



Debreceni Intézményműködtető Központ



**Adatvédelmi, adatkezelési, informatikai biztonsági,
valamint a közérdekű adatok megismerésére
irányuló kérelmek intézésének, a kötelezően
közzéteendő adatok nyilvánosságra hozatalának
szabályzata**

Hajnal János
igazgató

Tartalomjegyzék

I. Általános rendelkezések	4
1. A szabályzat célja.....	4
2. A szabályzat hatálya.....	4
3. Kapcsolódó jogszabályok	5
II. Részletes szabályok	7
1. Fogalmi meghatározások	7
2. Személyes adatok védelmére vonatkozó követelmények	9
2.1. A személyes adatok védelmének alapelvei.....	9
2.2. Az adatkezelés során alkalmazott jogalapok	10
2.3. Az érintett tájékoztatása az adat felvételéhez kapcsolódóan a GDPR 13. és 14. cikk szerint.....	11
2.4. Az adatvagyon leltár	11
2.5. Az érintettek jogai és azok érvényesítése	12
2.6. Az adatkezelés általános feltételei, az adatkezelésre vonatkozó szabályok, rendelkezések.....	14
2.7. Az adatkezelés típusai.....	15
2.8. Az adatkezelésre jogosultak köre és feladatai	16
2.9. Adatkezelési tevékenységek nyilvántartása.....	20
2.10. Adatvédelmi oktatás.....	20
2.11. Az adatfeldolgozó igénybevételére vonatkozó rendelkezések.....	20
2.12. Adatvédelmi incidens.....	21
2.13. Munkára alkalmas állapot vizsgálata	22
3. Informatikai biztonság	22
3.1. Az informatikai rendszer védelme.....	23
3.2. Biztonsági osztály, a védelmet igénylő adatok hozzáférési jogosultsága.....	23
3.3. Az informatikai eszközbázist veszélyeztető helyzetek.....	24
3.4. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek	24
3.5. Az informatikai eszközök környezete, azok védelme	25
3.6. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek	26
3.7. Központi számítógépek és a hálózat munkaállomásainak működésbiztonsága	28
4. A közérdekű adatok megismerésére irányuló kérelmek intézésének ügymenete, továbbá a kötelezően közzéteendő adatok nyilvánosságra hozatalának szabályai.....	31
4.1. A közérdekű adatok megismerésére irányuló kérelmek intézésének ügymenete..	31
4.2. A kötelezően közzéteendő adatok nyilvánosságra hozatalának szabályai.....	33

4.3.	A Központi Információs Közadat-nyilvántartás felületen előírt közzétételről és az átláthatósági eljárásról	33
III.	Záró rendelkezések	34

A Magyar Köztársaság Országgyűlése Magyarország európai uniós jogharmonizációs kötelezettségeinek teljesítése érdekében megalkotta az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvényt (Infotv.). A Debreceni Intézményműködtető Központ (továbbiakban: **DIM**) jelen szabályzata az Európai Parlament és a Tanács a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) szóló 2016/679. rendelete (GDPR rendelet) és az Infotv. rendelkezéseinek megfelelően készült. Jelen szabályzat információ biztonsági szabályozása során az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII.15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről rendelkezéseit kell figyelembe venni.

I. Általános rendelkezések

1. A szabályzat célja

Jelen szabályzat a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapítja meg. A szabályzatban foglaltakat kell alkalmazni a konkrét adatkezelési tevékenység során, valamint az adatkezelést szabályozó utasítások és tájékoztatások kiadásakor. A szabályzat célja, hogy meghatározza az informatikai rendszer adatbiztonsági követelményeinek érvényesülésével, a hardver és szoftver védelemmel kapcsolatos szabályokat és eljárásrendeket. A szabályzat célja továbbá, hogy meghatározza a közérdekű adatok megismerésére irányuló kérelmek intézésének szabályait, valamint szabályozza a kötelezően közzéteendő adatok nyilvánosságra hozatalával kapcsolatos általános feladatokat és a közzététel rendjét. A szabályzat célja, hogy biztosítsa a személyes adatok alaptörvény szerinti védelmének érvényesülését, az információs önrendelkezés megvalósulását, továbbá, hogy a DIM által kezelt személyes adatok tekintetében meghatározza az adatkezelés során irányadó adatvédelmi és adatbiztonsági szabályokat.

2. A szabályzat hatálya

Jelen szabályzat hatálya kiterjed a DIM által foglalkoztatott vezetőkre, közalkalmazottakra, megbízási szerződéssel foglalkoztatottakra, a DIM minden adatkezelésére és adatfeldolgozására, amely

- a) természetes személy személyes adataira, beleértve az adatkezelés minden elemét, függetlenül attól, hogy elektronikusan vagy papír alapon történik;
- b) közérdekű adatokra, azok közzétételére és megismerésére vonatkozik;
- c) valamint az adatvédelemmel, adatfeldolgozással kapcsolatos, a hardveres és szoftveres informatikai biztonsági szabályokra.

A DIM által kezelt személyes adatokat tartalmazó adattovábbításokra jelen szabályzat 1. számú melléklete szerinti nyilvántartást kell vezetni. Ennek vezetése a személyes adatokat kezelő részleg vezetőjének feladata. A nyilvántartást minden év december 31-i hatállyal a részlegvezető aláírásával le kell zárni, és azt az adatvédelmi tisztviselők részére megküldeni.

Amennyiben az adott évben nem történt adattovábbítás, akkor a nyilvántartást áthúzva (lezárva), dátummal és a részlegvezető aláírásával ellátva kell továbbítani az adatvédelmi tisztviselők részére.

3. Kapcsolódó jogszabályok

- az Európai Parlament és a Tanács (EU) 2016/679. rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (továbbiakban: GDPR)
- az információs önrendelkezési jogról az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.)
- az államháztartásról szóló 2011. évi CXCV. tv. (továbbiakban: Áht.)
- a költségvetési szervek belső kontrollrendszeréről és belső ellenőrzéséről szóló 370/2011. (XII.31.) Kormányrendelet (továbbiakban: Bkr.)
- a polgári törvénykönyvről szóló 2013. évi V. törvény (továbbiakban: Ptk.)
- a munka törvénykönyvéről szóló 2012. évi I. törvény (továbbiakban: Mt.)
- a közalkalmazottak jogállásáról szóló 1992.évi XXXIII. törvény (továbbiakban: Kjt.)
- 1995. évi CXVII. törvény a személyi jövedelemadóról (továbbiakban: Szja tv.)
- 1997. évi LXXX. törvény a társadalombiztosítás ellátásaira és a magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről (továbbiakban: TB tv.)
- kötelező egészségbiztosítás ellátásáról szóló 1997. évi LXXXIII. törvény (továbbiakban: Egbizt. tv.)
- 1993. évi XCIII. törvény a munkavédelemről
- 1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról
- 328/2011. (XII.29.) Korm. rendelet a személyes gondoskodást nyújtó gyermekjóléti alapellátások és gyermekvédelmi szakellátások térítési díjáról és az igénylésükhöz felhasználható bizonyítékokról
- a 11/2024. (I. 25.) Korm. rendelet a közérdekű és közérdekből nyilvános adatok átláthatósága és azok megismerhetőségére vonatkozó követelmények teljesülése ellenőrzésének részletes eljárási szabályairól, valamint egyes kormányrendeletek módosításáról
- a Magyar Államkincstárról szóló 310/2017. (X.31.) Korm. rendelet
- 1993. évi III. törvény a szociális igazgatásról és szociális ellátásokról

Kapcsolódó egyéb dokumentumok

- Munkamegosztási megállapodás – Áchim András Utcai Óvoda
- Munkamegosztási megállapodás – Alsójózsa Kerekerdő Óvoda
- Munkamegosztási megállapodás – Angyalkert Óvoda
- Munkamegosztási megállapodás – Boldogfalva Óvoda
- Munkamegosztási megállapodás – Faragó Utcai Óvoda
- Munkamegosztási megállapodás – Gönczy Pál Utcai Óvoda
- Munkamegosztási megállapodás – Görgey Utcai Óvoda
- Munkamegosztási megállapodás – Debreceni Arany János Óvoda
- Munkamegosztási megállapodás – Homokkerti Pitypang Óvoda
- Munkamegosztási megállapodás – Ifjúság Utcai Óvoda

- Munkamegosztási megállapodás – Ispotály Utcai Óvoda
- Munkamegosztási megállapodás – Karácsony György Utcai Óvoda
- Munkamegosztási megállapodás – Kemény Zsigmond Utcai Óvoda
- Munkamegosztási megállapodás – Közép Utcai Óvoda
- Munkamegosztási megállapodás – Kuruc Utcai Óvoda
- Munkamegosztási megállapodás – Lehel Utcai Óvoda
- Munkamegosztási megállapodás – Levendula Óvoda
- Munkamegosztási megállapodás – Liget Óvoda
- Munkamegosztási megállapodás – Margit Téri Óvoda
- Munkamegosztási megállapodás – Mesekert Óvoda
- Munkamegosztási megállapodás – Mosolykert Óvoda
- Munkamegosztási megállapodás – Nagyerdei Óvoda
- Munkamegosztási megállapodás – Pósa Utcai Óvoda
- Munkamegosztási megállapodás – Simonyi Úti Óvoda
- Munkamegosztási megállapodás – Sinay Miklós Utcai Óvoda
- Munkamegosztási megállapodás – Sípos Utcai Óvoda
- Munkamegosztási megállapodás – Szabadságtelepi Óvoda
- Munkamegosztási megállapodás – Százszorszép Óvoda
- Munkamegosztási megállapodás – Szivárvány Óvoda
- Munkamegosztási megállapodás – Táncsics Mihály Utcai Óvoda
- Munkamegosztási megállapodás – Thaly Kálmán Utcai Óvoda
- Munkamegosztási megállapodás – Tócsókerti Óvoda
- Munkamegosztási megállapodás – Újkerti Manófalva Óvoda
- Munkamegosztási megállapodás – DMJV Városi Szociális Szolgálat
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Áchim András Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Alsójózsai Kerekerdő Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Angyalkert Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Boldogfalva Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Faragó Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Gönczy Pál Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Görgey Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Debreceni Arany János Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Homokkerti Pityang Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Ifjúság Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Ispotály Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Karácsony György Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Kemény Zsigmond Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Közép Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Kuruc Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Lehel Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Levendula Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Liget Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Margit Téri Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Mesekert Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Mosolykert Óvoda

- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Nagyerdei Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Pósa Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Simonyi Úti Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Sinay Miklós Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Sípos Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Szabadságtelepi Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Százszorszép Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Szivárvány Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Táncsics Mihály Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Thaly Kálmán Utcai Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Tócoskerti Óvoda
- Adatfeldolgozási és közös adatkezelésről szóló szerződés – Újkerti Manófalva Óvoda
- Adatfeldolgozási szerződés – DMJV Család- és Gyermekjóléti Központja
- Adatfeldolgozási szerződés – Csokonai Nemzeti Színház Debrecen
- Adatfeldolgozási szerződés – Déri Múzeum
- Adatfeldolgozási szerződés – Debreceni Közterület Felügyelet
- Adatfeldolgozási szerződés – DMJV Egyesített Bölcsődei Intézménye
- Adatfeldolgozási szerződés – Méliusz Juhász Péter Könyvtár
- Adatfeldolgozási szerződés – Vojtina Bábszínház
- Adatfeldolgozási szerződés – DMJV Városi Szociális Szolgálat

II. Részletes szabályok

1. Fogalmi meghatározások

A szabályzatban az adatvédelmi szakkifejezések jelentése a következő:

- **adatállomány:** az egy nyilvántartásban (nyilvántartó-rendszerben) kezelt adatok összessége;
- **adatfeldolgozás:** az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelés összessége;
- **adatfeldolgozó:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel;
- **adatfelelős:** az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;
- **adatkezelés korlátozása:** a tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölése útján;
- **adatkezelés:** az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép -, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése;

- **adatkezelő:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.
- **adatközlő:** az a közfeladatot ellátó szerv, amely – ha az adatfelelős nem maga teszi közzé az adatot – az adatfelelős által hozzá eljuttatott adatot honlapon közzéteszi;
- **adatmegsemmisítés:** az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;
- **adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
- **adattörlés:** az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
- **adatvédelmi incidens:** az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát vagy az azokhoz való jogosulatlan hozzáférést eredményezi;
- **adatzárolás:** az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;
- **azonosítható természetes személy:** az a természetes személy, akit közvetlen vagy közvetett módon különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító, vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;
- **biometrikus adat:** egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat.
- **címzett:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz;
- **érintett:** bármely információ alapján azonosított vagy azonosítható természetes személy;
- **GDPR** (General Data Protection Regulation) az Európai Unió új Adatvédelmi Rendelete (Európai Parlament és a Tanács (EU) 2016/679 rendelet);
- **genetikai adat:** egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered;
- **harmadik személy:** olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek;
- **hozzájárulás:** az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozik vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez;

- **közérdekből nyilvános adat:** a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;
- **közérdekű adat:** az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;
- **különleges adat:** a személyes adatok különleges kategóriába 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;
- **nyilvánosságra hozatal:** az adat bárki számára történő hozzáférhetővé tétele;
- **személyes adat:** az érintettre vonatkozó bármely információ;
- **tiltakozás:** az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri;

2. Személyes adatok védelmére vonatkozó követelmények

2.1. A személyes adatok védelmének alapelvei

- **Jogszerűség, tisztességes eljárás és átláthatóság elve.** A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.
- **Célhoz kötöttség elve**
 - a) A foglalkoztatottak kizárólag a munkaköri leírásukban meghatározott feladataik ellátása céljából, a részükre biztosított jogosultságok rendeltetésszerű használatával kezelhetnek személyes adatot.
 - b) A konkrét, törvényben rögzített vagy az érintett által adott hozzájárulásban megfogalmazott célhoz nem köthető adatkezelés tilos.
 - c) Amennyiben az adatkezelés célja teljesült, vagy megszűnt, az adatkezelésre irányadó jogszabályban vagy a levéltári törvényben szereplő tárolási határidőt követően az elektronikusan tárolt adatot törölni a papír alapon tárolt adatot pedig selejtezni kell.
 - d) Azok a papír alapon tárolt adatok melyek nem selejtezhetők, az adatkezelésre jogosult személyek köre által kerül irattározásra.
- **Az adatminőség elve.** Amennyiben a DIM munkavállalója tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos, vagy időszerűtlen, köteles azt helyesbíteni, vagy az adat helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni és erről mindazokat értesíteni, akiknek az adat továbbításra kerül.
- **Adatbiztonság elve.** Az adat kezelése során biztosítani kell, hogy:
 - a) a személyes adat illetéktelen harmadik személy tudomására nem jusson (bizalmasság)

- b) az adat illetéktelen harmadik személy által nem legyen módosítható (sértetlenség)
- c) az adat elérhető legyen a feljogosított személyek, szervezetek számára (rendelkezésre állás)
- **Adatminimalizálás elve.** A DIM kizárólag annyi és olyan személyes adatot kezelhet, amely az érintett egyértelmű azonosításához és ügyének elintézéséhez minimálisan szükséges, arra alkalmas.
- **Pontosság elve.** A személyes adatoknak pontosnak és naprakésznek kell lenniük. A pontatlan személyes adatokat haladéktalanul törölni kell, vagy helyesbíteni, ennek érdekében minden ésszerű intézkedést meg kell tenni.
- **Korlátozott tárolhatóság elve.** A személyes adatokat olyan formában kell tárolni, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé, figyelemmel a vonatkozó jogszabályokban meghatározott tárolási kötelezettségre.
- **Integritás és bizalmas jelleg elve.** Megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítani kell a személyes adatok megfelelő biztonságát, ideértve a személyes adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet.
- **Elszámoltathatóság elve.** Gondoskodni kell a jelen szabályzatban foglaltak folyamatos érvényesüléséről, az adatkezelés folyamatos felülvizsgálatáról és szükség esetén az adatkezelési eljárások módosításáról, kiegészítéséről.

Az adatvédelem fenti elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell.

2.2. Az adatkezelés során alkalmazott jogalapok

Az adatkezelés jogalapját a DIM minden adatkezelési folyamatnál meghatározza. Az adatkezelésre jogalapot csak a GDPR 6. cikk (1) és 9. cikk (2) bekezdésekben rögzítettek szerint határoz meg a DIM.

- **Hozzájáruláson alapuló adatkezelés:** az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez.
- **Szerződésen alapuló adatkezelés:** 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.
- **Jogi kötelezettségen alapuló adatkezelés:** az adatkezelés a DIM-re vonatkozó jogi kötelezettség teljesítéséhez szükséges.
- **Közérdek, közhatalmi jogosítvány:** az adatkezelés közérdekű vagy az adatkezelőre átruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.
- **Jogos érdek:** az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

A DIM egy adott személyes **adatkör** kezelése vonatkozásában egy jogalap alapján végzi az adatkezelést. Az adatkezelés **jogalapja** az adatkezelés során változhat.

2.3. Az érintett tájékoztatása az adat felvételéhez kapcsolódóan a GDPR 13. és 14. cikk szerint

Abban az esetben, amennyiben az adatkezelés során a személyes adatokat a DIM közvetlenül az érintettől szerzi meg, úgy a személyes adatok megszerzésének időpontjában alábbiakról tájékoztatja az érintettet:

- a DIM pontos megnevezése, elérhetőségei,
- a DIM adatvédelmi tisztviselőjének elérhetőségei,
- az adatkezelés célja,
- az adatkezelés jogalapja,
- amennyiben az adatkezelés célja a DIM vagy egy harmadik fél jogos érdekeinek érvényesítése, úgy a DIM vagy a harmadik fél jogos érdekének megnevezése,
- amennyiben a DIM a személyes adatokat az adatkezelés során harmadik fél számára átadja, a személyes adatok címzettjei, illetve a címzettek kategóriái,
- a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,
- a hozzáférési jog gyakorlásának szabályai,
- a helyesbítési jog gyakorlásának szabályai,
- a törlési jog gyakorlásának szabályai,
- az adatkezelés korlátozására irányuló jog gyakorlásának szabályai,
- a tiltakozási jog gyakorlásának szabályai,
- az adathordozhatósághoz való jog gyakorlásának szabályai,
- a hozzájárulás visszavonására irányuló jog gyakorlásának szabályai, amennyiben az adatkezelés jogalapja az érintett hozzájárulása [GDPR. 6. cikk 1.) a.)] vagy a [GDPR. 9. cikk 2.) a.)] pontba foglalt jogalap,
- a Nemzeti Adatvédelmi és Információs szabadság Hatósághoz (továbbiakban: Hatóság) címzett panasz benyújtásának jogáról;
- annak ténye, hogy a személyes adat kezelése, szolgáltatása jogszabályon, szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele és az érintett köteles-e a személyes adatokat megadni, valamint a lehetséges következmények, amennyiben az érintett személyes adatait nem adja meg,
- az automatizált döntéshozatal ténye, valamint legalább az ennek során alkalmazott logika és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

A DIM a GDPR 14. cikke szerint nem kezel személyes adatot.

A tájékoztatást a DIM elsősorban a jelen szabályzat függelékét képező adatkezelési tájékoztatóval valósítja meg. Ezen tájékoztatót a DIM minden olyan esetben elkészíti, amikor az érintettet tájékoztatnia kell az adatkezelésről.

A tájékoztató nyilvánosságra hozatalának szabálya: a jelen szabályzat szerint elkészített adatkezelési tájékoztató elválaszthatatlan részét képezik a szabályzatnak.

2.4. Az adatvagyon leltár

A DIM a tevékenysége körében végzett adatkezelésre vonatkozó, a GDPR és a jogszabályok által előírt kötelezettségeknek megfelelő technikai és szervezési intézkedések megalkotása

céljából adatvagyon leltárt készít. Az adatvagyon leltár tartalmazza a DIM által kezelt összes adatkört.

Az adatvagyon leltárban meghatározásra kerülnek:

- a kezelt adatok köre
- az adatkezelés célja
- az adatkezelés jogalapja
- tárolás helye
- tárolás módja
- tárolás időtartama
- adat forrása
- adat megadásának időpontja
- címzett (ha van)
- közlés célja (ha van címzett)

2.5. Az érintettek jogai és azok érvényesítése

Az érintett jogai mindig az adott adatkezelés jogalapjához idomul.

	Hozzájárulás	Szerződés teljesítése	Jogi kötelezettség	Jogos érdek	Közérdek, közhatalmi jogosítvány
Tájékoztatáshoz való jog	x	x	x	x	x
Hozzájárulás visszavonásához való jog	x				
Hozzáféréshez való jog	x	x	x	x	x
Adatok módosításához, helyesbítéséhez, törléséhez való jog	x	x	x	x	x
Adatkezelés korlátozásához való jog	x	x	x	x	x
Tiltakozáshoz való jog				x	x
Adathordozhatósági joghoz való jog	x	x			
Jogorvoslathoz való jog	x	x	x	x	x

Az érintett **tájékoztatást** kérhet személyes adatai kezeléséről, valamint kérheti személyes adatainak **helyesbítését**, illetve - a jogszabályban elrendelt adatkezelések kivételével - **törlését**. Az érintett kérelmére az adatkezelő tájékoztatást ad az általa kezelt, illetőleg az általa megbízott feldolgozó által feldolgozott **adatairól**, az adatkezelés céljáról, jogalapjáról, időtartamáról, az **adattfeldolgozó nevéről, címéről** (székhelyéről) és az adatkezeléssel összefüggő **tevékenységéről**, továbbá arról, **hogyan** kik és milyen célból kapják vagy kapták meg az adatokat.

Az adatkezelő köteles a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 30 napon belül írásban, közérthető formában megadni a tájékoztatást.

A valóságnak nem megfelelő adatot az adatkezelő **helyesbíteni** köteles.

A személyes adatot **törölni** kell, ha:

- kezelése jogellenes,
- az érintett kéri,
- az hiányos vagy téves - és ez az állapot jogszerűen nem korrigálható -, feltéve, hogy a törlést törvény nem zárja ki,
- az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt,
- azt a bíróság vagy az adatvédelmi tisztviselő elrendelte.

Az adatkezelő minden olyan címzettet tájékoztat a 16. cikk, a 17. cikk (1) bekezdése, illetve a 18. cikk szerinti valamennyi helyesbítésről, törlésről vagy adatkezelés – korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel.

Hozzáférés joga

Az érintett jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

- a) az adatkezelés célja;
- b) az érintett személyes adatok kategóriái;
- c) azon címzett vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják,
- d) a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges ezen időtartam meghatározásának szempontjai;
- e) az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
- f) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
- g) ha az adatokat nem az érintettől gyűjtötték, a forrásokra vonatkozó minden elérhető információ;

Korlátozáshoz való jog

Az érintett jogosult arra, hogy kérésére a DIM korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

- a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az Adatkezelő ellenőrizze a személyes adatok pontosságát;
- b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
- c) az Adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy
- d) az érintett 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.

Az érintett **tiltakozhat** személyes adatának kezelése ellen, ha:

- a személyes adatok kezelése (továbbítása) kizárólag az adatkezelő vagy az adatátvevő jogának vagy jogos érdekének érvényesítéséhez szükséges, kivéve, ha az adatkezelést törvény rendelte el,

- a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik,
- a tiltakozás jogának gyakorlását egyébként törvény lehetővé teszi.

Az adatkezelő – az adatkezelés egyidejű felfüggesztésével – a tiltakozást köteles a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 nap alatt megvizsgálni, és annak eredményéről a kérelmezőt írásban tájékoztatni. Amennyiben a tiltakozás indokolt, az adatkezelő köteles az adatkezelést – beleértve a további adatfelvételt és adattovábbítást is – megszüntetni, és az adatokat zárolni, valamint a tiltakozásról, illetőleg az annak alapján tett intézkedésekről értesíteni mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbította, és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében. Az adatkezelő az érintett adatát nem törölheti, ha az adatkezelést törvény rendelte el. Az adat azonban nem továbbítható az adatátvevő részére, ha az adatkezelő egyetértett a tiltakozással, illetőleg a bíróság a tiltakozás jogosságát megállapította.

Adathordozhatósághoz való jog

Az érintett – a GDPR 27. cikk (1) bekezdésében foglalt feltételek fennállása esetén – jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formában megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa.

Jogorvoslathoz való jog

Az Adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak okozott kárt, illetve az általa vagy az általa igénybe vett adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is megtéríti. Az Adatkezelő mentesül az okozott kárért való felelősség és a sérelemdíj megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső elháríthatatlan ok idézte elő. Ugyanígy nem téríti meg a kárt, amennyiben az a károsult szándékos vagy súlyosan gondatlan magatartásából származott. Ha az Adatkezelő nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be NAIH-nál (1055 Budapest, Falk Miksa u. 9-11.) és élhet - lakóhelye vagy tartózkodási helye szerint illetékes törvényszéknél is - bírósági jogorvoslati jogával.

A DIM az érintettnek adott minden tájékoztatást főszabály szerint írásban tesz meg, ideértve az elektronikus utat is.

2.6. Az adatkezelés általános feltételei, az adatkezelésre vonatkozó szabályok, rendelkezések

- Személyes adat akkor kezelhető, ha:
 - a) azt törvény, vagy – törvény felhatalmazása alapján az abban meghatározott körben, különleges adatnak vagy bűnügyi személyes adatnak nem minősülő adat esetén – helyi önkormányzat rendelete közérdeken alapuló célból elrendeli;
 - b) a) pontban meghatározottak hiányában az az adatkezelő törvényben meghatározott feladatainak ellátásához feltétlenül szükséges és az érintett a személyes adatok kezeléséhez kifejezetten hozzájárul;
 - c) az a) pontban meghatározottak hiányában az az érintett vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy

javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges és azzal arányos, vagy

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

A DIM adatkezelést végző munkavállalója büntetőjogi felelősséggel tartozik a személyes adatok jogszerű kezeléséért.

Amennyiben a kezelt személyes adatokban változás következik be, vagy az adatkezelés célja módosul, akkor azt az adatkezelő (a részlegek esetén az adott részleg vezetője) haladéktalanul írásban (e-mail) jelezni köteles az adatvédelmi tisztviselők részére. Az adatkezelési tájékoztatóban a módosítást az adatvédelmi tisztviselő végzi el.

Ha a kötelező adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény, helyi önkormányzat rendelete vagy az Európai Unió kötelező jogi aktusa nem határozza meg, az adatkezelő az adatkezelés megkezdésétől legalább háromévente felülvizsgálja, hogy az általa illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges – e. Ezen felülvizsgálat körülményeit és eredményét az adatkezelő dokumentálja, e dokumentációt a felülvizsgálat elvégzését követő tíz évig megőrzi és azt a Hatóság kérésére a rendelkezésére bocsátja.

- A személyes adatokhoz csak az illetékes munkaköröket betöltő személyek férhetnek hozzá.
- Az adatkezelő vállalja, hogy amennyiben bármilyen módon változtatna a személyes adatok kezelésére vonatkozó célokon és jogalapokon, ezekről a változásokról az adatkezelési tájékoztatóban értesíti az érintetteket. A személyes adatok kezeléséről és védelméről szóló jelen Szabályzat mindig a ténylegesen alkalmazott elveket és a valóságos gyakorlatot tükrözi.
- Amennyiben az arra feljogosított hatóságok a jogszabályokban előírt módon kérik fel személyes adatok átadására a DIM-et, az adatkezelő - törvényi kötelezettségének eleget téve - átadja a kért és rendelkezésre álló információkat.
- Törvény közérdekből - az adatok körének kifejezett megjelölésével - elrendeli a személyes adat nyilvánosságra hozatalát. Minden egyéb esetben a nyilvánosságra hozatalhoz az érintett írásbeli hozzájárulása szükséges. Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg. Az érintett hozzájárulását megadottnak kell tekinteni az érintett közszereplése során általa közölt vagy a nyilvánosságra hozatal céljából általa átadott adatok tekintetében. Az érintett kérelmére indult eljárásban a szükséges adatainak kezeléséhez való hozzájárulását vélelmezni kell. Erre a tényre az érintett figyelmét fel kell hívni.
- Az elektronikusan (e-mailben) kiküldött leveleket a következő záradékkal kötelező ellátni:
*„Ez az e-mail (annak bármely csatolmánya) bizalmas információkat tartalmaz és kizárólag a címzettnek szól. Amennyiben nem Ön a címzett, vagy tévesen kapta meg ezt a levelet, kérjük, azonnal értesítsen Bennünket válaszléssel küldése útján, majd törölje a levél teljes tartalmát (beleértve az esetleges melléklete(ke)t is)!
Felhívjuk a figyelmét, hogy az eredeti címzettnek szánt információk másolása, mentése, továbbítása vagy nyilvánosságra hozatala szigorúan tilos.”*

2.7. Az adatkezelés típusai

A DIM ügyviteli és nyilvántartási típusú adatkezelést végez.

Az ügyviteli típusú adatkezelés szorosan a feladatellátáshoz kapcsolódik, alapvető rendeltetése az adott feladatellátással kapcsolatos ügyintézés elvégzéséhez szükséges adatok biztosítása. A

nyilvántartási típusú adatkezelés az előre meghatározott feladat alapján gyűjtött személyes adatfajtákból strukturált adatállományt hoz létre, az adatkezelés időtartama alatt biztosítva az adatok különböző jellemzők alapján történő lekérdezhetőségét. A feladattal összefüggésben gyűjtött adatok kezelése ebben az esetben elválik az alapeljárástól, az adatok kezelésének időtartamát az adatok kezelésére felhatalmazást adó törvény, munkaviszony, szerződéses viszony vagy az érintett beleegyezésében foglaltak határozzák meg.

2.8. Az adatkezelésre jogosultak köre és feladatai

Igazgató feladatai:

- felelős a DIM adatkezelésének jogszerűségéért;
- gondoskodik az adatkezelés személyi és tárgyi feltételeinek biztosításáról;
- kinevezi a DIM adatvédelmi tisztviselőit (két főt, a feladatellátás folyamatossága érdekében);
- a DIM, mint adatkezelő tekintetében meghozza az adatkezelésre vonatkozó döntéseket;
- a személyes adatok továbbítása és a közérdekű adatok közzététele a jóváhagyásával történhet;
- részt vesz jelen szabályzat rendelkezéseire vonatkozó oktatásokon;
- jogviszonyának fennállása alatt és annak megszüntetését követően is titokként megőrzi a beosztásával, annak ellátásával kapcsolatban tudomására jutott személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy körülményt, amelyet az őt alkalmazó adatkezelő vagy adatfeldolgozó nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni;
- köteles jelen szabályzat 2. számú, 2/a. számú melléklete szerinti Adatkezelési és számítógépes felhasználói nyilatkozatban foglaltakat aláírni, az abban foglaltakat betartani és betartatni.

Gazdasági igazgató feladatai

- véleményezi jelen szabályzat módosítására vonatkozó javaslatokat;
- gondoskodik jelen szabályzat végrehajtásához szükséges eszközök fedezetének rendelkezésre állásáról;
- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet;
- részt vesz, valamint biztosítja a vezetése alatt álló dolgozók részvételét a jelen szabályzat rendelkezéseire történő oktatáson;
- jelen szabályzat 4. számú mellékletében foglaltak szerint gondoskodik a kötelezően közzéteendő adatok rendszergazda részére történő továbbításáról;
- jogviszonyának fennállása alatt és annak megszüntetését követően is titokként megőrzi a beosztásával, annak ellátásával kapcsolatban tudomására jutott személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy körülményt, amelyet az őt alkalmazó adatkezelő vagy adatfeldolgozó nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni;
- köteles jelen szabályzat 2. számú, 2/a. számú melléklete szerinti Adatkezelési és számítógépes felhasználói nyilatkozatban foglaltakat aláírni, az abban foglaltakat betartani és betartatni.

Részlegvezetők feladatai

- véleményezi jelen szabályzat módosítására vonatkozó javaslatokat;
- az adatvédelmi tisztviselőkkel egyeztetve végrehajtja jelen szabályzat rendelkezéseinek a **részleg** munkatársainak munkaköri leírásain történő átvezetését;
- a vezetése alatt álló **munkavállalók** vonatkozásában jelen szabályzat előírásainak betartatása, annak **ellenőrzése**;
- az előírások ellen **vétőkkel** szemben felelősségre vonási eljárást kezdeményezhet;
- vezeti az **adattovábbítások** nyilvántartását, jelen szabályzat 1. számú melléklete alapján;
- részt vesz, valamint biztosítja a vezetése alatt álló dolgozók részvételét a jelen szabályzat rendelkezéseire történő oktatáson;
- elkészíti jelen szabályzat 4. számú mellékletében foglalt, kötelezően közzéteendő adatot, és továbbítja az igazgatási részlegvezetőnek, aki a rendszergazda felé továbbítja;
- jogviszonyának fennállása alatt és annak megszűntetését követően is titokként megőrzi a beosztásával, annak ellátásával kapcsolatban tudomására jutott személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy körülményt, amelyet az őt alkalmazó adatkezelő vagy adatfeldolgozó nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni;
- köteles jelen szabályzat 2. számú, 2/a számú melléklete szerinti Adatkezelési és számítógépes felhasználói nyilatkozatban foglaltakat aláírni és aláíratni, az abban foglaltakat betartani és betartatni.

A fentiekén túl az egyes részlegvezetők további feladatai:

- A **személyzeti-munkaügyi részlegvezető** vezeti a DIM részére beadott, állásra jelentkezők önéletrajzának 8. számú melléklet szerinti nyilvántartását. A nyilvántartásban **csak** azok az önéletrajzok szerepelhetnek, amelyek esetében a jelentkező nyilatkozatot tett annak kezelésére. A nyilvántartott önéletrajzot az adatkezelési tájékoztatónak megfelelően 1 év után meg kell semmisíteni.
- A **műszaki részlegvezető** feladata
 - az informatikai **rendszerek**, szoftverek védelmi eszközök működésének szervíz ellátás biztosítása, a védelmi előírások folyamatos betartása, a védelmi rendszer érvényesülésének **ellenőrzése**;
 - felelős az informatikai rendszerek üzembiztonságáért, biztonsági másolatok készítéséért és **karbantartásáért**;
 - kialakítja a **védelmi** eszközök alkalmazására vonatkozó döntés előkészítése érdekében a **szakterületek** bevonásával a biztonságot növelő intézkedéseket;
 - rendszeresen **beszámol** a rendszergazda és a hálózati informatikus tevékenységéről a gazdasági igazgatónak.
- A **belső ellenőrzési vezető** gondoskodik jelen szabályzat rendelkezéseinek betartására vonatkozó, **ütemezett** ellenőrzéséről, valamint a gazdasági szervezettel nem rendelkező intézményeknél az adatvédelemmel, adatkezeléssel, informatikai biztonsággal, közzétételi kötelezettséggel kapcsolatos feladatok elvégzésének ütemezett ellenőrzéséről.

Rendszergazda feladatai:

- feladata a **védelmi** eszközök működésének, szervíz ellátás biztosításának folyamatos **ellenőrzése**;
- felelős a DIM informatikai rendszere hardver eszközeinek karbantartásáért, és időszakos hardver tesztjeiért;

- ellenőrzi a vásárolt szoftverek helyes működését, vírusmentességét, a használat jogszerűségét;
- a vírusvédelemmel foglalkozó szolgáltatóval kapcsolatot tart;
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek izolálásáról;
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működése és biztonsága szempontjából a lényeges paraméterek alakulását;
- ellenőrzi a rendszer önadminisztrációját;
- tevékenységéről rendszeresen beszámol a műszaki részlegvezetőnek;
- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot;
- előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét;
- a részére továbbított, adatvédelemmel, adatkezeléssel, kötelezően közzéteendő adatokkal kapcsolatos anyagok honlapon történő megjelenéséről gondoskodik;
- az adatvédelmi oktatáson a hálózati informatikussal közösen az adatvédelem informatikai biztonságára vonatkozó szabályokat ismerteti;
- részt vesz a jelen szabályzat rendelkezéseire vonatkozó oktatásokon;
- jogviszonyának fennállása alatt és annak megszüntetését követően is titokként megőrzi a beosztásával, annak ellátásával kapcsolatban tudomására jutott személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy körülményt, amelyet az őt alkalmazó adatkezelő vagy adatfeldolgozó nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni;
- Köteles jelen szabályzat 2. számú, 2/a. számú melléklete szerinti Adatkezelési és számítógépes felhasználói nyilatkozatban foglaltakat aláírni, az abban foglaltakat betartani és betartatni.

Hálózati informatikus feladatai:

- hálózat üzemeltetése (LAN, WIFI, VPN) hálózat és internetes betáplálás konfigurálása, üzemeltetése
 - router-tűzfal menedzsment (portszűrés, portforwarding)
 - hálózati végpontok kiosztása, aktiválása, DHCP
 - wireless-hálózat menedzsment
- szerverkonfigurálás, adminisztrálás és üzemeltetés
 - fileserver üzemeltetés, megosztások, jogosultsági rendszer kialakítása
 - felhasználói hozzáférések kezelése
 - internetes szolgáltatások
 - domain adminisztráció
 - e-mail adminisztráció: e-mail fiókok létrehozása, adminisztrálása
- munkaállomás konfigurálás, adminisztrálás és üzemeltetés
 - MS Windows munkacsoportos hálózati környezet megtervezése, létrehozása, üzemeltetése
- nyomtató konfigurálás, adminisztrálás és üzemeltetés
 - hálózati nyomtatók LAN-ba implementálása, megosztása
- felhasználó támogatás távsegítséggel
- az adatvédelmi oktatáson a rendszergazdával közösen az adatvédelem informatikai biztonságára vonatkozó szabályokat ismerteti;
- részt vesz a jelen szabályzat rendelkezéseire vonatkozó oktatásokon;
- jogviszonyának fennállása alatt és annak megszüntetését követően is titokként megőrzi a beosztásával, annak ellátásával kapcsolatban tudomására jutott személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatás gyakorlásához kötött

titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy körülményt, amelyet az őt alkalmazó adatkezelő vagy adatfeldolgozó nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni;

- Köteles jelen szabályzat 2. számú, 2/a. számú melléklete szerinti Adatkezelési és számítógépes felhasználói nyilatkozatban foglaltakat aláírni, az abban foglaltakat betartani és betartatni.

Adatvédelmi tisztviselő feladatai:

- elősegíti az adatkezelő illetve az adatfeldolgozó – a személyes adatok kezelésére vonatkozó jogi előírásokban meghatározott – kötelezettségeinek teljesítését, így különösen a személyes adatok kezelésére vonatkozó jogi előírásokról naprakész tájékoztatást nyújt és azok érvényesítésének módjaival kapcsolatban tanácsot ad az adatkezelő, az adatfeldolgozó és az azok által foglalkoztatott, az adatkezelési műveleteket végző személyek részére;
- folyamatosan figyelemmel kíséri és ellenőrzi a személyes adatok kezelésére vonatkozó jogi előírások, jogszabályok és belső adatvédelmi és adatbiztonsági szabályzatok érvényesülését, ennek keretei között az egyes adatkezelési műveletekhez kapcsolódó egyértelmű feladat meghatározás, az adatkezelési műveletekben foglalkoztatottak adatvédelmi ismereteinek bővítése és tudatosságnövelése, a kötelezően közze teendő adatok a honlapon történő, jelen szabályzat szerinti megjelenését;
- elősegíti az érintettet megillető jogok gyakorlását, így különösen kivizsgálja az érintettek panaszait és kezdeményezi az adatkezelőnél, illetve az adatfeldolgozónál a panasz orvoslásához szükséges intézkedések megtételét;
- kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat tanácsi rendelet 35. cikkelye szerinti elvégzését;
- együttműködik a felügyeleti hatósággal;
- lefolytatja az esetlegesen előforduló adatvédelmi incidens kivizsgálására vonatkozó eljárást, szükség esetén bejelenti a NAIH felé, vezeti az előforduló incidensek nyilvántartását, jelen szabályzat 7. sz. mellékletében foglalt nyilvántartó lap használatával;
- elkészíti jelen szabályzatot, gondoskodik annak aktualizálásáról;
- szükség szerint a jelen szabályzat rendelkezéseire vonatkozó oktatások megtartása.
- közreműködik a háromévente esedékes adatkezelési felülvizsgálatot, annak dokumentációját megőrzi, eredményéről nyilvántartást vezet;
- az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi;
- az adatvédelmi tisztviselő jogviszonyának fennállása alatt és annak megszüntetését követően is titokként megőrzi a tevékenységével, annak ellátásával kapcsolatban tudomására jutott személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy körülményt, amelyet az őt alkalmazó adatkezelő vagy adatfeldolgozó nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni;
- Köteles jelen szabályzat 2. számú, 2/a. számú melléklete szerinti Adatkezelési és számítógépes felhasználói nyilatkozatban foglaltakat aláírni, az abban foglaltakat betartani és betartatni.

Az előzőekben fel nem sorolt valamennyi, a DIM alkalmazásában álló, adatkezelés és/vagy adatfeldolgozást végző munkatárs feladatai

- részt vesz jelen szabályzat rendelkezéseire vonatkozó oktatásokon;
- jogviszonyának fennállása alatt és annak megszűntetését követően is titokként megőrzi a beosztásával, annak ellátásával kapcsolatban tudomására jutott személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy körülményt, amelyet az őt alkalmazó adatkezelő vagy adatfeldolgozó nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni;
- Köteles jelen szabályzat 2. számú, 2/a. számú melléklete szerinti Adatkezelési és számítógépes felhasználói nyilatkozatban foglaltakat aláírni, az abban foglaltakat betartani.

2.9. Adatkezelési tevékenységek nyilvántartása

Az adatkezelési tevékenységek nyilvántartását a DIM az elszámoltathatóság elvéből következően annak érdekében végzi, hogy a GDPR-nak való megfelelést nyomon tudja követni és igazolni tudja. A nyilvántartásokat a DIM írásban vezeti, papíralapon vagy elektronikus formátumban.

2.10. Adatvédelmi oktatás

Az adatvédelmi tisztviselők szükség szerint jelenléti vagy online oktatást tartanak az adatvédelmi tudatosság emelése érdekében, amelyen kötelesek részt venni a DIM munkatársai. Az adatvédelmi oktatásnak legalább az alábbi témákra kell kiterjednie:

- az előző oktatás óta eltelt időszak tapasztalatai az adatvédelem területén,
- amennyiben az előző oktatás óta módosult a szabályzat, a módosítással kapcsolatos legfontosabb tudnivalók,
- az esetlegesen megtörtént adatvédelmi incidens bemutatása, értékelése, a helyesbítő-megelőző intézkedések ismertetése,
- az adatvédelem területén történt általános változások, jogszabály módosítások, Magyarországon és az Európai Unióban, különös tekintettel a hatóságok bírságolási gyakorlatára.

Az adatvédelmi tisztviselő rendkívüli oktatást tart – amennyiben az indokolt – az alábbi esetekben:

- adatvédelmi incidens megtörténte,
- marasztalással záruló NAIH-eljárás lefolytatása a DIM-mel szemben.

Új dolgozók belépésekor a személyzeti-munkaügyi részleg tájékoztatja az adatvédelmi tisztviselőket, akik az alapvető adatvédelmi szabályokat, eljárásokat e-mailben megküldik. A dolgozó ezek megismerését és tudomásul vételét nyilatkozatban aláírásával igazolja.

2.11. Az adatfeldolgozó igénybevételére vonatkozó rendelkezések

Ha az adatkezelést a DIM nevében más végzi, a DIM kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciát nyújtanak az adatkezelés GDPR követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

Az adatfeldolgozó által végzett adatkezelés vonatkozásában a DIM és az adatfeldolgozó szerződést kötnék, mely az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint a vállalkozás kötelezettségeit és jogait határozza meg.

Ezen szerződés tartalmazza az alábbiakat:

Az adatfeldolgozó

- a személyes adatokat kizárólag a DIM írásbeli utasítása alapján kezeli,
- biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak,
- alkalmazza legalább a vállalkozás által előírt szintű adatbiztonsági fentebb említett feltételeket,
- az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti a DIM-et abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében,
- segíti a DIM-et az adatvédelmi incidens szerinti kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat,
- vállalja, hogy a nála bekövetkező adatvédelmi incidens esetén haladéktalanul tájékoztatja a DIM-et,
- az adatkezelési szolgáltatás nyújtásának befejezését követően a DIM döntése alapján minden személyes adatot töröl vagy visszajuttat a DIM-nek és törli a meglévő másolatokat.

2.12. Adatvédelmi incidens

Amennyiben bármely foglalkoztatott tudomására jut, hogy személyes adatok jogosulatlan kezelésére, továbbítására, nyilvánosságra hozatalára, azaz adatvédelmi incidensre került, vagy kerülhetett sor, haladéktalanul tájékoztatnia kell az adatkezelő részleg vezetőjét, a rendszergazdát és az adatvédelmi tisztviselőt. Az adatkezelő amennyiben az incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve, akkor az érintettet haladéktalanul, a Hatóságot a tudomásszerzést követően 72 órán belül tájékoztatja. Az adatvédelmi incidenst nem kell bejelenteni, ha valószínűsíthető, hogy az nem jár kockázattal az érintettek jogainak érvényesülésére.

Ha az adatkezelő a bejelentési kötelezettségét akadályoztatása miatt határidőben nem teljesíti, akkor a bejelentéshez mellékelni kell a késedelem okát feltáró nyilatkozatot is.

A bejelentési kötelezettség keretei között az adatkezelő

- ismerteti az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek körét és hozzávetőleges számát, valamint az incidenssel érintett adatok körét és hozzávetőleges számát;
- tájékoztatást nyújt az adatvédelmi tisztviselő nevééről és elérhetőségéről;
- ismerteti az adatvédelmi incidensből eredő következményeket;

- ismerteti az adatvédelmi incidens kezelésére tett vagy tervezett – az adatvédelmi incidensből eredő esetleges hátrányos következmények mérséklését célzó és egyéb intézkedéseket;

Ha a fent felsoroltak közül valamely információ a bejelentés időpontjában nem áll az adatkezelő rendelkezésére, azzal az adatkezelő a bejelentést annak benyújtását követően utólag – az információ rendelkezésre állásáról való tudomásszerzését követően haladéktalanul – kiegészíti.

A bejelentési kötelezettségre az adatkezelő az adatvédelmi tisztviselőt jelöli ki.

A bejelentési kötelezettséget az adatvédelmi tisztviselő a Hatóság által e célra biztosított elektronikus felületén teljesíti, a www.naih.hu weboldalon, az ott e célra rendszeresített nyomtatvány elektronikus kitöltésével.

A vizsgálati jelentésben szereplő adatokat, az adatvédelmi incidens nyilvántartásában is rögzíteni kell (7. számú melléklet). Amennyiben az adott évben nem történt adatvédelmi incidens, akkor áthúzva, dátummal és az adatvédelmi tisztviselők aláírásával nyilvántartást le kell zárni.

2.13. Munkára alkalmas állapot vizsgálata

A DIM székhelyén és valamennyi telephelyén a munkavállaló csak biztonságos munkavégzésre alkalmas állapotban, a munkavédelemmel kapcsolatos utasítások és előírások betartásával tartózkodhat és végezhet munkát. A munkavállaló köteles a munkatársaival együttműködni, és munkáját úgy végezni, hogy az mások, vagy saját testi épségét ne veszélyeztesse.

A DIM székhelyén és valamennyi telephelyén tilos a munkavállalóknak alkoholos befolyásoltság, vagy egyéb tudatmódosító szer hatása alatt tartózkodniuk. Ezen tudatmódosító szerek hatása alatt a munkaképesség nem biztosítható. A munkáltató ellenőrizheti, hogy a munkavállalók betartják-e az alkoholfogyasztás tilalmával kapcsolatos szabályokat. A munkáltató ellenőrzési gyakorlata nem járhat az emberi méltóság megsértésével.

3. Informatikai biztonság

A szabályozás célja, jelen szabályzat bevezetőjében foglaltakon túl:

- a titok-, munka, vagyon- és tűzvédelemre vonatkozó intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése, (adatvédelmi incidens megakadályozása)
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig, kiterjed:

- a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- a DIM tulajdonában lévő, illetve az általa bérlet valamennyi informatikai berendezések, valamint a gépek műszaki dokumentációira is,
- az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- a rendszer - és felhasználói programokra,
- az adatok felhasználására vonatkozó utasításokra,
- az adathordozók tárolására, felhasználására
- az otthoni munkavégzés szélesebb körben történő alkalmazásával az otthoni, privát hálózatra és az informatikai munkaeszközöknek a DIM, mint munkáltató érdekében történő használatára is.

3.1. Az informatikai rendszer védelme

A védelem kiterjed:

- a rendszer elemeinek elhelyezésére szolgáló helyiségekre,
- az alkalmazott hardver eszközökre és azok működési biztonságára,
- az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
- az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerekre, valamint feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírászerű felhasználására, reprodukálhatóságára,
- a személyhez fűződő és vagyoni jogokra.

A védelem eszközei: A mindenkor technikai fejlettségének megfelelő műszaki, szervezeti, programozási, jogi intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

3.2. Biztonsági osztály, a védelmet igénylő adatok hozzáférési jogosultsága

A DIM a 2. biztonsági osztályba tartozik, általános informatikai feldolgozást végez, személyes adatokat is kezel, ezáltal azok is sérülhetnek. A 41/2015.(VII.15.) BM rendelet szerinti, a biztonsági szinthez tartozó követelmények jelen szabályzatban átvezetésre kerültek.

Az adatok feldolgozásakor meg kell határozni munkakörönként az egyes adatkezelésre és adatfeldolgozásra alkalmas programok hozzáférési jogosultságát. A hozzáférési jogosultságokat munkakörönként jelen szabályzat 5. számú melléklete tartalmazza. Az

adatvédelemmel kapcsolatos követelményeket az éves ismétlő oktatás során, valamint az új dolgozóval belépéskor ismertetni kell.

Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

3.3. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

Környezeti infrastruktúra okozta ártalmak

Elemi csapás: földrengés, árvíz, tűz, villámcsapás stb.

Környezeti kár: légszennyezettség, nagy teljesítményű elektromágneses térerő, elektrosztatikus feltöltődés, a levegő nedvességtartalmának felszökése vagy leesése, piszkolódás (pl.: por).

Közüzemi szolgáltatásba bekövetkező zavarok: feszültség-kimaradás, feszültség-ingadozás, elektromos zárlat, csőtörés.

Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás: behatolás az informatikai rendszerek környezetébe, illetéktelen hozzáférés (adat, eszköz), adatok-eszközök eltulajdonítása, rongálás (gép, adathordozó), megtevesztő adatok bevitele és képzése, zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás: figyelmetlenség (ellenőrzés hiánya), szakmai hozzá nem értés, a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása, a jelszó gyakori megváltoztatásának elmulasztása, a megváltozott körülmények figyelmen kívül hagyása, illegális másolattal vírusfertőzött adathordozó behozatala, biztonsági követelmények és gyári előírások be nem tartása, adathordozók megrongálása (rossz tárolás, kezelés), a karbantartási műveletek elmulasztása.

3.4. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

Tervezés és előkészítés során előforduló veszélyforrások:

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
- hibás adatrögzítés,
- adatelőkészítés,
- az ellenőrzési szempontok hiányos betartása.

A rendszerek megvalósítása során előforduló veszélyforrások:

- hibás adatállomány működése,
- helytelen adatkezelés,
- programtesztelés elhagyása.

A működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság,
- szervezetlenség,
- képzetlenség,

- szándékos elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

3.5. Az informatikai eszközök környezete, azok védelme

A szerverszoba minimális igénye

- a szerverszobát a legbiztonságosabb, legvédelettebb területre kell telepíteni,
- a lehető legkevesebb nyílászáróval kell rendelkeznie,
- váratlan áramkimaradás esetén a szerver(ek)e)t intelligens UPS – sel ellátni (szünetmentes tápegységgel), mellyel az áramkimaradás folyamatosságát biztosítani lehet,
- tűzvédelem,
- hűtés.

Egyéb vagyonvédelmi előírások

- a szerverszobát biztonsági zárral kell felszerelni,
- a szerverszobába való be – és kilépés rendjét szabályozni kell,
- csak az illetékes dolgozók tartózkodhatnak a szerverszobában,
- a szerverszoba kulcsának felvétele illetve leadása csak aláírás ellenében történhet,
- a munkaidőn túl a szerverszobában csak engedéllyel lehet dolgozni,
- a számítógépek monitorait úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- a szerverszobába történő illetéktelen behatolás tényét az igazgatónak azonnal jelenteni kell,
- az informatikai eszközöket csak a kijelölt dolgozók használhatják,
- az informatikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

Adathordozók

- könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni,
- a használni kívánt adathordozót (CD, DVD, pendrive) a tárolásra kijelölt helyről kell kivinni és oda kell vissza is helyezni,
- a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,
- adathordozót az intézményből kiadni csak szervezeti egységvezetői engedéllyel szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

Vírusvédelem

A szerverek és munkaállomások vírusvédelmére az alábbi szabályokat kell betartani:

- minden munkaállomásra és szerverre vírusellenőrző szoftvert kötelező telepíteni,
- a vírusellenőrző programnak minden újonnan érkezett állománnyal kapcsolatos fájlművelet esetén meg kell vizsgálni az adathordozó tartalmát. Ha adathordozón a vírusellenőrző program vírust talált, nem engedhet másolást, futtatást, amíg a vírusoktól nem mentesítik az adathordozót.

- biztosítani kell a vírusvédelmet ellátó programok, valamint a vírusok adatait tartalmazó állományok rendszeres gyártó által kibocsátott verziók telepítésével történő mielőbbi frissítését,
- a felhasználók részéről **tilos** a vírusellenőrző szoftver beállításainak módosítása.

Tűzvédelem

A szerverszoba mérsékelt tűzveszélyes üzemet jelent.

A tűzvédelem feladatait, sajátos előírásokat a szerverszobára vonatkozóan a Központi tűzvédelmi szabályzat tartalmazza.

A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.

A DIM azon helyiségeiben, ahol informatikai eszközöket használnak vagy tárolnak, a bejárat előtt min. 1 db 5 kg-os CO2 tűzoltó készüléket kell elhelyezni.

Az informatikai eszköz elhelyezésére szolgáló helyiségben elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.

A szerverszobában dohányozni **tilos!**

A szerverszobában, valamint a munkaállomásoknál ételt, italt fogyasztani **tilos!**

3.6. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

A számítógépek és szerverek védelme

Elemi csapás (vagy más ok) esetén a számítógépekben, vagy a szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- új adatfeldolgozás, helyiségek kialakítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell.

A működési biztonság megóvását **jelenti** a szükséges alkatrészek beszerzése.

Az üzemeltetés, karbantartás és szervizelés rendjét a Beszerzési Szabályzat szabályozza.

A karbantartási munkákat **tervezetten**, körültekintően és gondosan kell elvégezni.

A munkák szervezésénél **figyelembe** kell venni:

- a gyártó előírásait, ajánlásait,
- a tapasztalatokat,
- a hardver tesztek által **feltárt** hibákat.

Alapgép szétbontását (kivéve a **garanciális** gépeket) csak a rendszergazda végezheti el.

Az informatikai feldolgozás folyamatának védelme

Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- tesztelt adathordozóra lehet adatállományt rögzíteni,
- a bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
- az adatrögzítés szoftver **védelme**, lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek **ellenőrző** funkciókkal és biztosítják a rögzített tételek visszakeresésének és **javításának** lehetőségét is,
- hozzáférési lehetőség:
 - a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz (alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá)
 - az adatok **bevitele** során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a **személy** nem végezheti.

A szerver(ek) rendszergazda jelszavát és az operációs rendszerek rendszergazda jelszavát lezárt borítékban, zárható szekrényben kell tárolni. A boríték felbontására a műszaki igazgatóhelyettes intézkedhet, ennek tényét dokumentálni kell.

Mentések, file-ok védelme

Az informatikában a legnagyobb értéket a számítógépen tárolt adatok jelentik. Ezek védelmében meghatározó jelentőségű a biztonsági másolatok készítése.

A mentések folyamata:

- A mentéseket naponta, központi mentő szoftverrel kell végrehajtani.
- A mentések végrehajtásának ellenőrzéséről azon szervezeti egység vezetője köteles gondoskodni, ahová az **adott** program telepítésre, használatra került. A mentések végrehajtását a rendszergazda felé, a szervezeti egység vezetője jelezni köteles.
- A mentésből a **rendszerek**, a szoftverkörnyezet beállításainak, valamint a tárolt adatoknak teljes körűen visszaállíthatónak kell lennie a mentés pillanatának állapotára.
- A szerverek estében az adatokat 1 példányban kell menteni, és mástól fizikailag elkülönült helyiségben **elzárt**, a szerverterem tűzterétől elkülönülő térben, tűzbiztos helyen kell tárolni.
- A szerverek mentésére **napi** különbözeti, valamint hétfélig teljes rendben kerül sor. A hálózati aktív eszközökét a **beállítás** változtatásakor kell elvégezni.
- A mentett adatokhoz csak az arra jogosultak férhetnek hozzá.

Az egyéb mentéseket meghatározott időszakonként el kell végezni.

A munkák során létrehozott **dokumentumok** mentése archiválás céljából az azt létrehozó munkatársak (felhasználók) **feladata**.

A Polisz Komplex Integrált Gazdálkodási és Ügyviteli rendszer (továbbiakban: Polisz) fejlesztő szolgáltató szerverén található, **ezért** annak mentése a szolgáltató feladata az alábbiak:

- a személyi anyagok **adatállománya**
- a főkönyvi könyvelés és a hozzá kapcsolódó kötelezettségvállalás, számlázó, pénztár, tárgyi eszköz, készlet **adatai**,
- az iktatórendszer **adatállománya**,
- az étkeztetés **adatállománya**.

A levelezések, a felhasználó gépén tárolt anyagok mentését kérésre a rendszergazda végzi el.

Szoftver védelem

Operációs rendszerek védelme

A hálózati informatikusnak biztosítani kell, hogy a szerverek operációs rendszere naprakész állapotban legyen és a hálózati megosztások, könyvtárak mindig hozzáférhetőek legyenek a felhasználók számára.

Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.

Minden felhasználónak jelszóval kell védenie a programját. Ezeket a jelszavakat illetéktelen személyektől gondosan védeni kell.

Gondoskodni kell arról, hogy a tárolt programok, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek.

A programokról nyilvántartást kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:

- a program azonosítója,
- a program készítőjének neve,
- a feldolgozási rendszer megnevezése.

A program dokumentáció a rendszerdokumentációnak része. A DIM-nél használt programokat a 6. számú melléklet tartalmazza. Az alkalmazott, személyes adatok kezelésére, feldolgozására alkalmas programokra vonatkozó szerződéseket, adatkezelésre, feldolgozásra vonatkozó, a szolgáltató által kötelezően meghatározott nyilatkozatot, szerződést jelen szabályzat függelékében el kell helyezni.

Programok megőrzése, nyilvántartása

- a programokról naprakész nyilvántartást kell vezetni,
- a nyilvántartásból egyértelműen megállapítható legyen a program azonosítására és kezelésére vonatkozó adatok.

A programok nyilvántartásáért és működőképes állapotban való tartásáért a rendszergazda a felelős.

Programok fizikai védelme

A védelem érdekében a felhasználás helyétől elkülönítetten, behatolástól védetten egy-egy duplikált példányt kell tárolni az alkalmazott programok telepítő készletéből.

3.7. Központi számítógépek és a hálózat munkaállomásainak működésbiztonsága

Központi gépek (Server)

Szünetmentes áramforrást kötelező használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.

A központi gépek háttértár adatairól folyamatos biztonsági mentést kell készíteni. A mentéseket heti egy alkalommal külső adattároló egységre kell másolni. Minden év elején az előző évben keletkezett és archiválandó dokumentumokat menteni kell, külső adattárolóra. Az így keletkezett mentéseket 5 évig meg kell őrizni.

Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.

A vásárolt, egyedi fejlesztésű, szoftver eszközökről biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag el kell különíteni.

Munkaállomások (USER-ek)

A DIM-nél használatban lévő számítógépekről név és beosztás szerinti, jelen szabályzat 6. számú mellékletét képező nyilvántartást kell vezetni.

A DIM elektronikus információs rendszereihez való összes csatlakozást azonosítani és hitelesíteni kell. Különösen érzékeny és biztonságilag aggályos, ha a csatlakozási kezdeményezés olyan hálózathoz érkezik, ami kívül esik a DIM biztonsági követelmény hatókörén (otthoni munkavégzés, szolgáltatók). Belső hálózat védelme érdekében:

- technikailag kell biztosítani, hogy csak a központilag nyilvántartott munkaállomásról lehessen a rendszerekbe belépni;
- egységes munkaállomás névhasználatot kell kialakítani, a hálózatban lévő munkaállomások pontos azonosítása érdekében;
- tartományvezérelt (Active Directory) felhasználói munkaállomás használat;
- kívülről csak biztonságos csatornán (VPN) keresztül történhet feladatvégzés.

A hálózatra idegen programot, adatot másolni csak a rendszergazda és a hálózati informatikus közreműködésével lehet.

A hálózaton a részleg valamennyi munkatársa által használt adatok, kimutatások, összesítők hozzáférhetősége, megismerése érdekében külön meghajtó áll rendelkezésre, jele: X.

A személyes adatok védelme érdekében a meghajtó használatára vonatkozó szabályok:

- a meghajtón a hálózati informatikus által részlegenként létrehozott, mappákban lehet anyagokat elhelyezni;
- a részlegenként létrehozott mappákhoz csak a részleg munkatársai férhetnek hozzá;
- a létrehozott részleg mappában új mappa kialakítására csak a részlegvezetőnek van jogosultsága;
- a részlegmappába anyagokat csak a részlegvezető engedélyével lehet elhelyezni;
- a meghajtó „gyökerében” csak a hálózati informatikus hozhat létre további mappát, a szervezeti egységvezetők kérésére, amely mappa hozzáférési, módosítási javaslatait az egységvezetőnek meg kell határozni;
- a meghajtón a közérdekű, mindenki által hozzáférhető mappában a szervezeti egységvezetők és a titkárnők helyezhetnek el anyagokat, kizárólag olyan anyagokat, amelyek személyes adatokat nem tartalmaznak (pl. szabályzatok, körlevelek, utasítások, stb.);
- magánjellegű anyagokat a meghajtón szigorúan tilos elhelyezni!

- valamennyi mappához a hozzáférést biztosítani kell: az igazgató, a szervezeti egységvezetők, valamint a belső ellenőrzés részére.

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal, különös tekintettel abban az esetben, ha az egy külső, fizikai adathordozón érkezik (Külső háttértárak: CD, DVD lemez, USB flashdrive, vagy disc).

Vírusfertőzés gyanúja esetén a rendszergazdát azonnal értesíteni kell.

A számítógépeken a biztosított vírusirtó program futtat, azokra más vírus irtót telepíteni tilos. Vírusmentesítő programot futtatni csak a rendszergazda felügyelete mellett szabad.

Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.

A DIM informatikai eszközeiről programot illetve adatállományokat másolni jogos belső felhasználói igények kielégítésein kívül nem szabad.

A hálózati vezeték és egyéb csatlakozó elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.

Az informatikai eszközt és tartozékait helyéről elvinni a rendszergazda tudta és engedélye nélkül nem szabad.

A munkaállomások tekintetében az alábbi rendelkezéseket is be kell tartani:

- A munkaállomások nincsenek jól védhető helyen, ezért védelmükről szoftveres úton gondoskodni kell.
- Ha a felhasználó napközben magára hagyja a gépet, zárolást, vagy jelszavas képernyővédőt kell alkalmaznia.
- Ha a felhasználó munkaviszonya megszűnik, akkor felhasználói azonosítóját meg kell szüntetni.

A munkaállomások (számítógépek) fellelhetőségét, nyilvántartási számát, szervezeti egységeknél alkalmazott programokat a 6. számú melléklet tartalmazza.

Internet hozzáféréssel kapcsolatos intézkedések

- Minden munkaállomás internetes kapcsolattal is rendelkezik.
- Az internetes gépen minden esetben működtetni kell a vírusvédelmet.
- A vírusok és az illetéktelen hozzáférések miatt tűzfalat kell konfigurálni.
- A tűzfal működése közben keletkező állományokat az üzemeltetőnek rendszeresen ellenőrizni kell.
- A dolgozók részére történő internetes hozzáférhetőséget, azon való keresés kiterjesztést a munkaköri feladatok végrehajtása érdekében kell az egyes beosztásokban biztosítani.

A hálózatra történő csatlakozás ellenőrzése:

- Felhasználói munkaállomásokról (asztali és mobil), kizárólag csak biztonságos beléptetési folyamat után lehet elérni a DIM hálózati erőforrásait.
- A DIM számítógép-hálózata kizárólag a DIM által meghatározott tartományos rendszer szerint működhet.
- Nem csatlakozhat olyan **munkaállomás** a hálózatra, ami:
 - nem megbízható **hálózati** kapcsolattal rendelkezik;
 - nem tagja a megfelelő DIM.LOCAL tartománynak;
 - nem rendelkezik naprakész vírusvédelmi megoldással.

4. A közérdekű adatok megismerésére irányuló kérelmek intézésének ügymenete, továbbá a kötelezően közzéteendő adatok nyilvánosságra hozatalának szabályai

A szabályozás rendelkezéseit kell alkalmazni a DIM kezelésébe lévő közérdekű adatok, közérdekből nyilvános adatok, valamint közalkalmazottainak, munkavállalóinak közérdekből nyilvános adata (továbbiakban együtt: közérdekű adat) igénylésénél, továbbá hatásköre és illetékessége szerint kezelésében álló közérdekű adatok közzétételénél.

4.1. A közérdekű adatok megismerésére irányuló kérelmek intézésének ügymenete

Az igény benyújtása

A közérdekű adat megismerése iránt bárki

- szóban,
- írásban vagy
- elektronikus úton

igényt nyújthat be.

Az igény benyújtásának helye és módja

- Szóbeli igények benyújtása
Személyesen a DIM Debrecen, Kálvin tér 2/A szám alatti székhelyén a titkárságon, a Szervezeti és működési szabályzatban szabályozott ügyfélfogadási időben.
- Írásbeli igények benyújtása
Az igénylő közérdekű adat megismerésére vonatkozó írásbeli igényét benyújthatja:
 - a DIM által e célra rendszeresített igénybejelentő lapon (3. sz. melléklet)
 Személyesen a DIM Debrecen, Kálvin tér 2/A szám alatt a titkárságon benyújtva.
 Postai úton az intézmény igazgatójának címzett levélben.
 Elektronikus úton az info@diminfo.hu e-mail címre küldött levélben történhet.

A benyújtott igények teljesítése

A közérdekű adat megismerésére irányuló igények teljesítéséről az intézmény igazgatója, gazdasági adatok vonatkozásában a gazdasági igazgató gondoskodik.

A szóban előterjesztett igényt akkor lehet szóban teljesíteni, ha

- az igénylő szóban kéri a választ, illetve az számára kielégítő,
- az igényelt adat más módon jogszerűen már nyilvánosságra került,
- az igényelt adat a DIM munkatársainak nevére, beosztására, hivatali elérhetőségére vonatkozik,
- az igény a DIM eljárására, hatáskörére, az alkalmazott jogszabályokra vonatkozó általános tájékoztatással teljesíthető.

Amennyiben a szóban előterjesztett igény szóban azonnal nem válaszolható meg, az igénylésről feljegyzést kell készíteni és az igénylőt tájékoztatni kell arról, hogy igényének teljesítésére írásban kerül sor. A feljegyzés elkészítése az igazgató által az adott igénynek megfelelő, kijelölt személy feladata.

Az adatigénylésnek közérthető formában és – amennyiben az aránytalan költséggel nem jár – az igénylő által kívánt technikai eszközzel, illetve módon írásban (vagy, ha az igényben elektronikus levelezési címet is közölt, úgy elektronikus úton) kell – a közérdekű adat megismerésére irányuló igénynek a tudomásra jutást követő – legrövidebb idő alatt, legfeljebb azonban 15 napon belül eleget tenni. Az adatigénylést nem lehet elutasítani arra való hivatkozással, hogy annak közérthető formában nem lehet eleget tenni.

Ha az adatigénylés jelentős terjedelmű, illetve nagyszámú adatra vonatkozik, az előző bekezdésben meghatározott határidő egy alkalommal 15 nappal meghosszabbítható. Erről az igénylőt az igény kézhezvételét követő 15 napon belül tájékoztatni kell.

Az igény teljesítésének megtagadásáról, annak indokaival együtt 15 napon belül írásban vagy – amennyiben az igényben elektronikus levelezési címét közölte – elektronikus úton értesíteni kell az igénylőt. Az értesítésben tájékoztatni kell az igénylőt arról, hogy – az igényének nem teljesítése miatt – bírósághoz fordulhat.

A közérdekű adat megismerése iránti igény teljesítése nem tagadható meg azért, mert a nem magyar nyelvű igénylő az igényét anyanyelvén vagy az általa értett más nyelven fogalmazza meg.

Az adatokat tartalmazó dokumentumokról vagy dokumentumrészről, annak tárolási módjától függetlenül az igénylő másolatot kaphat. A fénymásolat elkészítése annak a részlegnek a feladata, ahol az adatokat tartalmazó dokumentumot tárolják.

Ha a közérdekű adatot tartalmazó dokumentum az igénylő által meg nem ismerhető adatot tartalmaz, a másolaton a meg nem ismerhető adatot felismerhetetlenné kell tenni.

A közérdekű adatigénylésre adott válasz kiadmányozásánál a *Szervezeti és működési szabályzat* szerint kell eljárni.

4.2. A kötelezően közzéteendő adatok nyilvánosságra hozatalának szabályai

A DIM a kötelezően közzéteendő adatokat a www.diminfo.hu honlapján teszi közzé. Az adatok honlapra történő felvételéért az igazgatási részlegvezetőtől kapott anyagok alapján a rendszergazda a felelős.

A DIM kötelezően közzéteendő adatait jelen szabályzat 4. számú melléklete tartalmazza. A melléklet szerinti adatokból a részletes költségvetéssel és beszámolóval kapcsolatos nyilvánosságot úgy biztosítja, hogy azokat az előírt formában és határidőre a Magyar Államkincstár (elektronikusan) és az irányító szerv részére (elektronikusan és papír alapon) továbbítja.

Az Infotv. 71/D. § (4) bekezdésében meghatározott adatszolgáltatást a közfeladatot ellátó szervek, a helyi önkormányzatok és a köztulajdonban álló gazdasági társaságok elektronikus úton, a Hatóság által, annak honlapján közzétett módon teljesítik.

4.3. A Központi Információs Közadat-nyilvántartás felületen előírt közzétételről és az átláthatósági eljárásról

A nemzetbiztonsági szolgálatok kivételével minden költségvetési szerv köteles meghatározott gazdálkodási adatait az újonnan létrehozott Központi Információs Közadat-nyilvántartás felületén (a továbbiakban: KIF felület) kéthavi rendszerességgel közzé kell tenni. A közzététel módját és pontos tartalmát az Infotv. 37/C. §-a és a Központi Információs Közadat-nyilvántartás részletszabályairól szóló 499/2022. (XII. 8.) Korm. rendelet tartalmazza.

Az adatszolgáltatást a KIF felületről letölthető adatlapon (9. sz. melléklet) a Felhasználói Szabályzatban található útmutatók szerint kell teljesíteni. A Nemzeti Adatvédelmi és Információs Hatóság (a továbbiakban: NAV) az adatokat az adatlap beérkezését követő munkanapon a KIF felületen közzéteszi.

Amennyiben egy költségvetési szerv a KIF felületen közzétételi kötelezettségét nem teljesítette vagy a közzétételre a valóságnak nem megfelelő adatokkal vagy hiányosan került sor, a Hatóság bejelentés alapján átláthatósági hatósági eljárást indít és hivatalból átláthatósági hatósági eljárást indíthat. Az átláthatósági hatósági eljárásban az ügyintézési határidő 45 nap. A Hatóság jogsértés esetén elrendeli a KIF felületen a közzétételi kötelezettség soron kívüli, de legfeljebb 15 napon belüli teljesítését. Amennyiben közzétételi kötelezettségének a költségvetési szerv 15 napon belül továbbra sem tesz eleget, a Hatóság bírságot szabhat ki.

A DIM adatszolgáltatási kötelezettségének teljesítése érdekében a gazdálkodási részleg 1. vezetője a közzétételi határidőt 2023.február 28-tól kezdődően minden második hónap utolsó napja) megelőzően 5 nappal az elkészített adatszolgáltatást megküldi a felelős gazdálkodási részlegvezetőnek ellenőrzésre, valamint ezt követően a gazdasági igazgatónak, a közzététel

hivatali kapun történő továbbítása érdekében. Ezzel egyidejűleg a gazdálkodási részleg 1. vezetője az adatszolgáltatás igazgatási részlegvezetőnek történő megküldéssel gondoskodik a DIM honlapján történő megjelenéséről.

III. Záró rendelkezések

A szabályzatot készítette: Papp Attila és Veresné Horog Éva adatvédelmi tisztviselők.

Jelen szabályzat 2024. március 1-jén lép hatályba és egyidejűleg minden korábbi e tárgykörben kiadott szabályozás hatályát veszti. A szabályzat egy eredeti példányban készült, mely a DIM titkárságán kerül elhelyezésre.

A szabályzat felülvizsgálata és aktualizálása a jogszabályi és személyi változások függvényében történik. Az aktualizálásért az adatvédelmi tisztviselők a felelősek, a szabályzatot az igazgató hagyja jóvá.