A szoftverkezelés biztonságával kapcsolatban követelmény, hogy az Adatkezelő kizárólag jogtiszta, az üzemeltetéshez, adatkezeléshez és feldolgozáshoz szükséges, előzetesen engedélyezett informatikai rendszerek, alkalmazások, programok, irodai szoftvercsomagok, feldolgozó programok futhassanak.

12. A rosszindulatú szoftverek (pl. vírusok, malware programok, stb.) elleni védekezés követelményeként megfelelő megelőző, felderítő és korrekciós mechanizmusokat kell bevezetni és folyamatosan alkalmazni.

13. Biztosítani kell az ügykezelés folytonosságot, a rendszer folyamatos működést úgy, hogy az ügymenetben bekövetkezett zavarokat késlekedés nélkül ellensúlyozni, kivizsgálni, kijavítani lehessen. Ennek megfelelően a kritikus folyamatokat védeni kell a nagyobb hibák, katasztrófák következményeitől.

14. Az informatikai biztonsági eseményeket észlelni és kezelni kell a megfelelően kidolgozott, dokumentált, a munkatársak által elsajátított eljárás alapján. Ezzel kapcsolatban követelmény az események visszakereshetősége, a naplózás.

15. A dokumentációs rendszert rendszeresen felül kell vizsgálni, aktualizálni, karban kell tartani, hogy az informatikai rendszerekben történt változásokat, alkalmazott eljárásokat az Adatkezelő dokumentált formában végezhesse. Ennek megfelelően a következő esetekben kell felülvizsgálatot végrehajtani:
    a. Az Adatkezelő és/vagy a szervezetek, szervezeti egysége igényei, céljai megváltoznak
    b. új területek, szolgáltatások jelennek meg, módosulnak vagy szűnnek meg
    c. új informatikai szolgáltatások, technológiák, rendszerek, rendszerelemek jelennek meg, módosulnak, vagy szűnnek meg
    d. a kockázatelemzés következtében új, lényeges változtatások válnak szükségessé.

16. Az Adatkezelő célúl tűzte ki a kockázatokkal arányos védelem biztosítása érdekében a kockázatelemzés rendszeres és részletes, belső szabályozás szerinti elvégzését a fenyegetések, a gyenge pontok, a nem elviselhető kockázati pontok meghatározására, valamint az ezekhez kapcsolódó védelmi intézkedéseket, amelyekhez vonatkozó határidőt és felelőst kell rendelni.

17. Az Adatkezelő számára az információbiztonság sikeres megvalósítása során kritikus tényezőként kell tekinteni a következőket:
    a. Vezetőség elkötelezettségének mértéke
    b. a környezet naprakész és pontos meghatározása a biztonsági szabályozáshoz
    c. a biztonsági követelmények, a kockázatbecslés és a kockázatkezelés megértése és helyes alkalmazása;
    d. a biztonság hatékony menedzselése valamennyi érintett felé;
    e. gondoskodás a kellő oktatásról és képzésről;
    f. átfogó, mindenre kiterjedő és kiegyensúlyozott ellenőrzési rendszer bevezetése, a teljesítőképességének értékeléséhez és a helyesbítési javaslatok visszacsatolásához;
    g. a biztonsági események kezelésének megfelelő szabályozása, értékelése, visszacsatolása.

Lezárva: Budapest, 2026. szeptember hó 30. napján

Gráczer Irma
Igazgató
Budapest Főváros XV. Kerületi Önkormányzat
Göncz Árpád Szociális Intézmény

Bp. Főv. XV. ker. Önkormányzat Göncz Árpád Szociális Intézmény 1157 Bp., Árendás köz 4-6.

- ADATVÉDELMI SZABÁLYOZÁS –
Az adatvédelmi utasítás *1. számú* melléklete:

Budapest Főváros XV. Kerületi Önkormányzat
Göncz Árpád Szociális Intézmény

ADATVÉDELMI SZABÁLYZAT

Hatályos: 2026. 09. 30. napjától

Adatkezelő: **Budapest Főváros XV. Kerületi Önkormányzat Göncz Árpád Szociális Intézmény** (székhely: 1157 Budapest, Árendás köz 4-6., képviseli: Gráczer Irma Igazgató, e-mail cím: igazgato@gaszixv.hu, tel.: 06-1-307-6263, 06-1-306-3184; adatvédelmi tisztviselő: Dr. Miklós Péter, dmp@dmp.hu). Érintett – az adott adatkezelés jogalapjához igazodóan – jogaival (hozzáférés, helyesbítés, törlés, elfeledtetés, korlátozás, tiltakozás, adathordozhatóság joga, hozzájárulás visszavonásának joga) az Adatkezelő elérhetőségére küldött kérelemmel élhet, továbbá panasszal fordulhat a hatósághoz (www.naih.hu, ugyfelszolgalat@naih.hu, 1363 Bp., Pf. 9.), és ha megítélése szerint megsértették jogait, fordulhat a lakóhelye szerint illetékes bírósághoz.

BEVEZETÉS

1. A Göncz Árpád Szociális Intézmény, mint adatkezelő ezúton tájékoztatja a jelen Adatvédelmi Szabályzat megismerőjét, hogy tiszteletben tartja minden természetes személy jogszabályokban biztosított jogait, továbbá az adatvédelem alapelveit és szabályait, ezért a végzett adatkezelései során 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 szóló, az Európai Parlament és a Tanács (EU) 2016/679. sz. általános adatvédelmi rendelete (a továbbiakban: „***GDPR***"), továbbá *„Az információs önrendelkezési jogról és az információszabadságról"* szóló 2011. évi CXII. törvény (a továbbiakban: „***Infotv***"), a működésre vonatkozó más jogszabályok, iránymutatások, állásfoglalások és az ezekkel összhangban levő adatvédelmi szabályozási dokumentáció. Így különösen, de nem kizárólagosan a jelen Adatvédelmi Szabályzat (a továbbiakban: „***Szabályzat***"), valamint a belső adatbiztonsági dokumentáció egyéb mindenkori rendelkezései alapján (a rovábbiakban: „***Egyéb intézkedések***") jár el.

2. A Göncz Árpád Szociális Intézmény fenntartja a jogot arra, hogy az adatvédelmi szabályozási dokumentáció bármelyik részét, egészét, egységét egyoldalú döntése alapján – különösen az időközben módosulandó jogszabályi háttérrel és egyéb belső szabályzattal való összehangolása érdekében- illetve azon túlon is bármikor megváltoztassa.

3. Az adatvédelmi szabályozási dokumentáció minden tagjának mindenkor hatályos változata elektronikus formában a Göncz Árpád Szociális Intézmény belső informatikai rendszerében, papír alapon az Adatkezelő központi székhelyen érhető el (a pontos elérhetőség a lábjegyzetben található). A fentiek alapján a szabályozási dokumentáció, így többek között a Szabályzat rendelkezéseit a Göncz Árpád Szociális Intézmény magára nézve kötelezőnek tekinti, és működése során ezeknek megfelelően jár el.

4. Hivatkozva az 1. pontra, a jelen Szabályzat az érintettek számára a Budapest Főváros XV. Kerületi Önkormányzat Göncz Árpád Szociális Intézmény által végzett adatkezelési tevékenységeket általánosan és egyedien, részletesen is szabályozza a következő, egyébként az átláthatóság elvét (GDPR 5. cikk (1) a) pont) kielégítő módon:
    a. Szabályzat fejezetei általános rendelkezéseket tartalmaznak minden végzett adatkezelésre vonatkozóan,
    b. a Szabályzat hivatkozik belső utasításokra és más, a szabályozási dokumentáció részét képező szabályozó, valamint tájékoztató dokumentumokra (Word formátumú verzióban a kereszthivatkozások működnek)
    c. az egyes végzett adatkezelési tevékenységek leírását a vonatkozó 2023/GÁSZI/GDPR belső adatvédelmi utasítás, valamint a függelékek tartalmazzák egységekre bontva és csoportosítva. Így az adott adatkezelési tevékenység meghatározás minden esetben együttesen értelmezendők a dokumentumok. A leírásokat egyrészt a Munkatársaknak, Partnereknek ismerniük és betartaniuk szükséges, valamint folyamatosan kötelesek vezetni a nyilvántartásokat, adatkezelési nyilvántartásokat, adatvagyon leltárt, mivel a leírások tájékoztatóként is szolgálnak, így ezeket a Munkatársaknak elérhetővé kell tenniük, valamint ilyen célból át kell adniuk más érintettek számára;

d. A vonatkozó 2023/GÁSZI/GDPR belső adatvédelmi utasítás mellékleteiben meghatározott leírások/tájékoztatók a Göncz Árpád Szociális Intézmény adatvagyonleltárát is alkotják, így képezve egy összetett egységet;
e. A vonatkozó 2023/GÁSZI/GDPR belső adatvédelmi utasítás mellékletben meghatározott egyes adatkezelési tevékenységek leírásai/tájékoztatói tartalmaznak táblázato(ka)t, valamint kérdés-felelet formátumban jöttek létre, a gyors és könnyű áttekinthetőség miatt, továbbá a jobb olvashatóság érdekében a kérdések vastag betűvel szedettek, a dőlt betűvel jelölt részek pedig értelmező magyarázatokat tartalmaznak

5. A Göncz ÁrpádSzociális Intézmény törekszik arra, hogy minél pontosabban betartsa a Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlásait, így különösen az előzetes tájékoztatás adatvédelmi követelményeiről szóló 2015. szeptember hó 29. napján kiadott ajánlását, és ezért a lehető legérthetőbben fejezi ki az adatvédelmi szabályokat, szükség esetén példákkal magyarázva azokat, valamint részletesen bemutatja az egyes adatkezelési tevékenységeket, hogy az érintett megismerhesse azokat.

6. **Tekintettel az előzetes tájékoztatás kötelezettségére, valamint az átláthatóság elvére, továbbá a működés üzleti titkaira, a Göncz Árpád Szociális Intézmény az egyes tájékoztatók összefoglaló táblázatát, mint az adatvédelmi szabályozási dokumentáció részét képező Külső Adatkezelési Tájékoztatót a http://gaszixv.hu/ oldalon tette közzé, valamint papír alapon elérhetővé tette a 1157 Budapest, Árendás köz 4-6., címen.**

1. FEJEZET: FOGALOMMEGHATÁROZÁS

1. A Göncz Árpád Szociális Intézmény a következő fogalmakat használja a jelen Szabályzatban és annak mellékleteiben, függelékeiben, ezért javasolja a fogalmak és az Adatkezelőre vonatkozó jellemző példák részletes áttekintését.

Fogalom meghatározása	Magyarázó és jellemző példa
Adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja	Adatkezelő a 2. fejezetben meghatározott személy: Göncz Árpád Szociális Intézmény
Érintett: bármely információ alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy;	Minden természetes személy, akinek adatát az Adatkezelő kezeli, pl. Munkatárs, ügyfél, természetes személy Partner, Partner kapcsolattartója, stb. Az érintett fogalma minden egyes adatkezelés esetében meghatározásra került I. sz. mellékletben, az adott adatkezelés leírásában.
Személyes adat fogalma: az érintettre vonatkozó bármely információ	Pl. név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező, így ezek személyes adat a telefonszám, e-mail cím, anyja neve, IP cím, bankszámlaszám, stb. Az egyes adatkezelés során a kezelt személyes adatok körei (legalább hivatkozással) meghatározásra kerültek.
Különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok	Pl. egészségügyi adat
Hozzájárulás: az érintett akaratának önkéntes, kifejezett és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez, így tehát a hozzájárulásnak 3 alapeleme van: az önkéntesség, a határozottság, és a megfelelő tájékozottság	A gyakorlatban ilyen valamely adatkezeléshez hozzájáruló nyilatkozat (pl. képkészítéshez)
Adatkezelés: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.	Adatkezelési művelet vagy tevékenység egy másik adatkezeléstől a célja alapján válik el. Pl. egyszeri információkérés, adattörlés, stb.
Profilalkotás: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják	Ilyen adatkezelést az Adatkezelő nem végez!
Álnevesítés: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni	Pl. azonosító kibocsátása és használata egy érintettel kapcsolatban
Adattovábbítás vagy adatközlés: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele	Adattovábbítás Partner, hatóság, stb. felé

Adatfeldolgozás: adatfeldolgozó által végzett adatkezelés;	Például tárhelyszolgáltatás, stb., amelyeket az Adatkezelő külső vállalkozótól igénybe vesz
Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel	Pl. tárhelyszolgáltató, stb.
Adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges	Elektronikusan tárolt adatok visszaállíthatatlan törlése
Adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése, így például az adatokat tartalmazó irat ledarálása	Pl. papír alapú dokumentumok fizikai megsemmisítése
Adatállomány: az egy nyilvántartásban kezelt adatok összessége	Egy-egy adatbázisban kezelt adatok összessége
Nyilvántartási rendszer: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető	Adatkezelő által használt elektronikus és/vagy papír alapú nyilvántartás
Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval, vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak	Pl. egy másik adatkezelő
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	Pl. hackelés eredménye, zsarolóvírus, adatszivárgás, adatlopás
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	Valamilyen megbetegedés, étel vagy más allergia, stb.
Partner: az Adatkezelő szolgáltatásait szerződés alapján igénybe vevő és/vagy az Adatkezelő szolgáltatásainak teljesítéseit elősegítő jogi személyek, jogi személyiséggel nem rendelkező gazdasági társaságok, amelyek felé az Adatkezelő személyes adatot továbbít vagy továbbíthat, vagy amelyek az Adatkezelő számára adattárolási, feldolgozási, kapcsolódó informatikai és egyéb biztonságos adatkezelést elősegítő tevékenységet végeznek vagy végezhetnek	Ilyenek például az adatfeldolgozást végző szervezetek, mint amilyen egy külső marketinges cég, stb.
Munkatárs: az Adatkezelővel közalkalmazotti, megbízási-, munka-, vagy egyéb jogviszonyban levő természetes személy, aki az Adatkezelő szolgáltatásainak ellátásnak, teljesítésének feladatával van bízva és adatkezelési vagy adatfeldolgozási feladatai során személyes adatokkal kapcsolatba kerül vagy kerülhet, és akinek tevékenységével kapcsolatban az Adatkezelő teljes felelősséget vállal az érintettek személyi köre és harmadik személyek irányában	Közalkalmazott, megbízott, stb.
Weboldal	A http://gaszixv.hu/ portál és minden aloldala, amelynek üzemeltetője az Adatkezelő
Közösségi oldal	https://www.facebook.com/gaszixv

2. FEJEZET: AZ ADATKEZELŐ MEGHATÁROZÁSA

2.1 Az Adatkezelő személye

1. Jelen Adatvédelmi Szabályzat szempontjából Adatkezelő:

Göncz Árpád Szociális Intézmény

a. székhely és a tényleges adatkezelés címei:
1157 Budapest, Árendás köz 4-6.,

telephelyek címei:
Az aktuális Szervezeti és Működési Szabályzatban

b. adószám: 15515579-2-42
c. internetes elérhetőségei (és a vonatkozó tényleges adatkezelések webhelyei):
   i. http://gaszixv.hu/
   ii. https://www.facebook.com/-
d. telefonszám: 06-1-307-6263, 06-1-306-3184
e. e-mail: Igazgato@gaszixv.hu
f. intézmények és szolgáltatások elérhetőségei: http://gaszixv.hu/
g. képviseli: Gráczer Irma Igazgató
h. adatvédelmi tisztviselő neve és elérhetősége: Dr. Miklós Péter, postai úton elérhető a az Adatkezelő 1157 Budapest, Árendás köz 4-6. szám alatti székhelyére címzett levél, e-mail-ben pedig a dmp@dmp.hu címre küldött e-mail útján

2.2. Közös adatkezelés

1. Adatkezelő együttes, közös adatkezelést nem végez.

2.3. Adatfeldolgozó igénybevétele

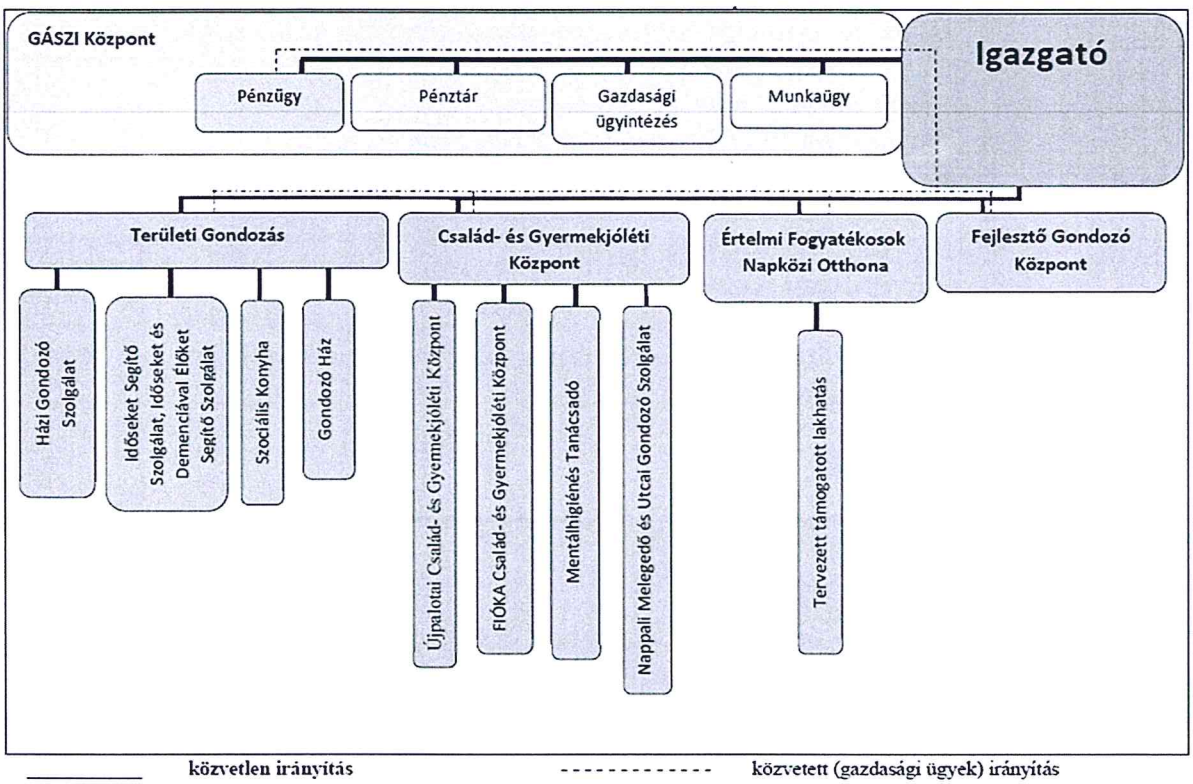
Nem adatfeldolgozó az Adatkezelő nevében eljáró saját Munkatárs (gondozó, szociális és terápiás munkatárs, egységvezető), továbbá az a szerv, amely hatósági jogkörében jár el (működést engedélyező szerv, fenntartó, Magyar Államkincstár): ezek önálló adatkezelők, illetve címzettek [GDPR 4. cikk 8. pont, 28. cikk].

1. Az 1993. évi III. törvény (továbbiakban: „***Szt.***") 92/K. § (7) bek. alapján felhatalmazást kapott a működést engedélyező szerv arra, hogy a működés személyi és tárgyi feltételeinek, a működés jogszerűségének, a szociális szolgáltatásra való jogosultság megállapításának, illetőleg az intézményi jogviszonyra vonatkozó szabályok megtartásának ellenőrzése érdekében, az ahhoz szükséges mértékben
   - megismerhesse és kezelhesse az ellátott, törvényes képviselője, az ellátott tartására jogszabály, szerződés vagy bírósági határozat alapján köteles személy, a térítési díjat, az egyszeri hozzájárulást megfizető és a belépési hozzájárulás megfizetését vállaló személy, továbbá a szolgáltató, intézmény alkalmazottjának a személyes adatait,
   - betekinthessen az Adatkezelő létrehozásával, működésével és megszűnésével, illetve az intézményi jogviszony keletkezésével, fennállásával és megszűnésével összefüggő

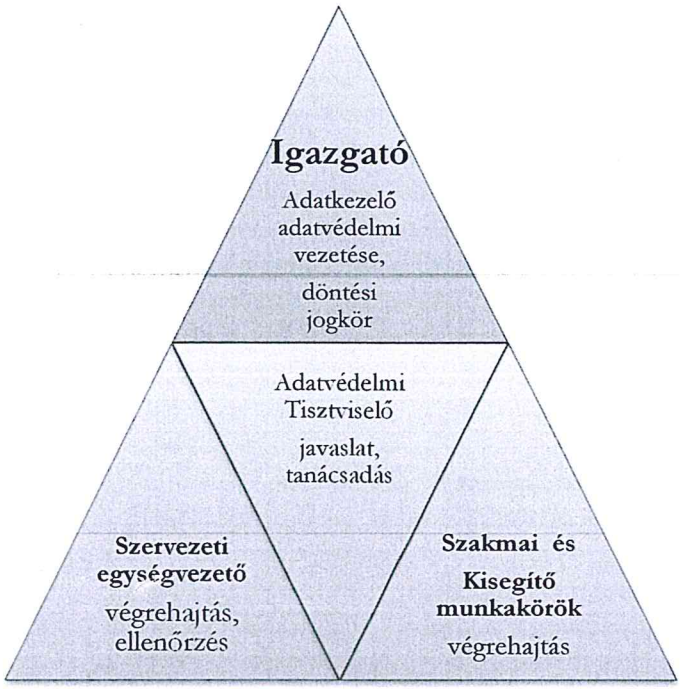
iratokba, kérhesse azok bemutatását, azokról másolatot készíthet, illetve azokat zár alá vehesse.

2.2 A 369/2013. (X. 24.) Korm. rendelet 3. § (1) bek. alapján a Kormány az Szt. és a Gyvt. alkalmazása során működést engedélyező szervnek a fővárosi és megyei kormányhivatalt (a továbbiakban: „***Kormányhivatal***") jelöli ki. A Kormányhivatal e hatósági jogkörében nem az Adatkezelő adatfeldolgozója, hanem önálló adatkezelő (címzett) [GDPR 4. cikk 8. pont, 28. cikk]; a felé történő adatszolgáltatás jogalapját a fenti jogszabályi rendelkezések adják. Az Adatkezelő tényleges adatfeldolgozói jellemzően az IT- és rendszerüzemeltetési szolgáltatók, valamint az étkeztetést és a szállítást végző szolgáltatók.

2.3 Az Adatkezelő szervezeti felépítése



2.4 Az Adatkezelő adatvédelmi szervezete



1. Az Adatkezelő adatvédelemmel, adatkezeléssel, adatbiztonsággal és információbiztonsággal kapcsolatos vezetését az Igazgató (továbbiakban: „***Adatkezelő adatvédelmi vezetése***") látja el.

2. Az Adatkezelő adatvédelmi vezetése a Munkatársak felé tett szabályzatokkal és utasításokkal, illetve intézkedésekkel az Adatkezelő teljes szervezetét irányítja adatvédelem, adatkezelés szempontjából.

3. Az Adatkezelő adatvédelmi vezetése

   a) biztosítja az adatvédelmi tevékenység irányításához és ellátásához, valamint az érintett jogai gyakorlásához szükséges személyi és tárgyi feltételeket;
   b) felelős az adat- és titokvédelmi, valamint biztonsági és információbiztonsági szabályzatok kiadásáért és betartatásáért;
   c) dönt az Adatkezelőn kívüli Partnerek személyéről, és a vonatkozó, adatfeldolgozást is felölelő szerződés tartalmáról;
   d) gondoskodik arról, hogy az adatvédelmi tevékenység során esetleg előforduló, feltárt hiányosságok megszűntetéséről, szükség szerint a felelősségre vonásról;
   e) meghatározza az adatkezelési tevékenységeket;
   f) meghatározza a szervezeti egységek vezetőinek javaslata alapján a szervezeten kívüli személy vagy szerv által elvégzendő adatfeldolgozási feladatok időpontját;
   g) rendszeresen ellenőrzi az adatkezelést és adatvédelmet, valamint az informatikát érintő nyilvántartásokat;

h) engedélyezi a Munkatárs munkakör ellátásához szükséges informatikai alkalmazásokhoz való hozzáférési jogosultságot;
i) jóváhagyja és kiadja a belső adatvédelmi szabályozási dokumentáció elemeit;
j) ellát egyéb olyan feladatot, amelyet a jelen Szabályzattól formailag eltérő más szabályzat, utasítás vagy jogszabály meghatároz.

4. Az egységvezetők
   a) meghatározzák az irányításuk alatt álló adatgazdák hozzáférési jogosultságait;
   b) koordinálják az adatgazdák adatvédelemmel és adatkezeléssel kapcsolatos tevékenységét;
   c) gondoskodnak az adatgazdák helyettesítési rendjéről;
   d) javaslatot tesznek az Adatkezelő vezetése felé a Partnerek – ideértve az adatfeldolgozókat is – személyére;
   e) biztosítják az irányításuk alá tartozó szervezeti egységnél az adatkezelés és az adatvédelem rendjét.

5. A fentieken túl a szervezeti egységvezető köteles
   a) az adatkezeléssel, adatvédelemmel kapcsolatos szabályokat megismerni és betartani,
   b) oktatáson részt venni, a beosztottak részvételét támogatni és ellenőrizni, oktatási anyagok ismeretét ellenőrizni,
   c) tájékoztatást nyújtani a beosztott Munkatársak és egyéb érintettek számára,
   d) az Adatkezelőn kívülről jövő megkeresések, és/vagy jogok érvényesítésének észlelést követően annak azonnali írásbeli (ideértve az e-mail-t is) továbbítása az adatvédelmi tisztviselő, vagy ha ilyen pozíció átmenetileg betöltetlen, úgy az Intézményvezető vagy helyettese számára,
   e) adatvédelmi vagy adatbiztonsági incidens estén az incidens jelzését/észlelését követően azonnal jelezni azt és annak körülményeit az adatvédelmi tisztviselő, vagy ha ilyen pozíció átmenetileg betöltetlen, úgy az Intézményvezető vagy helyettese számára, és közreműködni az incidens elhárításában, kárenyhítésben, részletes felderítésben.

6. Amennyiben az Adatkezelő adatvédelmi tisztviselőt nevezett ki, úgy az adatvédelmi tisztviselő feladatait a GDPR és az Infotv rendelkezései, valamint az adatvédelmi tisztviselővel kötött szerződés határozza meg.

7. Az adatvédelmi tisztviselő feladataiból adódóan adatkezelési tevékenységek céljait, eszközeit nem határozhatja meg, kizárólag javaslatot tehet, tanácsot adhat, és kizárólag az Adatkezelő jogosult az adatkezelések céljait, eszközeit meghatározni az ehhez kapcsolódó nyilvántartásokat, leltárokat folyamatosan vezetni és naprakészen tartani.

8. Abban az esetben, ha az Adatkezelő Adatvédelmi vezetése egy vagy több adatkezeléssel, adatvédelemmel, adatbiztonsággal kapcsolatos feladatot delegál az adatvédelmi kapcsolattartóra, úgy e személy konkrét feladatait a munkautasítás(ok), és/vagy munkaköri leírás tartalmazza, vagy a szerződő felek külön szerződésben határozzák meg, ezért azokat a jelen Szabályzatban meghatározni nem lehet.

9. Adatkezelő egyidőben, párhuzamosan kijelölhet adatvédelmi tisztviselőt és egy vagy több adatvédelmi kapcsolattartót is, ebben az esetben egy vagy több önálló dokumentumban a tisztviselő és a kapcsolattartó(k) feladatait pontosan el kell határolni és meg kell határozni az egymáshoz való alá-fölé vagy mellérendeltségi (pl. helyettesítési) viszonyukat is. Ha az

Adatkezelő adatvédelmi vezetése máshogyan nem rendelkezik, a kapcsolattartó a tisztviselő alárendeltje és a tisztviselőt – annak akadályoztatása esetén és idejében – helyettesíteni köteles.

10. A Jelen Szabályzat hatályba lépése pillanatában kinevezett adatvédelmi tisztviselő valamint az adatvédelmi kapcsolattartó(k) nevét és elérhetőségi adatait (ha ilyen pozíció(k) betöltésre került(ek)) a 2. fejezet tartalmazza.

11. Minden Munkatárs a rá vonatkozó jogszabályokból, belső szabályzatokból és szabályokból, utasításokból, munkaköri leírásból, oktatási anyagból fakadó kötelezettségeket betartva végzi feladatait.

12. Adat törlését, helyesbítését (módosítását), zárolását, továbbítását vagy megsemmisítését csak az Adatkezelő adatvédelmi vezetése, vagy az általa e feladattal megbízott Munkatárs végezheti el, és kizárólag abban az esetben, ha meggyőződött arról, hogy a műveletnek jogszabályokban, a Szabályzatban, vagy egyéb szabályzatban, utasításban meghatározott feltételei fennállnak.

13. Amennyiben jogszabály, vagy az adatvédelmi szabályozási dokumentáció valamely része előírja, az adatok törlésének, helyesbítésének (módosításának), zárolásának, továbbításának vagy megsemmisítésének tényét az azt végrehajtó Munkatársnak megfelelően dokumentálnia kell.

14. Minden Munkatárs köteles
    a) a munkafolyamatok megfelelő szabályozása, szervezése útján gondoskodni arról, hogy
        i. maradéktalanul érvényesüljenek az adat- és titokvédelmi előírások;
        ii. az egyes Munkatársak, valamint Partnerek kizárólag a feladatellátásukhoz szükséges mértékben juthassanak az adatok birtokába; ugyanakkor
        iii. adatkezelése során a rendelkezésre állás elve érvényesüljön, vagyis az adatok a hozzáférésre jogosult más Munkatárs, vagy harmadik személy számára elérhetőek és felhasználhatóak legyenek, ha azok a feladataik elvégzéséhez szükségesek;
        iv. az adatok illetéktelen harmadik személyek birtokába kerülésének kockázata a lehető legkisebbre csökkenjen; ennek körében például a feladatvégzésével összefüggésben az általa létrehozott, vagy birtokába került adatokat (pl. manuálisan kitöltött formanyomtatvány, kinyomtatott Word vagy Excel dokumentum, stb.) köteles megvédeni a jogosulatlan hozzáféréstől, az elveszéstől, a fizikai károsodástól és a megsemmisüléstől. Ennek érdekében az adathordozó dokumentumokat a közvetlen felügyelete alatt, vagy a munkavégzés helyén, illetéktelenek számára nem hozzáférhető, zárt helyen (lezárt fiókban, szekrényben) kell tartania;
        v. az adott terület adatkezelési és adatmentési tevékenysége, annak folyamata a vonatkozó adatvédelmi jogszabályokkal, továbbá az Adatkezelő szabályzataival összhangban történjen;
        vi. minden Munkatárs köteles a vonatkozó adatkezelési nyilvántartásokat naprakészen tartani és az ehhez szükséges írásbeli intézkedéseket meghozni. Amennyiben új adatkezelés merül fel, vagy egyes adatkezelések változnak, megszűnnek, módosulni az egységvezető köteles előzetesen egyeztetni az adatvédelmi vezetés többi egységével és a szükséges módosításokat az egyeztetés alapján elvégezni.

b) az elvárható legnagyobb gondossággal eljárni. Ezzel összefüggésben köteles megtenni mindazokat a technikai és szervezési intézkedéseket, amelyeket a mindenkor hatályos vonatkozó jogszabály, a jelen Szabályzat, egyéb belső szabályzat, utasítás, munkaköri leírás, stb. előír, valamint ezen túlmenően is, mindazt, amit az adott helyzetben az ésszerűség megkövetel;
c) a felhasználói azonosító és a jelszó titkos kezelésére, e feladat teljesítése körében a Munkatárs az azonosító és jelszó adatait bármilyen adathordozón csak és kizárólag saját felhasználás céljából rögzítheti, és ez esetben gondoskodnia kell arról, hogy ahhoz rajta kívül senki más ne férhessen hozzá. A Munkatárs az elektronikus adattárolási helyeken (nyilvántartási rendszerben) rögzített adatokhoz csak a saját hozzáférési jogosultságának keretei között, a saját felhasználói azonosítójával és jelszavával jogosult hozzáférni;
d) az elektronikusan tárolt adatok elvesztésének megakadályozása érdekében a kizárólag általa használt adattárolási helyeken lévő adatokról rendszeres időközönként biztonsági mentést végezni, vagy végeztetni a megfelelő pozícióban levő más Munkatárssal;
e) titoktartás követelményét betartani, amely a személyes és a különleges kategóriájú személyes adatok tekintetében időkorlátozás nélkül fennáll.
f) a jogszabályok és az adatvédelmi szabályozási dokumentáció rendelkezéseit megismerni és betartani,
g) az adatkezeléssel, adatvédelemmel kapcsolatos oktatásokon részt venni,
h) tájékoztatást nyújtani az érintettek számára kérés esetén,
i) az Adatkezelőn kívülről jövő megkeresések, és/vagy jogok érvényesítésének észlelést követően azt azonnal továbbítani az adatvédelmi tisztviselő (kapcsolattartó felé, ha a pozíció betöltésre került),
j) adatvédelmi vagy adatbiztonsági incidens estén az incidens észlelését követően azonnal jelezni azt és annak körülményeit az Adatkezelő adatvédelmi vezetése számára, és az adatvédelmi tisztviselő (kapcsolattartó felé, ha a pozíció betöltésre került), és közreműködni az incidens elhárításában, kárenyhítésben, részletes felderítésben,
k) a nem szabályozott működésbeli változások esetén, amelyek adatvédelemre, adatkezelésre is kihathatnak, az észlelést követően azonnali jelezni a változás mibenlétét az adatvédelmi tisztviselő (kapcsolattartó) felé,
l) együttműködni az adatvédelmi tisztviselővel (kapcsolattartóval).

15. A Munkatársak egyes konkrét feladatait a belső adatvédelmi és adatbiztonsági dokumentációba tartozó dokumentumok, más szabályzatok, a vonatkozó szerződés, munkaköri leírás, és más dokumentumok szabályozzák

16. Amennyiben egy Munkatársat az Adatkezelő adatvédelmi vezetése adatvédelmi kapcsolattartóként nevezett meg, úgy az adatvédelmi kapcsolattartó a feladatai vonatkozásában a beszámolási kötelezettségét az adatvédelmi tisztviselő felé kell, hogy teljesítse. Amennyiben a tisztviselő akadályoztatva van (vagy nincsen kijelölve), úgy abban az esetben az Adatkezelő adatvédelmi vezetése felé kell, hogy teljesítse a beszámolási kötelezettségét. Az adatvédelmi kapcsolattartó az adatvédelmi tisztviselővel együttműködni köteles.

17. Minden Munkatárs felelős
    a) a jogszabályok, a jelen Szabályzat, és az adatvédelmi szabályozási dokumentáció más részeinek betartásáért és betartatásáért
    b) az általa kezelt személyes adatok integritásáért, sérthetetlenségéért, rendelkezésre állásáért,

c) a szándékos vagy gondatlan magatartásából fakadó adatvédelmi incidensekért, jogsértésekért.

18. Amennyiben adatkezeléssel összefüggő ügyben a vonatkozó jogszabályok és/vagy az Adatkezelő szabályzatainak rendelkezéseinek értelmezésével és/vagy alkalmazásával kapcsolatos kérdés merül fel, a Munkatárs iránymutatást kérhet az adatvédelmi tisztviselőtől (kapcsolattartótól), vagy végső soron az Adatkezelő adatvédelmi vezetésétől.

19. A Munkatárs, függetlenül pozíciójától, az adatkezelésre, adat- és titokvédelemre vonatkozó jogszabályi rendelkezések, továbbá mindenkor hatályos adatvédelmi szabályozási dokumentáció, így például az Adatvédelmi Szabályzat, egyéb adatvédelmi vagy más belső szabályzat, munkaköri leírás, intézményi utasítás, adatvédelmi oktatási anyag rendelkezéseinek megszegése esetén a magatartás, vagy mulasztás jellegétől függően
    a) büntetőjogi és/vagy
    b) polgári jogi és/vagy
    c) munkajogi felelősséggel tartozik.

2.5 Az érintett jogérvényesítésével kapcsolatos általános feladatok

1. Az Adatkezelő az érintettek joggyakorlásával, jogérvényesítésével kapcsolatos általános eljárása a következő:
    a) Az Adatkezelő indokolatlan késedelem nélkül, maximum az adott kérelem beérkezésétől számított 25 napon, törlés/elfeledtetés/tiltakozás esetében haladéktalanul, de legfeljebb 15 napon belül tájékoztatja az érintettet a kérelmében meghatározottakkal kapcsolatban megtett lépésekről, vagy arról, hogy milyen ténybeli vagy jogi ok alapján nem tesz eleget a kérelemnek, valamint az érintett jogairól és az érintett számára nyitva álló jogorvoslati lehetőségekről: a bírósághoz és a Nemzeti Adatvédelmi és Információszabadság Hatósághoz fordulás lehetőségéről.
    b) Az Adatkezelő az érintett tájékoztatását minden esetben írásban teszi meg az elszámoltathatóság elvének megvalósulása miatt, ezért szükség van az érintett postai vagy elektronikus címére.
    c) Az Adatkezelő írásban értesíti mindazokat a címzetteket, akikkel korábban az adatot közölte a kérelemben foglalt joggyakorlásról, amennyiben az szükséges, így ha a helyesbítés, törlés/elfeledtetés vagy adatkezelés-korlátozás jogával él az érintett.
    d) Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti, vagy ha a tájékoztatás lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel, vagy ha azt jogszabály kizárja.
    e) A fenti tájékoztatási és egyéb jogok érvényesítésével kapcsolatban felmerülő feladatokat
        a. az Adatkezelő kizárólag abban az esetben tudja időben ellátni, ha az a Munkatárs, aki az érintett kérelmét átvette (ideértve az e-mail-en történő átvételt is), az átvételt követően haladéktalanul értesíti arról a szervezeti egységvezetőt. Ha a szervezeti egységvezető az értesítést megkapta, vagy ha ő az átvevő, akkor haladéktalanul értesíteni köteles az adatvédelmi tisztviselőt (kapcsolattartót);
        b. az Adatkezelő adatvédelmi vezetése – az adatvédelmi tisztviselő (kapcsolattartó) javaslata alapján – a választ és a szükséges lépéseket kidolgozza, jóváhagyja és végrehajtja, végrehajttatja.
    f) A jogérvényesítéssel kapcsolatos konkrét feladatokat az adatvédelmi szabályozási dokumentáció más tagjai, elsősorban belső utasítások, részletesen meghatározzák.

2.6 Az adatvédelmi incidensekkel kapcsolatos általános feladatok

1. A Munkatársak kötelesek az Adatkezelő adatbiztonsággal kapcsolatos szabályait (utasításait) betartani és általánosságban minden ésszerű lépést megtenni azért, hogy az Adatkezelőt megóvják az adatvédelmi incidensektől.

2. Munkatárs, amennyiben észleli az adatvédelmi incidenst köteles a vonatkozó szabályzat (Lásd: Adatvédelmi Incidens Kezelési Szabályzat), és más, az adatvédelmi szabályozási dokumentációba tartozó szabályozó szerint eljárni.

3. Amennyiben attól kell tartani, hogy az incidensbe további számítástechnikai eszközök kerülnek be (pl. zsarolóvírus miatt), úgy az incidenssel érintett számítástechnikai eszközt előbb az elektromos és informatikai hálózatról leválasztani köteles és csak utána köteles megtenni a 2. pontban meghatározott feladatokat.

4. Az Adatkezelő adatvédelmi vezetése a jelzést haladéktalanul kivizsgálni köteles, bevonva az adatvédelmi tisztviselő (kapcsolattartó) segítségét, szükség esetén pedig külső (informatikai) szakember támogatását. Adatkezelő adatvédelmi vezetése a vonatkozó jogszabályokban, az adatvédelmi szabályozási dokumentáció egyes, releváns részeiben szabályzatban/utasításban meghatározott lépéseket végrehajtani, így – többek között – kárenyhítő, és további incidens bekövetkeztét megelőző lépéseket megtenni.

2.7 Adategyeztetéssel kapcsolatos általános feladatok

1. Adatkezelő a pontosság, naprakészség elvének érvényre juttatása miatt rendszeres időközönként adategyeztetést hajt végre a nyilvántartásában levő érintettek vonatkozásában.

2. Az Adatkezelő az adategyeztetések rendszerességét a jelen Szabályzattól formailag elkülönülő, az adatvédelmi szabályozási dokumentáció részét képező szabályozóban határozza meg. Amennyiben ez nem történik meg, úgy az Adatkezelő évente hajt végre adategyeztetést olyan (aktív) adatállományok (pl. ügyfelek, Munkatársak, Partnerek, Partnerek kapcsolattartói) vonatkozásában, amely adatállományok érintettek adatát, vagy adatait tartalmazzák. A már lezárt, passzív adatállományok (pl. bizonylatra felvitt adatok) vonatkozásában adategyeztetést az Adatkezelő nem hajt végre.

3. Adatkezelő egyes szervezeti egységei vonatkozásában különböző adategyeztetési határidőket határozhat meg.

4. Az adategyeztetést az Adatkezelő e-mail-ben, vagy ha e-mail cím nem áll rendelkezésre, úgy postai levélben hajtja végre.

5. Amennyiben az adategyeztetés sikeres, úgy Adatkezelő az új adatot (ha az értelmezhető) minden olyan adatállományba betáplálja, amelyben az eredeti adat is szerepelt, figyelemmel a pontosság, naprakészség, integritás, bizalmasság és elszámoltathatóság alapelveire.

6. Amennyiben az adategyeztetés sikertelen, úgy az adatot az Adatkezelő törli, megsemmisíti a nyilvántartásaiból, vagy ha a törlés az érintett jogait, érdekeit csorbítaná, zárolja a nem naprakész adatokat.

7. Az adategyeztetés feladatát a kijelölt Munkatárs köteles végrehajtani.

2.8 Az Adatkezelő adatvédelmi szervezetének oktatása

1. A Munkatársaknak éves jelleggel tartott adatvédelmi, adatbiztonsági képzésének biztosítása az Adatkezelő adatvédelmi vezetésének kötelezettsége. A képzést dokumentáltan kell megtartani a későbbi bizonyíthatóság miatt.

2. Adatkezelő vezetése az oktatással kapcsolatos feladatok (így pl. oktatási anyag összeállítása, jelenléti ívek és más dokumentumok létrehozása, oktatási napok meghatározása, meghívók kiküldése, az oktatás megtartása, stb.) elvégzésével Munkatársat, vagy az adatvédelmi tisztviselőt (kapcsolattartót) megbízhatja.

3. FEJEZET: A SZABÁLYZAT CÉLJA

1. A jelen Szabályzat elsődleges célja, hogy az Adatkezelővel kapcsolatba kerülő természetes személyek adatainak kezelésére vonatkozó alapvető elveket és rendelkezéseket meghatározza és betartsa annak érdekében, hogy a természetes személyek magánszférája és jogai védelemben részesüljenek a vonatkozó jogszabályi előírásoknak és hatósági állásfoglalásoknak megfelelően.

2. Hivatkozva a 3.1 pontban meghatározottakra, a jelen szabályzat célja annak biztosítása, hogy az Adatkezelő mindenben megfeleljen a hatályos jogszabályok adatvédelemmel kapcsolatos rendelkezéseinek, annak hatálya alatt és az azokban foglaltaknak megfelelően végezze a tevékenységét, amely különösen, azonban nem kizárólagosan az alábbiak:
   - az Európai Parlament és a Tanács (EU) 2016/679 Rendelete,
   - az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
   - 1993. évi III. törvény a szociális igazgatásról és szociális ellátásokról
   - 1/2000. (I. 7.) SzCsM rendelet a személyes gondoskodást nyújtó szociális intézmények szakmai feladatairól és működésük feltételeiről
   - 29/1993. (II.17.) Korm. Rendelet a személyes gondoskodást nyújtó szociális ellátások térítési díjáról
   - 9/1999. (XI.24.) SZCSM rendelet a személyes gondoskodást nyújtó szociális ellátások igénybevételéről
   - 8/2000. (VIII.4.) SZCSM rendelet a személyes gondoskodást végző személyek adatainak működési nyilvántartásáról
   - 9/2000. (VIII.4.) SZCSM rendelet a személyes gondoskodást végző személyek továbbképzéséről és a szociális szakvizsgáról
   - 321/2009. (XII.29.) Korm. Rendelet a szociális szolgáltatók és intézmények működésének engedélyezéséről és ellenőrzéséről
   - 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről
   - 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról
   - a munka törvénykönyve (2012. évi I. törvény)
   - egyéb, vonatkozó, törvénynél alacsonyabb szintű, adatvédelmi vonatkozású jogszabályok rendelkezéseinek.

3. Az Adatkezelő a működésre vonatkozó ágazati jogszabályok előírásait is betartja, így tehát Adatkezelő kiemelten fontosnak tartja, egyben elkötelezett az iránt, hogy az érintett adatait, és az érintetek jogait, az adatvédelem elveit és szabályait tiszteletben tartsa és betartsa.

4. FEJEZET: A JELEN SZABÁLYZAT HATÁLYA

1. Időbeli hatály: Lásd a Jelen Szabályzatot kiadó/módosító utasítás hatályát.

2. Személyi hatály: kiterjed
   - az Adatkezelőre, valamint
   - azokra a Partnerekre, akik a rendelkezések hatályát szerződésben vagy nyilatkozatban magukra nézve kötelezően elfogadták. Ha a Szabályzat szövegezéséből más nem következik, a Partnerek a Munkatársakra vonatkozó rendelkezések szerint kötelesek eljárni. A Szabályzat megismerése és betartása az Adatkezelő valamennyi Munkatársának munkaköri kötelessége.

3. Területi hatály: Jelen Szabályzat hatálya kiterjed az Adatkezelő tulajdonában, vagyonkezelésében, használatában, bérletében lévő ingatlanokra, ahol az Adatkezelő adatkezelést végez.

4. Tárgyi hatály: Jelen Szabályzat hatálya kiterjed az Adatkezelő minden szervezeti egységében folytatott valamennyi személyes adatokat tartalmazó adatkezelésre és adatra függetlenül attól, hogy az elektronikusan és/vagy papíralapon történik. Papír alapú adatkezelés esetében Adatkezelő a jelen szabályzattól formailag különálló iratkezelési szabályzatot léptet hatályba.

5. FEJEZET: AZ ÉRINTETT JOGAI ÉS JOGORVOSLATI LEHETŐSÉGEI

1. Jelen fejezet az érintettek személyes és különleges kategóriájú személyes adataival kapcsolatos jogairól és jogorvoslati lehetőségeiről rendelkezik.

2. Az érintett jogai és jogorvoslati lehetőségei a GDPR, és Infotv alapján az alábbiakban kerültek meghatározásra.

3. Az Adatkezelő felhívja a személyi hatálya alá tartozók figyelmét, hogy az érintett jogaival az **igazgato@gaszixv.hu e-mail címre küldött kérelmével, vagy Adatkezelő más elérhetőségén (lásd 2. fejezet) keresztül élhet.**

4. Személyes adatok védelméhez való jog az 1993. évi III. törvény alapján: Az 1993. évi III. törvény 94/E. § (5) bekezdés alapján az ellátást igénybe vevő érintettet megilleti személyes adatainak védelme, valamint a magánéletével kapcsolatos titokvédelem. Az igénybevételi eljárás során különös figyelmet kell fordítani arra, hogy az ellátást igénylő adataihoz csak az arra jogosult személyek férjenek hozzá. Az Intézményvezető köteles biztosítani továbbá, hogy az intézményi elhelyezés során az ellátott egészségi állapotával, személyes körülményeivel, jövedelmi viszonyaival kapcsolatos információkról más ellátást igénybe vevő, valamint arra illetéktelen személy ne szerezhessen tudomást, különös figyelemmel az ellátást igénybe vevő szociális rászorultságának tényére.

5. Az adatbiztonsági követelmények teljesülése és az érintett jogainak védelme érdekében az Adatkezelő kérelmet kézhez vevő Munkatársa köteles meggyőződni az érintett és a hozzáférési jogával élni kívánó személy személyazonosságának egyezéséről, joggyakorlás jogi és ténybeli lehetőségeiről, ennek érdekében a tájékoztatás, az adatokba történő betekintés, illetve azokról másolat kiadása is az érintett személyének azonosításához kötött. Ennek megfelelő a Munkatársak feladatait önálló belső utasítások rendezik minden jogérvényesítés kapcsán.

Előzetes tájékozódáshoz való jog

6. **Az előzetes tájékozódáshoz való jog**: az érintett jogosult arra, hogy az adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően tájékoztatást kapjon.

7. Az érintett e joga nem kérelméhez kapcsolódik, hanem alapvetően megilleti az érintettet, ezért az Adatkezelő külön kérelem nélkül is tájékoztatja az érintettet a következőkről:
   a. az Adatkezelő - ha valamely adatkezelési műveletet adatfeldolgozó végez, az adatfeldolgozó - megnevezése és elérhetőségei;
   b. az adatvédelmi tisztviselő elérhetőségei;
   c. a személyes adatok tervezett kezelésének célja;
   d. az adatkezelés jogalapja;
   e. adatkezelés időtartama;
   f. amennyiben jogos érdeken alapul az adatkezelés, úgy a jogos érdek mibenléte;
   g. a kezelt személyes adatok továbbítása vagy tervezett továbbítása esetén az adattovábbítás címzettjei;
   h. a kezelt személyes adatok gyűjtésének forrása;
   i. automatizált döntéshozatal ténye, ideértve a profilalkotást is (továbbá az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír), amennyiben Adatkezelő ilyet végez;
   j. az érintett személyes adatok kategóriái;
   k. az érintett azon jogáról, hogy kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról, GDPR 6. cikk (1) bekezdésének a) pontján vagy a 9. cikk (2) bekezdésének a) pontján alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való joga, továbbá a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;
   l. arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása.

8. Adatkezelő a tájékoztatást tipikusan, de nem kizárólagosan a következő módokon hajtja végre:
   a. a tájékoztatást az egyes adatkezelések tájékoztatóiban fogalmazza meg, amelyek megtalálhatóak a vonatkozó 2023/GÁSZI/GDPR sz. belső adatvédelmi utasításban, és amelyeket közzétesz székhelyén, az adatkezelés tényleges helyszínén (ha eltér a székhelytől) papír alapon, továbbá
   b. az egyes adatfelvételi űrlapokhoz tartozó adatkezelési tájékoztatást tartalmazó táblázatok és a vonatkozó adatkezelési tájékoztató tartalmazza az adatkezelési tudnivalókat, vagy a hivatkozást az adatkezelési tájékoztatóra,

c. minden aktuálisan végzett, külső érintett személyes adataira vonatkozó adatkezelési tájékoztatók összefoglaló táblázatait és az érdemi tényeket elektronikusan is elérhetővé tesz a weboldalon, sőt, amennyiben az átláthatóság, tisztességes eljárás elve, jogszerűség ezt megköveteli, önálló, részletes adatkezelési leírásokat is közzétesz,
d. az adatkezelési tájékoztatókat és egyébként a teljes adatvédelmi és adatbiztonsági szabályozási dokumentációt elérhetővé teszi a belső hálózatán, ahonnan azok letölthetőek, kinyomtathatóak,
e. megfelelő tájékoztatás található az esetleges hozzájáruló nyilatkozatokban,
f. közzétesz tájékoztató táblákat, amennyiben szükséges, akkor matricákat,
g. közzétesz közös adatkezelésre vonatkozó megállapodások lényegi részeit,
h. közzétesz érdekmérlegelési teszteket, vagyok azok kivonatát, hatásvizsgálatot, amennyiben ilyen eljárást végez annak összesítését papír alapon és amennyiben szükséges akkor elektronikusan.

9. Az előzetes tájékozódáshoz való joggal kapcsolatban a Munkatársak feladatait a vonatkozó belső utasítás tartalmazza.

Hozzáférés joga

10. **A „hozzáférés joga"**: Az Infotv és GDPR alapján az érintett jogosult arra, hogy kérelmére személyes adatait és az azok kezelésével összefüggő információkat az Adatkezelő a rendelkezésére bocsássa. A nevezett jogszabályok előírásai alapján az érintett kérelmére az Adatkezelő tájékoztatást ad
    a. az adatkezelés céljáról/céljairól,
    b. az általa kezelt adatokról és személyes adatok kategóriáiról,
    c. azon címzettek vagy címzettek kategóriáiról, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket (adatfeldolgozókról és adatközlés más címzettjeiről), továbbá tájékoztatást ad a továbbításra vonatkozóan a GDPR 46. cikk szerinti megfelelő garanciákról,
    d. az adatkezelés jogalapjáról, jogszerűségéről,
    e. az adatkezelés időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól,
    f. adott esetben ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információról,
    g. az érintettet az Infotv/GDPR alapján megillető jogokról, valamint azok érvényesítése módjáról,
    h. adott esetben az automatizált döntéshozatalról, ideértve a profilalkotást is, valamint a logikára és arra vonatkozó érthető információkról, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár,
    i. az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, ha az érintett ilyen incidens alanyává vált.

11. Az Adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri. Az érintett által kért további másolatokért az Adatkezelő az adminisztratív költségeken alapuló, ésszerű mértékű díjat számíthat fel.

12. Adatkezelő a tájékoztatást arányosan korlátozza, vagy megtagadja

    a. ha a tájékoztatás hátrányosan érinti mások jogait, szabadságait;
    b. ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusának rendelkezése alapján az Adatkezelő személyes adatot akként vesz át, hogy az adattovábbító adatkezelő az adattovábbítással egyidejűleg jelzi a személyes adat érintettje a nevezett törvényben biztosított jogainak korlátozását, vagy kezelésének egyéb korlátozását.
    c. az állam külső és belső biztonsága, így a honvédelem, a nemzetbiztonság, a bűncselekmények megelőzése vagy üldözése, a büntetés-végrehajtás biztonsága érdekében, továbbá állami vagy önkormányzati gazdasági vagy pénzügyi érdekből, az Európai Unió jelentős gazdasági vagy pénzügyi érdekéből, valamint a foglalkozások gyakorlásával összefüggő fegyelmi és etikai vétségek, a munkajogi és munkavédelmi kötelezettségszegések megelőzése és feltárása céljából - beleértve minden esetben az ellenőrzést és a felügyeletet is -, továbbá az érintett vagy mások jogainak védelme érdekében.
    d. az általa vagy részvételével végzett vizsgálatok vagy eljárások hatékony és eredményes lefolytatása érdekében.

13. Adatkezelő az elutasított hozzáférési kérelmekről a Nemzeti Adatvédelmi és Információszabadság Hatóságot évente értesíti, ha jogszabály alapján fennáll ilyen kötelezettsége.

14. A hozzáférési joggal összecseng a betekintéshez való jog: Az 1993. évi III. törvény 20. § és 20/C. §-a szerinti nyilvántartások vonatkozásában a betekintés jogát az 1993. évi III. törvény 22. §-a biztosítja az érintettek számára.

15. Az érintettnek, illetve képviselőjének joga van az egyes adatkezelések során keletkezett, az érintettre vonatkozó iratokba betekinteni. Az arra jogosult másolatot, kivonatot készíthet vagy másolatot kérhet.

16. Nem lehet betekinteni az olyan iratba, amely olyan adatokat tartalmaz, amelyre vonatkozóan az érintett az adatok zárt/korlátozott kezelését rendelte el.

17. A hozzáféréshez való joggal kapcsolatban a Munkatársak feladatait a **vonatkozó** belső utasítás tartalmazza.

A helyesbítés joga

18. A helyesbítés joga: Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését. Ez alapján az Adatkezelő, ha az általa kezelt személyes adatok pontatlanok, helytelenek vagy hiányosak, azokat az érintett kérelmére haladéktalanul pontosítja, helyesbíti, vagy kiegészíti. Ha a személyes adat a valóságnak nem felel meg, és a valóságnak megfelelő személyes adat az Adatkezelő rendelkezésére áll, a személyes adatot az Adatkezelő kötelezően helyesbíti, az érintett kérése nélkül is.

19. Adatkezelő mentesül a helyesbítés, pontosítás, kiegészítés kötelezettsége alól, ha

a. a pontos, helytálló, illetve hiánytalan személyes adatok nem állnak rendelkezésére és azokat az érintett sem bocsátja a rendelkezésére, vagy
b. az érintett által rendelkezésére bocsátott személyes adatok valódisága kétséget kizáróan nem állapítható meg.

20. Adatkezelő a helyesbítés megtörténtéről írásban tájékoztatja az érintettet, továbbá azt az adatfeldolgozót, aki a helyesbített adatot kezeli, valamint azt az adatkezelőt, aki felé az eredeti adatot továbbította.

21. Az 1993. évi III. törvény 20. § és 20/C. §-a szerinti nyilvántartások vonatkozásában a helyesbítés jogát az 1993. évi III. törvény 22. §-a biztosítja az érintettek számára.

22. A helyesbítéshez való joggal kapcsolatban a Munkatársak feladatait a vonatkozó belső utasítás tartalmazza.

A törléshez való jog

23. A törléshez való jog: az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, ha
    a. a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
    b. az érintett visszavonja a GDPR 6. cikk (1) bekezdésének a) pontja vagy a GDPR 9. cikk (2) bekezdésének a) pontja értelmében az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja. Az érintett kizárólag ezen jogalap esetében jogosult a korábban megadott hozzájárulást visszavonni, amely visszavonás a jövőre nézve szűnteti meg az ezen a jogalapon történő adatkezelést, amennyiben nincs a törlésnek egyéb akadálya. Ha az adatok kezelésének van más jogalapja a hozzájárulás visszavonására, vagy adatok törlésére vonatkozó érintetti kérelem esetén, valmaint a következő esetekben az Adatkezelő az adatokat nem törli:
        a) ha az adatok kezelését törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben, különleges kategóriájú személyes adatnak vagy bűnügyi személyes adatnak nem minősülő adat esetén - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli, vagy
        b) ha az adatkezelés 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
        c) ha az adatkezelés törvényben kihirdetett nemzetközi szerződés végrehajtásához feltétlenül szükséges és azzal arányos, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűncselekmények megelőzése, felderítése vagy üldözése érdekében vagy honvédelmi érdekből törvény elrendeli,
    c. az érintett a GDPR 21. cikk (1) bekezdése alapján tiltakozik az adatkezelés (közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges adatkezelés, vagy jogos érdekből történő adatkezelés) ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy
    d. az érintett a GDPR 21. cikk (2) bekezdése alapján, a közvetlen üzletszerzés érdekében történő adatkezelés ellen tiltakozik;
    e. a személyes adatokat jogellenesen kezelték;

az adatkezelés jogellenes, így *különösen*, ha az adatkezelés

1. az adatvédelem alapelveivel (lásd GDPR és Infotv) ellentétes,
2. célja megszűnt, vagy az adatok további kezelése már nem szükséges az adatkezelés céljának megvalósulásához,
3. törvényben, nemzetközi szerződésben vagy az Európai Unió kötelező jogi aktusában meghatározott időtartama eltelt, vagy
4. jogalapja megszűnt és az adatok kezelésének nincs másik jogalapja,

f. a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell, ideértve azt, ha az adatok törlését jogszabály, az Európai Unió jogi aktusa, a Hatóság vagy a bíróság elrendelte;

g. a személyes adatok gyűjtésére az EU 2016/679 Rendelet 8. cikk (1) bekezdésében említett, közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

24. Adatkezelő felhívja az érintettek figyelmét a törléshez való jog GDPR-ból fakadó korlátaira, amelyek a következők:
    a. a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása;
    b. a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása;
    c. népegészségügy területét érintő közérdek;
    d. az EU 2016/679 Rendelet 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben a törléshez való jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést; vagy
    e. jogi igények előterjesztése, érvényesítése, illetve védelme.

25. Az érintetti kérelemre induló törlés kapcsán a Munkatársak feladatait vonatkozó belső utasítás tartalmazza.

26. Az Infotv alapján, a törléshez való jog érvényesítése érdekében az Adatkezelő, érintetti kérelem nélkül is, haladéktalanul törli az érintett személyes adatait, ha
    a. az adatkezelés jogellenes,
        az adatkezelés jogellenes *különösen*, ha az adatkezelés
        1. az adatvédelem alapelveivel (lásd GDPR és Infotv) ellentétes,
        2. célja megszűnt, vagy az adatok további kezelése már nem szükséges az adatkezelés céljának megvalósulásához,
        3. törvényben, nemzetközi szerződésben vagy az Európai Unió kötelező jogi aktusában meghatározott időtartama eltelt, vagy
        4. jogalapja megszűnt és az adatok kezelésének nincs másik jogalapja,
    b. az adatkezelés az Infotv 4. §-ban rögzített alapelvekkel ellentétes,
    c. az adatkezelés célja megszűnt, vagy az adatok további kezelése már nem szükséges az adatkezelés céljának megvalósulásához,
    d. törvényben, nemzetközi szerződésben vagy az Európai Unió kötelező jogi aktusában meghatározott időtartama eltelt, vagy
    e. jogalapja megszűnt és az adatok kezelésének nincs másik jogalapja.
    f. az adatok törlését jogszabály, az Európai Unió jogi aktusa, a Hatóság vagy a bíróság elrendelte, vagy
    g. az Infotv 19. § (1) bekezdés b)-d) pontjában meghatározott időtartam eltelt.

27. Nem érintetti kérelemre induló törlés kapcsán a Munkatársak feladatait a **vonatkozó** belső utasítás tartalmazza.

Az elfeledtetéshez való jog

Elfeledtetéshez való jog: abban az esetben, ha az Adatkezelő valamely okból nyilvánosságra hozta a személyes adatot, és azt a fentiek értelmében törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az ésszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő más adatkezelőket, hogy az érintett kérelmezte a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

Magyarázat: az interneten megvalósuló adatkezelések kapcsán nem elegendő a törléshez való jogot biztosítani, hiszen az adatok nem csak egy adatkezelőnél rögzülnek, hanem sok más adathordozón is, ezentúl a keresőmotorok a korábban tárolt verziókat is elérhetővé teszik. Az általános adatvédelmi rendelet szabályai értelmében az internet sajátosságaira tekintettel azt is lehetővé kell tenni, hogy az érintett az adatok minden lehetséges elérési pontján töröltethesse azokat, hiszen csak ez vezet el a tényleges joggyakorláshoz.

Az elfeledtetés jogával kapcsolatosan kifejezetten kérjük az érintetteteket, hogy amennyiben az intézményben használnak keresőmotor jellegű, illetve egyéb platform szolgáltatást, akkor a beállítások során szíveskedjenek megtenni a szükséges intézkedéseket a saját személyes adataik védelme érdekében.

Magyarázat: egy érintett igénybe veszi az álláskeresése során az ingyenes internet elérhetőséget, akkor törölje a keresési előzményeket.

Az elfeledtetés jogával kapcsolatban a Munkatársak feladatait a vonatkozó belső utasítás tartalmazza.

Hozzájárulás visszavonásának joga

1. Az érintett jogosult arra, hogy bármely hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét, tehát a visszavonás kizárólag a jövőre vonatkozik, visszaható hatálya nincsen.

2.Az Adatkezelő a hozzájárulás visszavonása esetén az érintettet törli az adott adatkezeléshez kapcsolódó adatállományból (ha az egyéb feltételek fennállnak). Ennek megfelelően a Munkatársak feladatait a törlésre vonatkozó belső utasítás tartalmazza.

3. Magát a hozzájáruló nyilatkozatot az Adatkezelő a visszavonástól számított általános elévülési időben kezeli (tárolja, zárolja) a későbbi bizonyíthatóság, így az elszámoltathatóság elvének teljesítése miatt.

Adatkezelés korlátozásához/zárolásához való jog

4. **Az adatkezelés korlátozásához, vagy más néven zároláshoz való jog**: Az érintett jogosult arra, hogy kérésére az Adatkezelő korlátozza az adatkezelést, az adatokhoz történő hozzáférést, ha valamelyik feltétel fennáll:

a. ha az érintett vitatja az Adatkezelő, illetve az adatfeldolgozó által kezelt személyes adatok pontosságát, helytállóságát vagy hiánytalanságát, és a kezelt személyes adatok pontossága, helytállósága vagy hiánytalansága kétséget kizáróan nem állapítható meg, a fennálló kétség tisztázásának időtartamára,
b. az adatkezelés jogellenes (lásd az Infotv 20. § a) pontjában meghatározottakat), és az érintett ellenzi az adatok törlését, és e helyett kéri azok felhasználásának korlátozását;
c. az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
d. az érintett a GDPR 21. cikk (1) bekezdése szerint tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.
e. ha az adatok törlésének lenne helye, de az érintett írásbeli nyilatkozata vagy az Adatkezelő rendelkezésére álló információk alapján megalapozottan feltételezhető, hogy az adatok törlése sértené az érintett jogos érdekeit, a törlés mellőzését megalapozó jogos érdek fennállásának időtartamára,
f. ha az Infotv 20. § a) pontjában meghatározottak szerint (tehát jogellenes adatkezelés miatt) az adatok törlésének lenne helye, de az adatkezelő vagy más közfeladatot ellátó szerv által vagy részvételével végzett, jogszabályban meghatározott vizsgálatok vagy eljárások során az adatok bizonyítékként való megőrzése szükséges, ezen vizsgálat vagy eljárás végleges, illetve jogerős lezárásáig,
g. ha az Infotv 20. § a) pontjában meghatározottak szerint (tehát jogellenes adatkezelés miatt) az adatok törlésének lenne helye, de az Infotv 12. § (2) bekezdésében foglalt dokumentációs kötelezettség teljesítése céljából (nemzetközi adattovábbítás speciális esetei miatt) az adatok megőrzése szükséges, a 25/F. § (4) bekezdésben meghatározott időpontig (10 évig).

5. **Adatkezelő indokolatlan késedelem nélkül, maximum a kérelem beérkezésétől számított 15 (tizenöt) napon belül tájékoztatja az érintettet a kérelmében meghatározottakról, és/vagy korlátozza (zárolja) az adatokat, vagy tesz meg egyéb lépéseket a kérelemnek megfelelően, ha nincsen azt kizáró ok.**

6. A zárolás/korlátozás jogával kapcsolatban a Munkatársak feladatait a vonatkozó belső utasítás tartalmazza.

Az adathordozhatóság joga

1. Az **„adathordozhatósághoz való jog"**: Az érintett jogosult arra, hogy
   a. a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy
   b. ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha:
      a) az adatkezelés hozzájáruláson alapul; **és**
      b) az adatkezelés automatizált módon történik.

2.Az adatok hordozhatóságához való jog gyakorlása során az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

3. A jog gyakorlása nem sértheti a törléshez való jogot. Az említett jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges. A jog gyakorlása nem érintheti hátrányosan mások jogait és szabadságait.

4.Az adathordozhatóság jogával kapcsolatban a Munkatársak feladatait a **vonatkozó** belső utasítás tartalmazza.

A tiltakozáshoz való jog

1. A **tiltakozáshoz való jog**: Az érintett tiltakozhat személyes adatának kezelése ellen, a következő esetekben:

   a. ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, ideértve a profilalkotást is;
   b. ha az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, ideértve a profilalkotást is;
   c. személyes adatok kezelése közvetlen üzletszerzés érdekében történik, ideértve a profilalkotást is.
   d. ha a személyes adatok kezelésére a GDPR 89. cikk (1) bekezdésének megfelelően tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozhasson a rá vonatkozó személyes adatok kezelése ellen, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.

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

3. A tiltakozás jogával kapcsolatban a Munkatársak feladatait a vonatkozó belső utasítás tartalmazza.

Panasztétel joga

Panasztétel joga: amennyiben érintett az adatkezelés végrehajtását sérelmezi, azt az Adatkezelő, ha más jogérvényesítéssel a kérelmet nem lehet azonosítani, panaszként kezeli.

A panasztétel jogával kapcsolatban a Munkatársak feladatait a vonatkozó belső utasítás tartalmazza.

Amennyiben az érintett az Adatkezelő bármelyik döntésével nem ért egyet, vagy az Adatkezelő a hivatkozott határidőt elmulasztja, jogosult a felügyeleti hatósághoz – Nemzeti Adatvédelmi és Információszabadság Hatóság (székhely: 1055 Budapest, Falk Miksa utca 9-11.; postacím: 1363 Budapest, Pf. 9.; telefon: +36 (1) 391-1400; e-mail: ugyfelszolgalat@naih.hu; honlap: www.naih.hu) – fordulni a hatóság által meghatározott feltételek betartásával.

Bírósági jogérvényesítés joga

Bírósági jogérvényesítés: Az érintett a jogainak megsértése esetén bírósághoz fordulhat. A bíróság az ügyben soron kívül jár el. Azt, hogy az adatkezelés a jogszabályban foglaltaknak megfelel, az Adatkezelő köteles bizonyítani.

Kártérítésre és sérelemdíjra vonatkozó törvényi szabályok: Abban az esetben, ha az Adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével az érintett személyiségi jogát megsérti, az érintett az Adatkezelőtől sérelemdíjat követelhet.

Abban az esetben, ha Adatkezelő adatfeldolgozót vett igénybe, az érintettel szemben az Adatkezelő és az adatfeldolgozó a GDPR-ban meghatározott előírások megsértésével okozott kárért egyetemlegesen felelnek, továbbá a személyiségi jogsértés esetén járó sérelemdíjat egyetemlegesen kötelesek megfizetni az érintettnek.

Nem kell megtéríteni a kárt és nem követelhető a sérelemdíj annyiban, amennyiben a kár a károsult vagy a személyiségi jog megsértésével okozott jogsérelem az érintett szándékos vagy súlyosan gondatlan magatartásából származott.

6. FEJEZET: AZ ADATKEZELÉS ALAPELVEI

1. Jelen Szabályzat rendelkezése, valamint az Adatkezelő gyakorlata nem lehet ellentétes az adatkezelési elvekkel.

2. A Szabályzat a következő adatkezelési elveket vezeti be hatályba lépése napjától, amely elvek kötelező rendelkezések és iránymutatásul szolgálnak olyan kérdésekben, amelyeket a Szabályzat, vagy a belső adatvédelmi szabályozási dokumentációba tartozó dokumentum nem tárgyal.

A célhoz kötöttség elve

„Célhoz kötöttség" elve: (GDPR 5. cikk (1) b) pontja, Infotv 4. § (1)-(3) bek.) Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának. A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű cél(ok)ból történhet, és adatok nem kezelhetőek az eredeti céllal/célokkal össze nem egyeztethető módon. Nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.

Az elv megvalósulásával kapcsolatban a Munkatársak tipikus feladatait a **vonatkozó** sz. belső utasítás tartalmazza.

Jogszerűség, tisztességes eljárás és átláthatóság elve

„Jogszerűség, tisztességes eljárás és átláthatóság" elve: (GDPR 5. cikk (1) a), Infotv 4. § (1) és (5) bek.) Személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni, az adatok gyűjtésének és kezelésének tisztességesnek és törvényesnek kell lennie.

Az elvek megvalósulásával kapcsolatban a Munkatársak tipikus feladatait a **vonatkozó** belső utasítás tartalmazza.

Arányosság, szükségesség elve

„Arányosság, szükségesség, adatminimalizálás vagy adattakarékosság" elve: (GDPR 5. cikk (1) c) pontja, Infotv 4. § (2) bek.) Az adatoknak az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk. Máshogyan megfogalmazva csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. Az érintettet csak az adatkezelés céljához szükséges ideig lehet azonosítani. Mindezeknek megfelelően Adatkezelő csak és kizárólag olyan adatot kezel és annyi ideig, amely feltétlenül szükséges. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az Adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

Az elv megvalósulásával kapcsolatban a Munkatársak tipikus feladatait a **vonatkozó** belső utasítás tartalmazza.

Pontosság, naprakészség elve

„Pontosság, naprakészség" elve: (GDPR 5. cikk (1) d) pontja, Infotv 4. § (4) bek.) A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; Adatkezelőnek minden észszerű intézkedést meg kell tennie annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

Az elv megvalósulásával kapcsolatban a Munkatársak tipikus feladatait a **vonatkozó** belső utasítás tartalmazza.

Korlátozott tárolhatóság elve

„Korlátozott tárolhatóság" elve: (GDPR 5. cikk (1) e) pontja, Infotv 4. § (2) bek. második fordulata) A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a GDPR 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, a GDPR-ban az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is tekintettel.

A korlátozott tárolhatóság alól kivételként az az eset értelmezhető, amikor az adatok maradandó értékű iratokon szereplő adatok. Maradandó értékű iratnak minősülő dokumentum esetében az irat és így adat nem leselejtezhető, nem törölhető, nem semmisíthető meg. Maradandó értékű irattá minősítést az Adatkezelő adatvédelmi vezetése határozza el, figyelemmel jogszabályi előírásokról és a működésére.

Az elv megvalósulásával kapcsolatban a Munkatársak tipikus feladatait a vonatkozó belső utasítás tartalmazza.

Integritás és bizalmasság elve

„Integritás és bizalmasság" elve: (5. cikk (1) f) pontja, Infotv 4. § (4a) bek.) Személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

Az elv megvalósulásával kapcsolatban a Munkatársak tipikus feladatait a vonatkozó belső utasítás tartalmazza.

Elszámoltathatóság elve

„Elszámoltathatóság" elve: (GDPR 5. cikk (2) bek.) Az Adatkezelő felelős az alapelveknek és a Szabályzatban meghatározottaknak való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

Az elv megvalósulásával kapcsolatban a Munkatársak tipikus feladatait a vonatkozó belső utasítás tartalmazza.

Beépített és alapértelmezett adatvédelem gondolatisága

„Beépített és alapértelmezett adatvédelem" gondolatisága: nagyon tudatos adatvédelmi gondolkodásmód, amely nagyon röviden összefoglalva azt jelenti, hogy az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során az Adatkezelő megfelelő technikai és szervezési intézkedéseket – például álnevesítést – hajt végre a fenti elvek hatékony megvalósítása, a kötelezettségek teljesítése, jogi garanciák beépítése, stb. céljával, mindezeket pedig szabályozottan és részletesen dokumentáltan teszi meg. Az Adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

A gondolkodásmód implementálásával kapcsolatban a Munkatársak tipikus feladatait a vonatkozó belső utasítás tartalmazza.

7. FEJEZET: ADATKEZELÉS BEVEZETÉSÉVEL, VÉGZÉSÉVEL ÉS MEGSZÜNTETÉSÉVEL KAPCSOLATOS FELADATOK

1. Az adatkezelés bevezetése, módosítása, megszüntetése során a vonatkozó belső szabályokat, utasításokat e fejezet rendelkezéseivel együtt kell alkalmazni.

2. Adatkezelő adatvédelmi vezetése a végezni tervezett adatkezelés tervezetében
   a. meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés várható időtartamát, az adatkezelés egyéb feltételeit;

b. az előző pontban meghatározott feladat részeként javaslatot kér az adatvédelmi tisztviselőtől (kapcsolattartótól), hogy a végezni tervezett, esetleg eltérő célú adatkezelés összeegyeztethető-e az eredeti céllal, és az eredeti cél szerinti jogalap szolgálhat-e a tervezett adatkezelés új jogalapjául [GDPR 6. cikk (4) bek.];
c. amennyiben az adatkezelés jogalapja kérdéses, felkéri az adatvédelmi tisztviselőt, hogy működjön közre a GDPR 6. cikk (1) bekezdés e) pontja szerinti jogalap és a GDPR 6. cikk (3) bekezdése szerinti tagállami jogi alap azonosításában, illetve jogszabályi kötelezettség esetén a GDPR 6. cikk (1) bekezdés c) pontja szerinti jogalap alátámasztásában;
d. felkéri az adatvédelmi tisztviselőt (kapcsolattartót), hogy működjön közre a hatásvizsgálat tervezetének létrehozásában, amennyiben megítélése szerint hatásvizsgálat elkészítése szükséges,
e. felkéri az adatvédelmi tisztviselőt (kapcsolattartót), hogy vizsgálja meg azt a kérdést, hogy az adatkezelést közös adatkezelésként indokolt-e ellátni, illetve indokolt-e adatfeldolgozót bevonni; valamint automatizált döntéshozatali módszer, illetve profilalkotási módszer alkalmazására [GDPR 22. cikk (1) bek.], és ha szükséges azt, hogy a személyes adatok harmadik országba továbbíthatók-e ;
f. felkéri az adatvédelmi tisztviselőt (kapcsolattartót), hogy nézze át a hozzájáruló nyilatkozat tervezetét [GDPR 7. cikk (2) bek.], illetve a megfelelő szerződéses rendelkezések tervezetét, amennyiben a hozzájárulás a jogalap;
g. felkéri az adatvédelmi tisztviselőt (kapcsolattartót), hogy nézze át az adatkezelésről szóló tájékoztatás tervezetét (GDPR 13-14. cikk).

3. A fentieken túl az Adatkezelő adatvédelmi vezetése által meghatározott tervezetnek tartalmaznia kell a következő iránymutatásokat:
   a. az adatok felvételének, módosításának, törlésének rendje,
   b. adatszolgáltatási kötelezettségek meghatározása az adatok naprakészen tartása érdekében,
   c. a nyilvántartási rendszerből történő adattovábbítás, az ahhoz való hozzáférés rendje;
   d. az adatkezelésre vonatkozó különös adatbiztonsági intézkedések meghatározása;
   e. GDPR-nak, az Infotv-nek és egyéb alkalmazandó jogszabálynak megfelelő adatkezelési tájékoztató,
   f. hozzájáruláson alapuló adatkezelés esetén a hozzájáruló nyilatkozat mintája.

4. Fentiek alapján az adatvédelmi tisztviselőt (kapcsolattartót) az új adatkezelés bevezetésére vonatkozó igény megfogalmazásától kezdve be kell vonni az adatkezelés feltételeinek kidolgozása folyamatába.

5. Amennyiben az új adatkezelés bevezetése több szervezeti egységet érint, úgy valamennyi érintett egység vezetőjét (ha van, kapcsolattartót) és az adatvédelmi tisztviselőt be kell vonni az adatkezelés feltételei (döntés szerinti iránymutatások) részletes kidolgozásának folyamatába.

6. Az adatkezelés feltételeinek részletes kidolgozásában érintett szervezeti egységek vezetői kötelesek egymással és az adatvédelmi tisztviselővel (kapcsolattartóval), valamint az Adatkezelő adatvédelmi vezetésével együttműködni.

7. A feltételek és egyebek kidolgozását követően azokat az Adatkezelő adatvédelmi vezetése elé kell terjeszteni, aki meghozza az adatkezelés bevezetéséről szóló döntését.

8. Adatkezelés bevezetése minden esetben az Adatkezelő adatvédelmi vezetésének döntése alapján történik.

Feladatok az adatkezelés bevezetésével kapcsolatban

1.Az Adatvédelmi kapcsolattartó, amennyiben kijelölésre került, illetve az Adatkezelő

a. az adatkezelés bevezetéséről szóló döntést és az arról szóló tájékoztatást követően az adatkezelést bevezeti a vonatkozó adatkezelési tevékenységek nyilvántartásába (adatkezelői nyilvántartásba)
b. gondoskodik és közreműködik
    a) a célhoz kötött adatkezelés és az adattakarékosság elvének megfelelően gyűjtött adatokra vonatkozóan a beépített és alapértelmezett adatvédelem elveinek dokumentált érvényesüléséről;
    b) annak biztosításában, hogy az adathordozhatóság, adattörlés és adattisztítás célú módosítások szabályozott és dokumentált módon valósuljanak meg;
    c) annak biztosításában, hogy az adatvédelmi tájékoztatók és nyilatkozatok könnyen elérhetők legyenek az érintettek számára,
    d) annak biztosításában, hogy az adatkezeléssel kapcsolatos érintetti rendelkezéseket visszakereshető formában tárolják.

2. Az Adatkezelő adatvédelmi vezetése tájékoztatja az adatvédelmi tisztviselőt az adatvédelmi kapcsolattartón keresztül, amennyiben ez a pozíció betöltetlen, úgy a feladatokat vagy e feladattal megbízott Munkatárs hajtja végre, vagy maga az intézmény adatvédelmi vezetése.

3.Amennyiben az adatkezelés feltételei kidolgozásában részt vevők között véleményeltérés van, az adatvédelmi tisztviselő (vagy kapcsolattartó) javaslatot tesz a lehetséges megoldásra, amelyről az Adatkezelő adatvédelmi vezetése dönt.

4.Az adatvédelmi tisztviselő (kapcsolattartó) véleményét az adatkezelés bevezetéséről való döntést kezdeményező előterjesztésben ismertetni kell. Az adatvédelmi tisztviselő véleményétől való eltérést az előterjesztésben részletesen meg kell indokolni.

Feladatok az adatkezelés során

1.Az adatkezelés során az adatvédelmi tisztviselő (kapcsolattartó):

a. figyelemmel kíséri az adatkezelés feltételeinek folyamatos fennállását (beleértve az adatkezelés jogszerűségéhez szükséges tájékoztatások megadását, nyilatkozatok beszerzését stb.) és
b. szükség esetén kezdeményezi a szükséges intézkedéseket az adatkezelés feltételeinek módosítása iránt;
c. amennyiben az adatkezelés hozzájáruláson alapul, ellenőrzi, hogy az érintett a hozzájárulását szabályosan szerezték-e be [GDPR 7. cikk (1) bek.], azokat hogyan tárolják, kezelik;
d. amennyiben az adatkezelés jogos érdeken alapul, gondoskodik arról, hogy legalább az érintettel való első kapcsolatfelvételkor felhívják az érintett figyelmét a tiltakozási jogra, és hogy az erről szóló tájékoztatást egyértelműen és más információtól elkülönítve jelenítsék meg [GDPR 21. cikk (4) bek.];

e. közreműködik az érdekmérlegelési tesztek és adatvédelmi hatásvizsgálatok utóellenőrzésben, felülvizsgálatában [GDPR 35. cikk (11) bek.]
f. a hozzá érkezett kérdéseket, kéréseket, panaszokat kivizsgálja és
g. őrködik az adatkezelés jogszerűsége és más alapelvek betartása felett, beleértve azt, hogy szükség esetén javasolja az adatkezelés (azonnali hatályú) felfüggesztését, megszüntetését, módosítását az Adatkezelő adatvédelmi vezetése számára.

Feladatok az adatkezelés megszüntetésével kapcsolatban

a. Adatkezelés megszüntetéséről szóló döntés estén az adatvédelmi tisztviselő (kapcsolattartó) javaslatot tesz az Adatkezelő adatvédelmi vezetése számára a törlés/megsemmisítés módjára, idejére, az adatok esetleges archiválására meghatározott ideig, az adatkezelési tevékenységek (adatkezelői) nyilvántartásból történő törlésre.
b. Adatkezelő döntést hoz az adatkezelés megszüntetéséről.

Az érdekmérlegelési teszt elvégzésének módszertana

Az Adatkezelő közfeladatot ellátó szerv, ezért a közfeladatai ellátása körében végzett adatkezelésre a GDPR 6. cikk (1) bekezdés f) pontja szerinti jogos érdek jogalapot nem alkalmazza [GDPR 6. cikk (1) bekezdés második albekezdés]. Ennek megfelelően az Adatkezelő e körben érdekmérlegelési tesztet nem készít. A helyes jogalap a GDPR 6. cikk (1) bekezdés e) pontja, a GDPR 6. cikk (3) bekezdése szerinti tagállami jogi alap – így különösen a szociális igazgatásról és szociális ellátásokról szóló 1993. évi III. törvény, a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény és ezek végrehajtási rendeletei – megjelölésével; jogszabályi kötelezettség teljesítése esetén a GDPR 6. cikk (1) bekezdés c) pontja a konkrét jogszabályhely megjelölésével.

Az adatkezelés jogalapjának, valamint a GDPR 6. cikk (3) bekezdése szerinti tagállami jogi alapnak (a felhatalmazó vagy elrendelő jogszabályhelynek) az azonosítását az e feladattal megbízott Munkatárs/Partner készíti elő, és küldi meg az adatvédelmi tisztviselő, valamint az Adatkezelő adatvédelmi vezetése számára. Az adatkezelés kizárólag a jogalap és a felhatalmazó jogszabályi rendelkezés írásbeli rögzítését követően kezdhető meg.

Az adatvédelmi hatásvizsgálat elvégzésének módszertana

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

Adatvédelmi hatásvizsgálatot a GDPR 35. cikk (3) bekezdésében, illetve a Nemzeti Adatvédelmi és Információszabadság Hatóság honlapján (www.naih.hu) közzétett, mindenkori hatásvizsgálati jegyzékben szereplő adatkezelések, adatkezelési műveletek esetén kell végezni.

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

A hatásvizsgálat módszertanát minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani. Egy lehetséges módszertant alkalmazó szoftver a Nemzeti Adatvédelmi és Információszabadság Hatóság honlapján (www.naih.hu) érhető el.

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

8. FEJEZET:
ADATKEZELÉSEK JOGALAPJAI, JOGSZERŰSÉGE ÁLTALÁNOSSÁGBAN

1. Az Adatkezelő minden esetben tájékoztatja az érintetteket az adatkezelés jogalapjáról a szabályozási dokumentáció egyes részeiben, így többek között a vonatkozó 2023/GÁSZI/GDPR sz. utasítás mellékleteiben (adatkezelési tájékoztatókban), hozzájáruló nyilatkozatokban, vagy más tájékoztatóban, stb.

2. Összhangban az adatkezelések céljaival, a személyes adatok kezelése akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül (GDPR 6. cikk):

    a. az érintett előzetes és önkéntes hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
    b. az adatkezelés jogszerű, ha 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 jogszerű, ha az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
    d. az adatkezelés akkor is jogszerű, ha az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
    e. ***az adatkezelés jogszerű, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;***
    f. az adatkezelés jogszerű, ha 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.

3. Összhangban az adatkezelések céljaival, a különleges kategóriájú személyes adatok kezelése akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül (GDPR 9. cikk)
    a. az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha az érintett hozzájárulásával nem élhet;
    b. ***az adatkezelés az Adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi;***

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

d. az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott és az az adatkezelés céljának megvalósulásához szükséges és azzal arányos;

e. *az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el;*

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

g. *az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a közalkalmazott munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, továbbá a GDPR 9. cikk (3) bekezdésben említett feltételekre és garanciákra figyelemmel;*

h. az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechnikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan;

i. *az adatkezelés a GDPR 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.*

3. A hozzájárulás kizárólag akkor tekinthető jog szerint elfogadhatónak, ha mindhárom tartalmi követelményt, tehát
   a. az önkéntességet,
   b. a határozottságot (egyértelműséget) és
   c. megfelelő tájékozottságon alapulóságot is teljesíti.

4. Az érintett önkéntes, kifejezett adatszolgáltatása esetén az Adatkezelő a személyes adatot az érintett beleegyezésével kezeli.

5. Az önkéntességnek minden esetben aktív magatartással kell megvalósulnia.

6. Az Adatkezelőnek kell bizonyítania, hogy az adatkezelési művelethez az érintett hozzájárult, ezért az Adatkezelő a hozzájárulást írásban, vagy elektronikus úton veszi fel és tárolja el.

7. Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel.

8. Az érintett jogosult arra, hogy a korábban adott esetleges hozzájárulását bármikor visszavonja. Ebben az esetben a vonatkozó belső utasításnak megfelelően kell eljárni.

Például: az érintett kérheti hírlevélről történő törlését.

9. Az Adatkezelő a hozzájárulás visszavonása esetén az érintettet törli az adott adatkezeléshez kapcsolódó adatállományból (ha az egyéb feltételek fennállnak). Magát a hozzájáruló nyilatkozatot az Adatkezelő a visszavonástól számított általános elévülési időben kezeli (tárolja) a későbbi bizonyíthatóság, így az elszámoltathatóság elvének teljesítése miatt.

10. A GDPR 6. cikk (1) b) pontjában rögzített esetben hangsúlyos az, hogy a szerződés az érintett és az Adatkezelő között jöjjön létre, vagy ilyen szerződés megkötéséhez szükséges lépésekről legyen szó. Amennyiben a szerződés az érintett által képviselt szervezet és az Adatkezelő között jön létre, úgy az érintett (mint képviselő, kapcsolattartó) adatait az Adatkezelő a közfeladatának ellátásához, illetve a szerződés teljesítéséhez szükséges mértékben, a GDPR 6. cikk (1) bekezdés e) pontja alapján kezeli.

11. Kötelező adatkezelés esetén, ha az érintett az adatszolgáltatást elmulasztja, akkor az Adatkezelő a szolgáltatást/adatkezelést köteles megtagadni számára.

11. Kötelező adatkezelés kapcsán előfordulhatnak olyan dokumentációk, iratok, amelyek személyes adatokat tartalmaznak, és jogszabály meghatározza a formátumot is, amelyben kell ezeket vezetni, és vannak olyan dokumentációk, amelyeket vezetni kötelező, de nincsen formai megkötés.

12. Abban az esetben, ha az adatkezelés az Adatkezelő közfeladatának ellátásához szükséges, úgy Adatkezelő a GDPR 6. cikk (1) bekezdés e) pontját és az adatkezelést elrendelő, illetve felhatalmazó jogszabályi rendelkezést jelöli meg jogalapként.

9. FEJEZET:
AZ ADATKEZELÉS IDŐTARTAMA ÁLTALÁNOSSÁGBAN

1. Az adatkezelés időtartama minden adatkezelési tevékenység esetében meghatározásra került az adatkezelés leírásában, azonban ha az valamilyen hiba, hiányosság miatt nem alkalmazható, úgy a következő szabályokat kell alkalmazni:
    a. a cél megvalósulásáig és a személyes adatainak törléséig, vagy
    b. adatainak kezelésére vonatkozó engedélye visszavonásáig, vagy adatainak kezelési igényének visszavonásáig, és így személyes adatainak törléséig,
    c. jogszabályban meghatározott határidő lejártáig,

d. bíróság vagy hatóság törlésre vonatkozó döntésének végrehajtásáig,
e. a közfeladat ellátásához, illetve a jogszabályi kötelezettség teljesítéséhez szükséges idő elteltéig,
f. jogi igény érvényesíthetőségéig tart (A hatályos Ptk. 6:22 § alapján az általános elévülési idő 5 év).

2. Az 1993. évi III. törvény 20. § (1) bekezdése szerinti nyilvántartásból a szociális ellátásra való jogosultság megszűnésétől számított 5 (öt) év elteltével törölni kell az adott személyre vonatkozó adatokat.

3. Az 1993. évi III. törvény 20/C. § szerinti nyilvántartásokból („KENYSZI"), amely segítségével a Kincstár felé az Adatkezelő kötelezően adatokat továbbít, szociális ellátásra való jogosultság megszűnésétől számított öt év elteltével törölni kell az adott személyre vonatkozó adatokat.

4. Jogszabályon alapuló kötelező adatkezelés esetén, a vonatkozó törvény, vagy önkormányzati rendelet állapítja meg az adatkezelés időtartamát. Ha a kötelező adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény, helyi önkormányzat rendelete vagy az Európai Unió kötelező jogi aktusa nem határozza meg, úgy Adatkezelő a **vonatkozó** belső utasításnak megfelelően jár el.

10. FEJEZET:
ADATKÖZLÉS (ÁTADÁS, TOVÁBBÍTÁS, MEGOSZTÁS)

Adatmegosztás Adatkezelő szervezetén belül

1. Adatok Adatkezelőn belül történő megosztás kizárólag úgy történhet, ha a megosztani kívánt adat(ok)hoz a címzett Munkatársnak is van hozzáférési jogosultsága és a Munkatárs feladatainak ellátáshoz szükséges az adat.

2. A Munkatárs a megosztást megelőzően köteles beszerezni a címzett Munkatárs hozzáférési jogosultságával kapcsolatos információkat.

Adattovábbítás az Adatkezelőtől eltérő harmadik fél felé

1. Adatkezelő a Budapest Főváros XV. Kerületi Önkormányzat, mint fenntartó felé a mindenkor hatályos munkamegosztási szerződés alapján továbbíthat személyes adatokat, a Munkatársak feladatvégzésével. Ezen túlmenően is történhet adattovábbítás például a Magyar Államkincstár, hatóság, bíróság számára megkeresés esetén. Az adatkezelő minden esetben a mindenkor hatályos jogszabályi előírásonak, szakmai protokollnak, iránymutatásoknak, állásfoglalásoknak, vonatkozó szabályzatoknak megfelelően jár el az adatkezelések során.

2. Az adattovábbítást megelőzően a feladattal megbízott Munkatárs megvizsgálja a továbbítandó személyes adatok pontosságát, teljességét és naprakészségét, szükség esetén adategyeztetést hajt végre.

3. Személyes adatot az Adatkezelő harmadik országban, továbbá nemzetközi szervezet keretein belül adatkezelést folytató adatkezelő vagy adatfeldolgozó részére - a közvetett adattovábbítást is ideértve - akkor továbbíthat (a továbbiakban együtt: nemzetközi adattovábbítás), ha
   a. a nemzetközi adattovábbításhoz az érintett kifejezetten hozzájárult, vagy

b. a nemzetközi adattovábbítás az adatkezelés céljának eléréséhez szükséges, valamint
   i. annak során az adatkezelésnek az 5. §-ban előírt feltételei teljesülnek, és
   ii. a harmadik országban, illetve a nemzetközi szervezet keretein belül adatkezelést folytató adatkezelő vagy adatfeldolgozó tekintetében a továbbított személyes adatok megfelelő szintű védelme biztosított, vagy
c. a nemzetközi adattovábbítás az alább meghatározott kivételes esetekben szükséges: adattovábbítás az érintett kifejezett hozzájárulásának hiányában kizárólag abban az esetben lehetséges, ha az
   i. az érintett vagy más személy létfontosságú érdekeinek védelme érdekében szükséges, vagy
   ii. valamely EGT-állam vagy harmadik ország közbiztonságát közvetlenül és súlyosan fenyegető veszély elhárítása érdekében szükséges, vagy
   iii. egyedi ügyben, eseti jelleggel az adatkezelő által végzett vizsgálatok vagy eljárások hatékony és eredményes lefolytatása érdekében szükséges, és az nem jár az érintett alapvető jogainak aránytalan korlátozásával, vagy
   iv. egyedi ügyben, eseti jelleggel az érintett vagy más jogi igényeinek előterjesztése, érvényesítése, illetve védelme érdekében szükséges, és az nem jár az érintett alapvető jogainak aránytalan korlátozásával.

11. FEJEZET: ADATBIZTONSÁG, A SZEMÉLYES ADATOK TÁROLÁSA, AZ INFORMÁCIÓBIZTONSÁG

1. Adatkezelő gondoskodik arról, hogy a vonatkozó jogszabályokban előírt adatbiztonsági szabályok érvényesüljenek. Ennek érdekében megteszi a szükséges technikai és szervezési intézkedéseket a tárolt adatállományok tekintetében.

2. Az adatbiztonsági szabályok tervezetének kialakításába az adatvédelmi tisztviselőt (kapcsolattartót, ha betöltésre került ilyen pozíció) be kell vonni.

3. Az adatbiztonsági intézkedéseket érintően a szervezeti egység vezetője
   1. a területére vonatkozó információk adatvédelmi tisztviselő (kapcsolattartó) és Adatkezelő adatvédelmi vezetése felé történő szolgáltatásával közreműködik az adatkezelés biztonságát fenyegető kockázatok felmérésében és meghatározásában;
   2. közreműködik azon információbiztonságot érintő feladatok végrehajtásában, amelyek az adatbiztonsági követelmények megvalósulásához szükségesek;
   3. figyelemmel kíséri a belső adatvédelmi és adatbiztonsági szabályok érvényre jutását a területen belül, jelzi a szabályok megsértését az érintett Munkatársak, tisztviselő (kapcsolattartó) és az Adatkezelő adatvédelmi vezetése számára.

4. Az adatbiztonsági intézkedések mindennapi működésben történő betartására a jelen Szabályzat és a Belső Adatbiztonsági Szabályzat személyi hatálya alá tartozó minden személy köteles.

5. Az Adatkezelő működése során betartandó adatbiztonsági szabályokat (GDPR 32. cikk) a belső adatbiztonsági szabályozási dokumentáció elemei tartalmazzák, a jelen fejezet csupán röviden összefoglalja azt, hogy az Adatkezelő mit biztosít.

6. Az Adatkezelő biztosítja

1. az adatkezeléshez használt eszközök (a továbbiakban: adatkezelő rendszer) jogosulatlan személyek általi hozzáférésének megtagadását a következő intézkedésekkel:
   i. Logikai hozzáférés szabályozása
   ii. A munkaállomások kezelése
   iii. Szabályzatok

2. az adathordozók jogosulatlan olvasásának, másolásának, módosításának vagy eltávolításának megakadályozását a következő intézkedésekkel:
   i. Logikai hozzáférés szabályozás
   ii. Nyomon követhetőség (naplózás)
   iii. Rosszindulatú software-ek kiszűrése
   iv. A munkaállomások kezelése
   v. Fizikai hozzáférés védelem
   vi. Hálózati tevékenységek megfigyelése
   vii. Szabályzatok

3. az adatkezelő rendszerbe a személyes adatok jogosulatlan bevitelének, valamint az abban tárolt személyes adatok jogosulatlan megismerésének, módosításának vagy törlésének megakadályozását a következő intézkedésekkel:
   i. Logikai hozzáférés szabályozás
   ii. Nyomon követhetőség (naplózás)
   iii. Rosszindulatú software-ek kiszűrése
   iv. A munkaállomások kezelése
   v. Fizikai hozzáférés védelem
   vi. Hálózati tevékenységek megfigyelése
   vii. Szabályzatok

4. az adatkezelő rendszerek jogosulatlan személyek általi, adatátviteli berendezés útján történő használatának megakadályozását a következő intézkedésekkel:
   i. A munkaállomások kezelése
   ii. Karbantartás
   iii. Webhely biztonság
   iv. Hálózatbiztonság
   v. Fizikai hozzáférés védelem
   vi. Hálózati tevékenységek megfigyelése
   vii. Hardware biztonság
   viii. Szabályzatok

5. azt, hogy az adatkezelő rendszer használatára jogosult személyek kizárólag a hozzáférési engedélyben meghatározott személyes adatokhoz férjenek hozzá a következő intézkedésekkel:
   i. Logikai hozzáférés szabályozás
   ii. Nyomon követhetőség (naplózás)
   iii. Fizikai hozzáférés védelem

6. azt, hogy ellenőrizhető és megállapítható legyen, hogy a személyes adatokat adatátviteli berendezés útján mely címzettnek továbbították vagy továbbíthatják, illetve bocsátották vagy bocsáthatják rendelkezésére a következő intézkedésekkel,

i. Nyomon követhetőség (naplózás)
ii. Nyilvántartások vezetése

7. azt, hogy utólag ellenőrizhető és megállapítható legyen, hogy mely személyes adatokat, mely időpontban, ki vitt be az adatkezelő rendszerbe a következő intézkedésekkel:
   i. Logikai hozzáférés szabályozás
   ii. Nyomon követhetőség (naplózás)

8. a személyes adatoknak azok továbbítása során vagy az adathordozó szállítása közben történő jogosulatlan megismerésének, másolásának, módosításának vagy törlésének megakadályozását a következő intézkedésekkel:
   i. Logikai hozzáférés szabályozás
   ii. Nyomon követhetőség (naplózás)
   iii. Fizikai hozzáférés védelem

9. azt, hogy üzemzavar esetén az adatkezelő rendszer helyreállítható legyen a következő intézkedésekkel:
   i. Biztonsági mentés

10. azt, hogy az adatkezelő rendszer működőképes legyen, a működése során fellépő hibákról jelentés készüljön, továbbá a tárolt személyes adatokat a rendszer hibás működtetésével sem lehessen megváltoztatni:
    i. Biztonsági mentés
    ii. Logikai hozzáférés szabályozás
    iii. Hálózatbiztonság
    iv. Hálózati tevékenységek megfigyelése
    v. Szabályzatok
    vi. A munkaállomások kezelése

7. Az adatbiztonság szabályainak érvényesüléséről az Adatkezelő az adatbiztonsági szabályozási dokumentáció részeiben gondoskodik.

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

9. Adatkezelő az adatbiztonsági intézkedéseket évente felülvizsgálja.

12. FEJEZET:
AZ ADATKEZELŐ NYILATKOZATAI

1. Az Adatkezelő kijelenti, hogy

    1. az adatkezelés során a GDPR, az Infotv, valamint a működésére vonatkozó más jogszabályok adatvédelemre, adatkezelésre, adatbiztonságra irányuló rendelkezéseinek megfelelően jár el. Azon esetekben, amelyre a jelen Szabályzat nem tartalmaz rendelkezést automatikusan és teljeskörűen a mindenkor hatályos jogszabályokban foglaltak az alkalmazandók, amely kötelezést az Adatkezelő magára nézve általánosan elismer.

    2. az adatkezelés során az Adatkezelő tudomására jutott személyes adatokat kizárólag azok a Munkatársak ismerhetik meg, akiknek az adott adatkezeléssel kapcsolatban feladatuk van.

    3. gondoskodik arról, hogy a Szabályzat és általában az adatvédelmi szabályozási dokumentáció a mindenkor hatályos jogszabályokkal összhangban legyen és azt a Munkatársak megismerjék.

    4. a weboldal a látogatók személyes adatait bizalmasan, a hatályos jogszabályi előírásokkal összhangban kezeli, gondoskodik azok biztonságáról, technikai és szervezési intézkedéseket tesz, valamint az adatvédelem elveinek maradéktalan betartása érdekében eljárási szabályokat alakít ki.

    5. a tőle elvárható módon mindent megtesz az általa kezelt személyes adatoknak a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, törlés, sérülés, megsemmisülés elleni védelem biztosítása, az ehhez szükséges technikai feltételek garantálása érdekében.

    6. a személyes adatokat harmadik személy részére csak kivételesen és abban az esetben továbbítja, valamint az általa kezelt adatbázist más adatkezelővel csak abban az esetben kapcsolja össze, ha annak jogszabályi feltételei fennállnak.

    7. az adattovábbításokról nyilvántartást vezet, amely tartalmazza az Adatkezelő által kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat, ha jogszabály ilyeneket előír.

    8. az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából adatvédelmi incidens kezelési szabályzatot hozott létre és az incidensekről nyilvántartást vezet. Az Adatkezelő indokolatlan késedelem nélkül – ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott – megteszi a bejelentést a felügyeleti hatóságnak *kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.*

13. FEJEZET:
EGYÉB RENDELKEZÉSEK

1. Jelen Szabályzat – változó működésből, vagy változó jogszabályi környezetből fakadó, esetleg pontatlanságból származó félreértések elkerülése miatt történő – módosítására az ok felmerülését követő 15 napon belül az Adatkezelő adatvédelmi vezetése (kapcsolattartó) írásbeli javaslatot tesz az adatvédelmi tisztviselő zámára, aki dönt a javaslatról a benyújtását követő 15 napon belül. A Szabályzat végső szövegezésének jóváhagyása, elektronikus és papír alapú kiadása, a személyi hatály alá tartozók számára történő elérhetővé tétele az Adatkezelő adatvédelmi vezetésének feladata és felelőssége.

Kelt: Budapest, 2026. szeptember hó 30. napján

Gráczer Irma
Igazgató
Budapest Főváros XV. Kerületi Önkormányzat
Göncz Árpád Szociális Intézmény



Budapest Főváros XV. Kerületi Önkormányzat Göncz Árpád Szociális Intézmény

Adatvédelmi Incidens Kezelési Szabályzat

Hatályos: 2026. 09. 30.

Adatkezelő: **Budapest Főváros XV. Kerületi Önkormányzat Göncz Árpád Szociális Intézmény** (székhely: 1157 Budapest, Árendás köz 4-6., képviseli: Gráczer Irma Igazgató, e-mail cím: igazgato@gaszixv.hu, tel.: 06-1-307-6263, 06-1-306-3184; adatvédelmi tisztviselő: Dr. Miklós Péter, dmp@dmp.hu). Érintett – az adott adatkezelés jogalapjához igazodóan – jogaival (hozzáférés, helyesbítés, törlés, elfeledtetés, korlátozás, tiltakozás, adathordozhatóság joga, hozzájárulás visszavonásának joga) az Adatkezelő elérhetőségére küldött kérelemmel élhet, továbbá panasszal fordulhat a hatósághoz (www.naih.hu, ugyfelszolgalat@naih.hu, 1363 Bp., Pf. 9.), és ha megítélése szerint megsértették jogait, fordulhat a lakóhelye szerint illetékes bírósághoz.

A Budapest Főváros XV. Kerületi Önkormányzat
Göncz Árpád Szociális Intézmény

Adatvédelmi Incidens Kezelési Szabályzata

Az Adatkezelő, a Budapest Főváros XV. Kerületi Önkormányzat Göncz Árpád Szociális Intézmény Göncz Árpád Szociális Intézménye(székhely: 1157 Budapest, Árendás köz 4-6., adószám: 15515579-2-42, a tényleges adatkezelés címei: a székhely, telephelyek mindenkori címei, internetes elérhetősége: http://gaszixv.hu/, telefonszám: 06-1-307-6263, 06-1-306-3184, e-mail: Igazgato@gaszixv.hu, képviseli: Gráczer Irma Igazgató, adatvédelmi tisztviselő neve és elérhetősége: Dr. Miklós Péter, postai úton elérhető a székhely címére címzett levél, e-mail-ben pedig a dmp@dmp.hu címre küldött e-mail útján) összhangban az Adatvédelmi Szabályzattal és belső adatvédelmi szabályozási dokumentáció más elemeivel, megalkotta a jelen Adatvédelmi Incidens Kezelési Szabályzatát.

BEVEZETÉS

1. Az 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.

2. Adatvédelmi incidens többek között, nem kizárólag a következők esetek mindegyike:
   a) bármely számítástechnikai rendszer feltörése,
   b) zsarolóvírus fertőzése,
   c) Munkatárs vagy harmadik személy jogosulatlan hozzáférése papír alapon vagy elektronikus úton tárolt adatokhoz
   d) e-mail téves címzettnek történő kiküldése,
   e) személyes adatokat tartalmazó számítástechnikai vagy más eszköz elvesztése, stb.

1. FEJEZET: FOGALOMMEGHATÁROZÁS

1. A jelen Szabályzatban használt fogalmak tartalma megegyezik au Adatvédelmi Szabályzatban meghatározott fogalmak tartalmával.

2. FEJEZET: A SZABÁLYZAT CÉLJA

1. A jelen Szabályzat elsődleges célja, hogy a szabályokat hozzon az esetlegesen bekövetkező adatvédelmi incidensek kezelésére, elhárítására, károk enyhítésére, és megelőzésére.

3. FEJEZET: A SZABÁLYZAT HATÁLYA

1. Időbeli hatály: Lásd a Jelen Szabályzatot kiadó/módosító utasítás hatályát.

2. Személyi hatály kiterjed a Munkatársakra, és mindazon személyekre, akik jogait vagy jogos érdekeit az adatvédelmi incidens érinti. Amennyiben a jelen szabályzat adatvédelmi tisztviselőt vagy kapcsolattartót említ és a pozíció betöltetlen, úgy feladatait az Adatkezelő adatvédelmi vezetése látja. Személyi hatály továbbá kiterjed azokra a Partnerekre, akik a rendelkezések hatályát szerződésben vagy nyilatkozatban magukra nézve kötelezően elfogadták. Ha a

Szabályzat szövegezéséből más nem következik, a Partnerek a Munkatársakra vonatkozó rendelkezések szerint kötelesek eljárni.

3. Tárgyi hatály: Jelen Szabályzat hatálya kiterjed az Adatkezelő bármely szervezeti egységében bekövetkezett adatvédelmi incidensre.

4. Területi hatály: Adatkezelő minden szervezeti egysége.

4. FEJEZET: ADATVÉDELMI INCIDENS ÉS ÉSZLELÉSE

1. Adatvédelmi incidens észlelése, tudomásszerzése nem kizárólag, a következő lehet:

a) adatvédelmi incidensre utaló tényt az Adatkezelő Munkatársa felfedez,
b) az Adatkezelőnek küldött üzenet, amely adatvédelmi incidensre utaló tényt tartalmaz, függetlenül attól, hogy az üzenetet milyen módon küldték, vagy hogy a küldő nem beazonosítható
c) az Adatkezelőt telefonon vagy személyesen értesítik az adatvédelmi incidensre utaló tényről, függetlenül attól, hogy az értesítő személy beazonosítható-e vagy sem
d) írott vagy elektronikus sajtóból az Adatkezelő értesül az adatvédelmi incidensre utaló tényről, körülményről,
e) adatfeldolgozó (esetleg közös adatkezelésben résztvevő, ha van ilyen), hatóság értesíti az Adatkezelőt adatvédelmi incidensről.

5. FEJEZET: MEGELŐZŐ ÉS FELDERÍTŐ INTÉZKEDÉSEK

1. Adatkezelő az adatvédelmi incidensek megelőzése és felderítése érdekében a következő technikai és szervezési intézkedéseket tette meg és ezen intézkedések megtételét rendszeresen ellenőrzi:

a) Adatvédelmi szabályozási dokumentációt hozott létre és tart naprakészen;
b) Adatvédelmi Szabályzatban meghatározta az adatvédelem szervezetét;
c) Adatvédelmi tisztviselőt nevezett ki;
d) Munkatársakat informálta és folyamatosan informálja, oktatja az adatvédelmi és adatbiztonsági szabályozásról, annak változásáról;
e) A Munkatársak megismerik és nyilatkozatokban veszik tudomásul a kialakított szabályozási rendszer rendelkezéseit;
f) Munkatársak a személyes adatokkal kizárólag az adatvédelmi szabályozási rendszerben meghatározott jogosultságok alapján, célból és módon kerülhetnek kapcsolatban, azokat csak a meghatározott módon kezelhetik;
g) Adatkezelő az informatikai adatvédelmi incidensek megelőzése és felderítése céljából a naplózási rendet vezet be és folyamatosan ellenőriz;
h) Adatkezelő egyéb informatikai eszközök segítségével akadályozza meg az adatok jogellenes kezelését, vagy azokhoz történő jogellenes hozzáférést.

6. FEJEZET: ELŐZETES ÉRTÉKELÉSI MINTA ADATVÉDELMI INCIDENS ESETÉBEN

1. Az Adatkezelő adatvédelmi vezetése a lenti linken elérhető értékelési sémát köteles használni a következő megjegyzéssel:

2. Az adatvédelmi tisztviselő (kapcsolattartó) az értékelésben aktívan közreműködni, javaslatot adni köteles.

3. Az adatvédelmi incidens súlyossága értékelésének fő kritériumai a következők:
   a) Az Adatkezelési Környezet (AK) és annak vizsgálata
   b) Az Azonosíthatóság Mértékének (AM) meghatározása: azt tárja fel, hogy az adatvédelmi incidenssel érintett adatokból mennyire könnyen lehet az érintettek azonosítását elvégezni
   c) A Sérülés Körülményeinek (SK) leírása: a sérülés körülményeit vizsgálja, elsősorban a megsérült adat biztonságának csökkenését, illetve a rosszindulatú támadásra és a szándékosságra utaló valamennyi jelet

4. Az értékelési séma segítséget nyújt az adatvédelmi incidensben érintett adatok típusának meghatározásában (pl. egyszerű adat, pénzügyi adat, viselkedésre vonatkozó adat, érzékeny adat), az eset körülményeinek feltérképezésében (a veszélyességet csökkentő, illetve növelő faktorok), és végül a veszély súlyosságának (VS) objektív mérők szerinti megállapításában.

5. A séma képlete: VS = AK x AM + SK

6. A vizsgálat eredményeként az adatvédelmi incidens súlyosságának alacsony, közepes, magas vagy nagyon magas fokozatát állapíthatja meg az Adatkezelő adatvédelmi vezetése.

7. Amennyiben a Nemzeti Adatvédelmi és Információszabadság Hatóság létrehozta saját értékelési módszertanát, azt kell megfelelően alkalmazni.

8. A rendelkezésre álló módszertan elérhetősége: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity/at_download/fullReport

9. Adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott (azt észlelte), bejelenteni köteles a Nemzeti Adatvédelmi és Információszabadság Hatóság számára, 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.

10. Amennyiben az értékelés alapján az adatvédelmi incidenst a hatóság felé be kell jelenteni, úgy az adatvédelmi tisztviselő (kapcsolattartó) előkészíti és az Adatkezelő adatvédelmi vezetése számára megküldi a bejelentés tervezetét, aki annak tartalmát köteles megvizsgálni.

11. Adatkezelő a bejelentésben köteles legalább

    a) ismertetni az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
    b) közölni az adatvédelmi tisztviselő (kapcsolattartó) nevét és elérhetőségeit (ha van);
    c) ismertetni az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

d) ismertetni 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. Adatkezelő adatvédelmi vezetése dönt a bejelentésről és szükség esetén megteszi a bejelentést.

13. 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. Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell a GDPR-ban foglaltnak megfelelő információkat. Az érintettet nem kell tájékoztatni, 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, 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

7. FEJEZET: MUNKATÁRSAK KÖTELEZETTSÉGEI AZ ADATVÉDELMI INCIDENSSEL KAPCSOLATBAN

1. Adatvédelmi incidenssel kapcsolatban a Munkatársak kötelezettségei a következők, függetlenül attól, hogy Munkatárs az adatvédelmi incidenst csekély jelentőségűnek is gondolja: Munkatárs köteles az észlelését követően azonnal, késedelem nélkül
    a) értesíteni az adatvédelmi incidensről vagy feltételezett adatvédelmi incidensről valamint a körülményekről az adatvédelmi szervezet szerinti vezetőjét, az adatvédelmi tisztviselőt (kapcsolattartót, ha ilyen pozíció betöltésre került), és az Adatkezelő adatvédelmi vezetését;
    b) feljegyezni a körülményeket, így
        i. az észlelés napját és időpontját, valamint, ha megállapítható
        ii. a (feltételezett) adatvédelmi incidens bekövetkezésének napját és időpontját;
        iii. azoknak a személyes adatoknak a körét, amelyet az adatvédelmi incidens érint;
        iv. a jogsértés okát és terjedelmét, valamint az érintett adatok és a jogsértés közötti összefüggést

2. A vezető az értesítést követően, azonnal, késedelem nélkül köteles
    a) értesíteni az adatvédelmi tisztviselőt (kapcsolattartót), valamint az Adatkezelő adatvédelmi vezetését, ha az ő értesítése valamely okból elmaradt;
    b) megtenni minden intézkedést a (feltételezett) adatvédelmi incidens (jogsértés) megszüntetése és a kárenyhítés érdekében, és
    c) e megtett intézkedésekről, továbbá az intézkedések kimeneteléről, hatásairól, beleértve azt az álláspontot és annak alapját is kifejtve, hogy van-e további intézkedésre szükség, valamint az intézkedések megtételének dokumentálásának megtörténtéről, annak

elküldésével értesíteni az adatvédelmi tisztviselőt (kapcsolattartót), az Adatkezelő adatvédelmi vezetését.

3. Az Adatkezelő adatvédelmi vezetése, az adatvédelmi tisztviselő (kapcsolattartó) együttműködésével az értesítést követően, azonnal, késedelem nélkül köteles
   a) felülvizsgálni a már megtett intézkedéseket, azokról és hatásaikról további részletes tájékoztatást kérni;
   b) megtenni minden további intézkedést a (feltételezett) adatvédelmi incidens megszüntetése és kárenyhítés érdekében, szükség esetén, példálózó felsorolással élve Munkatársak jogosultságait átmenetileg megvonni vagy módosítani, jelszavakat módosítani, adathordozókat zárolni, elérhetetlenné tenni, portokat lezárni;
   c) elvégezni az adatvédelmi incidens értékelését:
   d) felmérni az adatvédelmi incidenssel érintett adatok számát;
   e) felmérni az adatvédelmi incidenssel érintett érintettek körét és számát;
   f) felmérni az adatvédelmi incidens hatásait az érintettekre és az Adatkezelőre nézve;
   g) az értékelésről írásos összefoglalást készíteni;
   h) amennyiben az adatvédelmi incidens közepes vagy jelentős hatású, tájékoztatni az érintetteket az adatvédelmi incidens körülményeiről, hatásairól, elhárítására tett intézkedésekről, megelőző intézkedésekről, kivéve, ha a tájékoztatástól el lehet tekinteni (lásd fentebb és a GDPR rendelkezéseit);
   i) az újabb adatvédelmi incidens bekövetkezésének megelőzése céljából intézkedéseket, valamint ha szükséges, javaslatokat is tenni az Adatkezelő mindenkori vezetője felé;
   j) amennyiben szükséges, egyéb informatikai vonatkozású intézkedéseket tenni az adatvédelmi incidens körülményeire tekintettel, példálózó felsorolással élve adatmentést, adat visszaállítást végezni;
   k) amennyiben a jogszabályi feltételek fennállnak, a feljelentés alapjául szolgáló dokumentációt összeállítani és a feljelentést megfogalmazni;
   l) a fentiekről és minden egyéb körülményről jelentést létrehozni;
   m) a belső nyilvántartást vezetni az adatvédelmi incidensről.

4. Adatkezelő az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat. Adatkezelő a nyilvántartást az I. sz. mellékletben megfogalmazott minta felhasználásával vezeti.

5. Az Adatkezelő adatvédelmi vezetése köteles
   a) megismerni az adatvédelmi incidens minden körülményét (a számára tett jelentést);
   b) informálódni az adatvédelmi incidensről, amennyiben annak minden körülménye számára nem érthető;
   c) azonnal elrendelni minden olyan intézkedést, amely intézkedés a kárenyhítést vagy a jövőbeni újabb adatvédelmi incidens megelőzését szolgálja;
   d) amennyiben a jogszabályi feltételek fennállnak, feljelentést/bejelentést tenni az illetékes rendőrkapitányságon/hatóságnál.

6. Adatkezelő adatvédelmi vezetése az adatvédelmi incidens bejelentését, amennyiben annak feltételei fennállnak, a Hatóság honlapján (www.naih.hu) elérhető, mindenkori adatvédelmi incidensbejelentő rendszeren keresztül teszi meg, vagy a hatóság által létrehozott

formanyomtatványt használja és azt elektronikusan vagy papír alapon küldi meg a hatóság számára.

8. FEJEZET: ZÁRÓ RENDELKEZÉSEK

1. A jelen Szabályzat tartalmára a 2011. évi CXII. törvény, valamint az EU 2016/679. sz. rendelete (GDPR) irányadó elsődlegesen.

2. Amennyiben jelen szabályzat hatálybalépését követően jogszabályváltozás folytán a hatályos jogszabály a jelen szabályzatban foglalt értelmező rendelkezéstől eltérően határoz meg valamely fogalmat, eljárást, lépést, akkor ezen rendelkezés helyébe minden további rendelkezés nélkül a mindenkor hatályos jogszabályi rendelkezés lép.

3. Amennyiben jelen szabályzat hatálybalépését követően jogszabályváltozás folytán jelen szabályzat valamely rendelkezése a hatályos jogszabályok rendelkezéseivel nem áll többé összhangban, akkor az érintett rendelkezés helyébe minden külön rendelkezés nélkül a hatályos jogszabályi rendelkezés lép.

Kelt: Budapest, 2026. szeptember hó 30. napján

Graczer Irma
Igazgató
Budapest Főváros XV. Kerületi Önkormányzat
Göncz Árpád Szociális Intézmény

