Gönczy Pál Utcai Óvoda

Adatvédelmi, adatkezelési, informatikai biztonsági szabályzata

Stefánine Máté Zsófia Irén
igazgató

Tartalomjegyzék

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 Gönczy Pál Utcai Óvoda (továbbiakban Óvoda) jelen szabályzata az Európai Parlament és a Tanács 2016/679. rendelete (GDPR rendelet) és az Infotv. rendelkezéseinek megfelelően készült. Jelen szabályzat információ biztonsági szabályozása során a 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.

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 továbbá, hogy meghatározza az informatikai rendszer adatbiztonsági követelményeinek érvényesülésével, a hardver s szoftver védelemmel kapcsolatos szabályokat és eljárásrendeket. Jelen szabályzat rendelkezéseit az Óvoda alábbi szabályzatain át kell vezetni:

- Szervezeti és Működési Szabályzat
- Iratkezelési Szabályzat

Jelen szabályzat hatályba lépésével rendelkezéseit az Óvoda valamennyi munkaköri leírásán át kell vezetni.

I. ADATVÉDELEM, ADATKEZELÉS

I.1. Általános adatvédelmi és adatkezelési szabályok

I.1.1. A szabályzat hatálya

Jelen szabályzat hatálya kiterjed a Gönczy Pál Utcai Óvodára (továbbiakban Óvoda) mint intézményre, valamint az általa foglalkoztatott vezetőkre, munkavállalókra, az Óvoda minden adatkezelésére és adatfeldolgozására,

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

Az Óvoda által kezelt, valamint a nem saját nyilvántartásban szereplő személyes adatokat tartalmazó adattovábbításokra jelen szabályzat 1. számú melléklete szerinti nyilvántartást kell vezetni. A nyilvántartást minden év december 31-i hatállyal le kell zárni.

I.1.2. A szabályzat célja

A szabályzat célja, hogy biztosítsa a személyes adatok alaptörvény szerinti védelmének érvényesülését, az információs önrendelkezés megvalósulását, továbbá, hogy az Óvoda által kezelt személyes adatok tekintetében meghatározza az adatkezelés során irányadó adatvédelmi és adatbiztonsági szabályokat.

I.1.3. 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.)
- 20/2012. (VIII. 31.) EMMI rendelet a nevelési-oktatási intézmények működéséről és a köznevelési intézmények névhasználatáról,
- 15/2013. (II.26.) EMMI rendelet a pedagógiai szakszolgálati intézmények működéséről,
- 2011. évi CXC. törvény a nemzeti köznevelésről,
- 328/2011. (XII.29.) Korm. rendelet a személyes gondoskodást nyújtó gyermekjóléti alapellátások és gyermekvédelmi szakellátások térítési díjáról és az igénylésükhöz felhasználható bizonyítékokról,
- 2012. évi I. törvény a munka Törvénykönyvéről,
- 2023. évi LII. törvény a pedagógusok új életpályájáról,
- 419/2024 (XII.23.) Korm. rendelet a pedagógus-továbbképzésről, a pedagógus-szakvizsgáról, valamint a továbbképzésben részt vevők juttatásairól és kedvezményeiről,

- 33/1998. (VI. 24.) NM rendelet a munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről,
- 1993. évi XCIII. törvény a munkavédelemről,
- 1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról,
- 217/1997. évi (XII.01.) kormányrendelet a kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény végrehajtásáról,
- 5/1993. (XII. 26.) MüM rendelet a munkavédelemről szóló 1993. évi XCIII. törvény egyes rendelkezéseinek végrehajtásáról.

I.1.4. Értelmező rendelkezések

- **GDPR** (General Data Protection Regulation) az Európai Unió új Adatvédelmi Rendelete (Európai Parlament és a Tanács (EU) 2016/679 rendelet);
- **érintett:** bármely információ alapján azonosított vagy azonosítható természetes személy;
- **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;
- **személyes adat:** az érintettre vonatkozó bármely információ;
- **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;
- **hozzájárulás:** az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez;
- **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.

- **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;
- **adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
- **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;
- **adatállomány:** az egy nyilvántartásban kezelt adatok összessége;
- **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;
- **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;
- **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;

I.2. Személyes adatok védelmére vonatkozó követelmények

I.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 adatot elektronikusan törölni, a papíralapú adathordozót pedig selejtezni kell.
d) Azok a papír alapú adathordozók melyek nem selejtezhetők, az adatkezelésre jogosult személyek köre által kerül irattározásra.

- **Az adatminőség elve.** Amennyiben az Óvoda foglalkoztatottja 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.** Az Óvoda 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.

I.2.2. Az adatkezelés során alkalmazott jogalapok

- **Hozzájáruláson alapuló adatkezelés**: az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez.
- **Jogi kötelezettségen alapuló adatkezelés**: az adatkezelés az Óvodára vonatkozó jogi kötelezettség teljesítéséhez szükséges.
- **Közérdek, közhatalmi jogosítvány:** az adatkezelés közérdekű vagy az adatkezelőre átruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.

I.2.3. Az adatvagyon leltár

Az Óvoda 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 az Óvoda 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)

I.2.4. Az érintettek jogai és azok érvényesítése

Az érintetti jogokat az adott adatkezelés jogalapja határozza meg.

	Hozzájárulás	Jogi kötelezettség	Közérdek, közhatalmi jogosítvány
Tájékoztatáshoz való jog	x	x	x
Hozzájárulás visszavonásához való jog	x		
Hozzáféréshez való jog	x	x	x
Adatok módosításához, helyesbítéséhez, törléséhez való jog	x	x	x
Adatkezelés korlátozásához való jog	x	x	x
Tiltakozáshoz való jog			x
Adathordozhatósághoz való jog	x		
Jogorvoslathoz való jog	x	x	x

I.2.5. Az adatkezelés általános feltételei

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 fen 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.

Az Óvoda minden adatkezelést végző alkalmazottja büntetőjogi felelősséggel tartozik a személyes adatok jogszerű kezeléséért.

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 Nemzeti Adatvédelmi és Információszabadság Hatóság kérésére a rendelkezésére bocsátja.

I.2.6. Az adatkezelés típusai

Az Óvoda 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.

I.2.7. Az adatkezelésre jogosultak köre és feladatai

Igazgató feladatai:

- felelős az Óvoda adatkezelésének jogszerűségéért;
- gondoskodik az adatkezelés személyi és tárgyi feltételeinek biztosításáról;
- az Óvoda, mint adatkezelő tekintetében meghozza az adatkezelésre vonatkozó döntéseket;
- a személyes adatok továbbítása a jóváhagyásával történhet.
- ellenőrzi a védelmi előírások betartását;
- kialakítja a védelmi eszközök alkalmazására vonatkozó döntés előkészítése érdekében a szakterületek bevonásával a biztonságot növelő intézkedéseket;
- felelős az informatikai rendszerek üzembiztonságáért, biztonsági másolatok készítéséért és karbantartásáért;
- feladata az informatikai eszközök, szoftverek, védelmi eszközök működésének, szervíz ellátás biztosítása, folyamatos ellenőrzése;
- jelen szabályzatot a Szervezeti és Működési Szabályzattal összeegyeztetni;
- a védelmi rendszer érvényesülésének ellenőrzése;
- a vezetése alatt álló dolgozók vonatkozásában jelen szabályzat előírásainak betartatása, annak ellenőrzése;
- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet;
- megszervezi a jelen szabályzat rendelkezéseire történő oktatást;
- 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 melléklete szerinti Adatkezelési és számítógépes felhasználói nyilatkozatban foglaltakat aláírni, az abban foglaltakat betartani és betartatni.
- gondoskodik jelen szabályzat végrehajtásához szükséges eszközök fedezetének rendelkezésre állásáról;

- az adatvédelmi tisztviselővel egyeztetve gondoskodik jelen szabályzat rendelkezéseinek munkaköri leírásokon történő átvezetéséről;
- vezeti az adattovábbítások nyilvántartását, jelen szabályzat 1. számú melléklete alapján;
- vezeti az Óvoda részére beadott, állásra jelentkezők önéletrajzának 6. 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;
- gondoskodik a jelen szabályzat 2. számú mellékletében foglalt Adatkezelési és számítógépes felhasználói nyilatkozat dolgozók részéről történő aláírásáról, valamint az aláírt nyilatkozat személyi anyagban történő elhelyezéséről;

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 közzéteendő 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 5. sz. mellékletében foglalt nyilvántartó lap használatával;
- elkészíti jelen szabályzatot, gondoskodik annak aktualizálásáról;
- 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.

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

- 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 melléklete szerinti Adatkezelési és számítógépes felhasználói nyilatkozatban foglaltakat aláírni, az abban foglaltakat betartani és betartatni.

I.2.8. Adatkezelési tevékenységek nyilvántartása

Az adatkezelési tevékenységek nyilvántartását az Óvoda az elszámoltathatóság elvéből következően annak érdekében végzi, hogy a GDPR-nak való megfelelést nyomon tudja követni és igazolni tudja.

A nyilvántartásokat az Óvoda írásban vezeti, papíralapon vagy elektronikus formátumban.

I.2.9. Az adatfeldolgozó igénybevételére vonatkozó rendelkezések

Ha az adatkezelést az Óvoda nevében más végzi, az Óvoda 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 az Óvoda és az adatfeldolgozó szerződést kötnek, 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 az Óvoda 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 az Óvodát abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében,
- segíti az Óvodát 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 az Óvodát,

- az adatkezelési szolgáltatás nyújtásának befejezését követően az Óvoda döntése alapján minden személyes adatot töröl vagy visszajuttat az Óvodának és törli a meglévő másolatokat.

I.2.10. 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 Óvoda igazgatóját és az adatvédelmi tisztviselőket. Az adatkezelő amennyiben az incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve, akkor az érintettet haladéktalanul, a hatóságot (NAIH) 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 nevéről 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 (5. számú melléklet).

II. INFORMATKAI 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,
- kiterjed az Óvoda tulajdonában lévő valamennyi informatikai berendezésekre,
- kiterjed a rendszer - és felhasználói programokra,
- kiterjed az adatok felhasználására vonatkozó utasításokra,
- kiterjed az adathordozók tárolására, felhasználására.

II.1. Az informatikai rendszer védelme

A védelem kiterjed:

- a rendszer elemeinek elhelyezésére szolgáló helyiségekre,
- az alkalmazott hardver eszközökre és azok működési biztonságára,
- az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,

- az adatfeldolgozó programrendszerekre, valamint feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,
- a személyhez fűződő és vagyoni jogokra.

A védelem eszközei: A mindenkori 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.

II.2. A védelmet igénylő adatok hozzáférési jogosultsága

Az Óvoda általános informatikai feldolgozást végez, személyes adatokat is kezel, ezáltal azok is sérülhetnek.

Az adatok feldolgozásakor meg kell határozni munkakörönként az egyes adatkezelésre és adatfeldolgozásra alkalmas programok hozzáférési jogosultságát. A hozzáférési jogosultságokat munkakörönként jelen szabályzat 3. számú melléklete tartalmazza. A kijelölt dolgozók előtt az adatvédelmi és egyéb szabályokat, jelen szabályzat tartalmának oktatása során a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.

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

II.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, feszültségingadozás, elektromos zárlat, csőtörés.

- **Emberi tényezőre visszavezethető veszélyek**

Szándékos károkozás: behatolás az informatikai rendszerek környezetébe, illetéktelen hozzáférés (adat, eszköz), adatok-eszközök eltulajdonítása, rongálás (gép, adathordozó), megtévesztő 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.

II.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 működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság,
- szervezetlenség,
- képzetlenség,
- szándékos elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

II.5. Az informatikai eszközök környezete, azok védelme

Vagyonvédelmi előírások

- váratlan áramkimaradás esetén a szerver(eke)t intelligens UPS – sel ellátni (szünetmentes tápegységgel), mellyel az áramkimaradás folyamatosságát biztosítani lehet,
- tűzvédelem,

- hűtés,
- a számítógépek monitorait úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- 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,
- a használni kívánt adathordozót (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 igazgatói 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 menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.

Az Óvoda 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 munkaállomásoknál ételt, italt fogyasztani tilos!

II.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.

A karbantartási munkákat tervezetten, körültekintően és gondosan kell elvégezni.

A munkák szervezésénél figyelembe kell venni:

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

Alapgép szétbontását (kivéve a garanciális gépeket) csak az informatikus 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 személyek férjenek hozzá)
    - az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

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 meghatározott időszakonként el kell végezni.
- A mentések végrehajtásának ellenőrzéséről az igazgató köteles gondoskodni, ahová az adott program telepítésre, használatra került.
- A mentésből a rendszerek, a szoftverkörnyezet beállításainak, valamint a tárolt adatoknak teljes körűen visszaállíthatónak kell lennie a mentés pillanatának állapotára.
- A mentett adatokhoz csak az arra jogosultak férhetnek hozzá.
- A munkák során létrehozott dokumentumok mentése archiválás céljából az azt létrehozó munkatársak (felhasználók) feladata.
- A levelezések, a felhasználó gépén tárolt anyagok mentését az informatikus végzi el.

Szoftver védelem

Operációs rendszerek védelme

Az informatikusnak biztosítani kell, hogy a szerverek operációs rendszere naprakész állapotban legyen és a hálózati megosztások, könyvtárak mindig hozzáférhetők 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. Az Óvodánál használt programokat az 4. számú melléklet tartalmazza.

Programok megőrzése, nyilvántartása

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

II.7. A munkaállomások működésbiztonsága

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

A számítógépek háttértár adatairól folyamatos biztonsági mentést kell készíteni.

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

Munkaállomások (USER-ek)
Az Óvodánál használatban lévő számítógépekről beosztás szerinti, jelen szabályzat 4. számú mellékletét képező nyilvántartást kell vezetni.
A hálózatra idegen programot, adatot másolni csak az informatikus közreműködésével lehet.

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal, különös tekintettel abban az esetben, ha az egy külső, fizikai adathordozón érkezik (Külső háttértárak: külső meghajtó, pendrive).

Vírusfertőzés gyanúja esetén az informatikust azonnal értesíteni kell.

A számítógépeken a biztosított vírusirtó program futhat, azokra más vírus irtót telepíteni tilos.

Vírusmentesítő programot futtatni csak az informatikus felügyelete mellett szabad.

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

Az Óvoda 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 nem szabad.

A munkaállomások tekintetében az alábbi rendelkezéseket is be kell tartani:
- 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.

Az Óvodánál a munkaállomások (számítógépek) fellelhetőségét, nyilvántartási számát, az alkalmazott programokat a 4. 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.

III. ZÁRÓ RENDELKEZÉSEK

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

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.

Jelen szabályzat 2026. február 1-jén lép hatályba, azzal, hogy minden korábbi, e tárgykörben történt szabályozás hatályát veszti. A szabályzat egy eredeti példányban készült, mely a Gönczy Pál Utcai Óvoda titkárságán kerül elhelyezésre.

Mellékletek

1. számú melléklet: Személyes adatokat tartalmazó nyilvántartásból történő adattovábbítás

2. számú melléklet: Adatkezelési és számítógépes felhasználói nyilatkozat

3. számú melléklet: Felhasználók hozzáférési jogosultságai, beosztás szerint

4. számú melléklet: A számítógépekre és programokra vonatkozó adatok

5. számú melléklet: Adatvédelmi incidensek nyilvántartása

6. számú melléklet: Alkalmazásra nem kerülő jelentkezők önéletrajzának nyilvántartása

Függelék

Adatkezelési tájékoztató