4959/1/2025

Fővárosi Önkormányzat Vázsonyi Vilmos Idősek Otthona

Titokvédelmi Szabályzat

1. Bevezetés

A jelen szabályzat célja, hogy a Fővárosi Önkormányzat Vázsonyi Vilmos Idősek Otthona (a továbbiakban: Intézmény) működése során egységes eljárásrendet biztosítson az üzleti titok, közadat, valamint a külső féltől származó, üzleti titokként minősített adatok kezelésére, védelmére, selejtezésére és megismerhetőségére.

2. Hatály

A jelen szabályzat személyi hatálya kiterjed az Intézmény minden foglalkoztatottjára és szerződéses partnerére. Tárgyi hatálya kiterjed az Intézményben keletkező, oda érkező, illetve onnan kimenő, üzleti titokra; a belső használatú, bizalmas és szolgálati használatú minősített adatra; közadatnak, valamint külső féltől származó, üzleti titokként minősített adatnak minősülő valamennyi adatra és dokumentumra, függetlenül azok formátumától. Időbeli hatálya a hatálybalépés napjától visszavonásig érvényes.

3. Jogszabályi alapok

A szabályzat alapját az alábbi jogszabályok releváns szakaszai képezik:

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (a továbbiakban: GDPR)
  2018 évi LIV. törvény az üzleti titok védelméről
  2011 évi CXII. törvény az információszabadságról (Infotv.)
- Polgári Törvénykönyv (2013. évi V. törvény)
  1997 évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyazonosító adatok kezeléséről és védelméről (a továbbiakban: Eüak.)
- 1/2000. (I. 7.) SzCsM rendelet a személyes gondoskodást nyújtó szociális intézmények szakmai feladatairól és működésük feltételeiről 4
- 9/1999. (XI. 24.) SzCsM rendelet a személyes gondoskodást nyújtó szociális ellátások igénybevételéről
- A 2009. évi CLV. törvény a minősített adatok védelméről csak akkor alkalmazandó, ha az intézmény felsőbb szervtől kapott vagy jogszabály alapján minősített adatot kezel.
- Bp. Főv. Önk. Közgyűlésének 17/2025. (VI.12) önkormányzati rendelete az átlátható működésről
- belső szabályzatok

4. Értelmező rendelkezések

A jelen szabályzat alkalmazásában:

- **Titok / Bizalmas információ:** Minden olyan információ, amelynek jogosulatlan hozzáférése, módosítása, nyilvánosságra hozatala vagy megsemmisítése kárt okozna a szervezetnek vagy az érintettnek. Magában foglalja az üzleti titkokat, személyes adatokat és különleges adatokat.
- **Üzleti titok:** Az Intézményben csak üzleti és annál gyengébb titok besorolás létezik. Üzleti titoknak minősülnek például az árajánlat mellékletében küldött árak, illetve

minden olyan adat, amelyet a készítő üzleti titoknak minősít.

- **Közadat:** Minden egyéb adat, amely nem minősül üzleti titoknak, közadatnak számít. Ezek az adatok alapvetően megismerhetők, mivel az Intézmény közfeladatot lát el. A közadatok közzétételéről és nyilvánosságáról külön szabályzat rendelkezik.
- **Külső féltől származó, üzleti titokként minősített adat:** Olyan adat, amelyet külső szerződő partner vagy harmadik fél üzleti titokként jelöl meg, és amelynek védelmére az Intézmény különös figyelmet fordít.
- **Személyes adat:** Azonosított vagy azonosítható természetes személyre (érintettre) vonatkozó bármely információ.
- **Különleges adat:** Fajra vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre, szakszervezeti tagságra utaló adatok, genetikai adatok, biometrikus adatok egyedi azonosítás céljából, egészségügyi adatok, vagy természetes személy szexuális élete vagy szexuális irányultságára vonatkozó adatok. Az egészségi állapotra vonatkozó adat például a különleges (szenzitív) adatok csoportjába tartozó személyes adat, amely kiemelt védelemben részesítendő.
- **Adatkezelés:** Személyes adatokon végzett bármely művelet vagy műveletek összessége, függetlenül attól, hogy automatizált eszközökkel vagy anélkül hajtják végre (pl. gyűjtés, rögzítés, rendszerezés, tárolás, módosítás, lekérdezés, felhasználás, nyilvánosságra hozatal, törlés, megsemmisítés).
- **Adatkezelő:** Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy egyéb szerv, amely önállóan vagy másokkal együtt meghatározza a személyes adatok kezelésének céljait és eszközeit.
- **Adatfeldolgozó:** Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.
- **Adatvédelmi incidens:** Olyan biztonsági esemény, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan nyilvánosságra hozatalát vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
- **Érintett:** Az azonosított vagy azonosítható természetes személy, akire a személyes adat vonatkozik.
- **Minősítő:** Az a személy, aki jogosult az adatok üzleti titokként történő minősítésére, jellemzően a készítő vagy az Intézmény vezetője.

5. Adatkezelési és titokvédelmi alapelvek

Saját működése során az intézmény nem keletkeztet üzleti titoknál magasabb besorolású dokumentumot.

Az Intézmény a személyes adatok kezelése során az alábbi alapelveket követi, összhangban a GDPR 5. cikkével:

- **Jogszerűség, tisztességes eljárás és átláthatóság:** Az adatokat jogszerűen, tisztességesen és az érintettek számára átlátható módon kell kezelni. Ez magában foglalja a világos adatkezelési tájékoztatók biztosítását az adatkezelés megkezdése előtt.
- **Célhoz kötöttség:** A személyes adatokat meghatározott, egyértelmű és jogszerű célból kell gyűjteni, és nem lehet azokkal a célokkal össze nem egyeztethető módon

továbbkezelni.

- **Adattakarékosság:** A személyes adatoknak megfelelőnek, relevánsnak és a célokhoz mérten szükségesnek kell lenniük.
- **Pontosság:** A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; a pontatlan személyes adatokat haladéktalanul törölni vagy helyesbíteni kell.
- **Korlátozott tárolhatóság:** A személyes adatokat olyan formában kell tárolni, amely az érintettek azonosítását csak addig teszi lehetővé, ameddig az adatok kezelésének céljaihoz szükséges. Az egészségügyi adatokat 50 évig, vagy bírósági eljárás esetén az ügy lezárásának időpontjáig lehet kezelni, ezt követően az adatokat meg kell fosztani a személyes azonosítás lehetőségétől.
- **Integritás és bizalmas jelleg:** A személyes adatokat olyan módon kell kezelni, amely megfelelő biztonságot garantál, beleértve a jogosulatlan vagy jogellenes kezelés, valamint a véletlen elvesztés, megsemmisülés vagy sérülés elleni védelmet, megfelelő technikai vagy szervezési intézkedések alkalmazásával.
- **Elszámoltathatóság:** Az adatkezelő felelős az elveknek való megfelelésért, és képesnek kell lennie annak bizonyítására. Ez magában foglalja az adatkezelési tevékenységek nyilvántartását. Amennyiben az adatkezelés hozzájáruláson alapul, az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult.

Ezek az alapelvek biztosítják, hogy az adatkezelés minden szakasza megfelel a jogszabályi és etikai követelményeknek. Az intézmény rendszeresen ellenőrzi, hogy az adatkezelési gyakorlat megfelel-e ezeknek az elveknek, és szükség esetén intézkedéseket vezet be a megfelelőség biztosítására. Az intézmény mindent megtesz annak érdekében, hogy a gondozottak és a munkatársak adatai a lehető legnagyobb biztonságban legyenek.

6. Szerepek és felelősségek

6.1. Vezetői felelősség

Az Intézményvezető viseli a végső felelősséget az adatvédelmi és titoktartási szabályozásoknak való megfelelés biztosításáért. Az intézményvezetőnek szabályoznia kell az intézményben foglalkoztatottak, valamint az intézményi ellátást igénybe vevő ellátottak adatvédelmével, adatbiztonságával kapcsolatos feladatokat, és jóvá kell hagynia a belső adatvédelmi és adatbiztonsági szabályzatot. Feladata továbbá, hogy folyamatosan ellenőrizze és figyelemmel kísérje, hogy az intézményben történő adatkezelés megfelel-e a jogszabályokban, valamint a belső dokumentumokban meghatározott szabályoknak.

6.2. Adatvédelmi tisztviselő (DPO[1]) feladatai és szerepe

Az Intézmény adatvédelmi tisztviselőt (DPO) alkalmaz a személyes adatok kezelésére vonatkozó jogi előírások teljesítésének és az érintettek jogai érvényesülésének elősegítése érdekében. A DPO kinevezése kötelező, mivel az Intézmény közfeladatot lát el, és nagy számban kezel különleges adatokat.

A DPO fő feladatai a GDPR 39. cikk és a 97. preambulumbekezdés alapján a következők:

- Tájékoztatást és tanácsot ad az adatkezelőnek és a foglalkoztatottaknak a GDPR és

[1] **DPO** – Data Protection Officer, adatvédelmi tisztviselő

egyéb adatvédelmi rendelkezések szerinti kötelezettségeikről.

- Felügyeli a GDPR-nak, a belső szabályzatoknak és az adatvédelmi stratégiáknak való megfelelést, beleértve a felelősségek kiosztását, a tudatosság növelését és a foglalkoztatottak képzését.
- Tanácsot ad az adatvédelmi hatásvizsgálattal (DPIA[2]) kapcsolatban, és nyomon követi annak elvégzését.
- Együttműködik a felügyeleti hatósággal (Nemzeti Adatvédelmi és Információszabadság Hatóság - NAIH) az adatkezeléssel kapcsolatos ügyekben, és kapcsolattartó pontként szolgál feléjük.
- Kapcsolattartóként működik az érintettek számára jogaik gyakorlásával kapcsolatban.

A DPO-nak függetlenül kell működnie, és közvetlenül a legfelsőbb vezetésnek kell jelentenie. Feladatai ellátásával kapcsolatban nem kaphat utasításokat az adatkezelőtől vagy az adatfeldolgozótól. A DPO nevét és elérhetőségeit közzé kell tenni az Intézmény székhelyén és telephelyén jól látható módon, a honlapján, az adatkezelési tájékoztatókban, az adatkezelési tevékenységek nyilvántartásában, az adatvédelmi incidensek nyilvántartásában, valamint az érintett hozzáférési jogával kapcsolatos intézkedések nyilvántartásában.

6.3. Foglalkoztatottak és külső partnerek kötelezettségei

Az Intézmény valamennyi foglalkoztatottja és szerződéses partnere köteles betartani a jelen Titokvédelmi Szabályzatot és a kapcsolódó eljárásokat. Kötelesek megőrizni a munkavégzés során hozzáférhetővé vált összes bizalmas információ titkosságát, és azonnal jelenteniük kell minden biztonsági incidenst vagy gyanús jogsértést. A foglalkoztatottak a személyes adatokkal kizárólag az adatvédelmi szabályozási rendszerben meghatározott jogosultságok alapján, célból és módon kerülhetnek kapcsolatba, azokat csak a meghatározott módon kezelhetik. A külső partnereknek szerződéses kötelezettségeik vannak a Titok Szabályzat és az alkalmazandó adatvédelmi törvények betartására, és megfelelő biztonsági intézkedéseket kell bevezetniük.

6.3.1 Általános kötelezettségek

1) Minden munkavállaló köteles titoktartási nyilatkozatot aláírni.
2) A titoktartási kötelezettség a munkaviszony megszűnése után is fennáll.
3) Védendő információt csak szolgálati célra lehet felhasználni.
4) Magáncélú felhasználás szigorúan tilos.
5) A titoktartási kötelezettség teljesítését rendszeres oktatásokkal és tudatosítással kell támogatni.
6) Az új munkavállalók speciális figyelmet igényelnek a titokvédelmi kultúra elsajátítása érdekében.

6.4. Képzés és tudatosság

Kötelező, rendszeres képzést kell biztosítani minden foglalkoztatott számára a Titok Szabályzatról, az adatvédelmi elvekről és a specifikus eljárásokról. A képzések elvégzését dokumentálni kell. Az adatvédelmi tisztviselő feladatai közé tartozik, hogy gondoskodjon az adatvédelmi ismeretek oktatásáról.

7. Titok- és adatbiztonsági intézkedések

7.1. Technikai és szervezési intézkedések (TOM[3]s)

---

[2] **DPIA** – Data Protection Impact Assessment, adatvédelmi hatásvizsgálat

[3] **TOM** – Technikai és Szervezési Intézkedés (Technical and Organizational Measure) – a GDPR 32. cikk szerinti intézkedések csoportja

Az Intézmény az alábbi technikai és szervezési intézkedéseket vezeti be és tartja fenn a bizalmas információk integritásának, bizalmas jellegének és rendelkezésre állásának biztosítására:

- **Hozzáférés-szabályozás:** Robusztus hozzáférés-kezelési rendszerek bevezetése (pl. szerepalapú hozzáférés, erős hitelesítés, hozzáférési jogok rendszeres felülvizsgálata) a jogosulatlan hozzáférés elleni védelemhez.
- **Titkosítás és álnevesítés:** Titkosítás alkalmazása a tárolt és továbbított adatokra, valamint álnevesítés alkalmazása, ahol lehetséges, a közvetlen azonosíthatóság csökkentése érdekében.
- **Fizikai biztonság:** Az adattároló létesítmények és eszközök fizikai hozzáférésének védelme.
- **Hálózati biztonság:** Tűzfalak, behatolásérzékelő/megelőző rendszerek és biztonságos hálózati konfigurációk alkalmazása.
- **Mentés és helyreállítás:** Rendszeres biztonsági mentések és robusztus katasztrófa-helyreállítási tervek szükségesek az adatok rendelkezésre állásának és ellenálló képességének biztosítására.
- **Biztonságos megsemmisítés:** Eljárásokat kell kidolgozni a már nem szükséges adatok és papír alapú nyilvántartások biztonságos törlésére vagy megsemmisítésére, megelőzve a véletlen megsemmisülést.
- **Dokumentumkezelés:** Az iratkezelési szabályzat szerint.

7.2. Különleges kezelési utasítások

Bizonyos dokumentumok esetében különleges kezelési utasítások alkalmazandók (pl. kivonat nem készíthető, elolvasás után visszaküldendő, zárt borítékban tárolandó, nem másolható). Ezek alkalmazásáról a minősítő dönt.

7.3. Adatvédelmi Hatásvizsgálat (DPIA)

Az adatvédelmi hatásvizsgálat (Data Protection Impact Assessment – DPIA) egy olyan folyamat, amelynek célja az adatkezelési műveletek által az érintettek jogaira és szabadságaira jelentett kockázatok azonosítása és értékelése, valamint azok mérséklésére szolgáló intézkedések meghatározása.

- **Mikor szükséges?** Adatvédelmi hatásvizsgálatot kell végezni legalább az alábbi esetekben: egy személy személyes jellemzőinek rendszeres és kiterjedt értékelése esetén, ideértve a profilalkotást is; különleges adatok nagy számban történő kezelése; nyilvános helyek nagymértékű, módszeres megfigyelése.
- **Célja:** A DPIA-t az adatkezelés megkezdése előtt kell elvégezni, és célja a lehetséges adatvédelmi kockázatok azonosítása és mérséklése.
- **A DPO szerepe:** Az adatvédelmi tisztviselő szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, és nyomon követi annak elvégzését.
- **Konzultáció a NAIH-val:** Amennyiben a fennmaradó kockázatok nem mérsékelhetők a bevezetett intézkedésekkel, az adatkezelés megkezdése előtt konzultálni kell az adatvédelmi hatósággal.

7.4. Adatvédelmi auditok

Az adatvédelmi audit a leghatékonyabb vizsgálat annak érdekében, hogy egy szervezet

teljeskörű, átfogó képet kapjon adatkezelési folyamatairól, az adatkezeléshez használt rendszereinek működéséről, illetve arról, hogy ezek mennyire felelnek meg a jogszabályi, adatvédelmi és egyéb előírásoknak. 19

- **Célja:** Az audit célja a szervezet adatkezelési gyakorlatának felmérése a GDPR, az Infotv., az ágazati jogszabályok és a NAIH ajánlások fényében. Segít feltárni a hiányosságokat és a kockázatokat, beleértve a bírság és a reputációs kockázatokat.
- **Szakaszai:** Az adatvédelmi audit jellemzően több szakaszból áll: háttérdokumentáció vizsgálat, gyakorlati működés vizsgálat, GAP analízis, akcióterv, és az akcióterv végrehajtása.
- **Előnyei:** Az audit eredményeként a szervezet pontos képet kap aktuális helyzetéről és a szabályozást igénylő területekről. Segít abban, hogy a vállalkozás ne csak megfeleljen a jogszabályi előírásoknak, hanem növelje az ügyfelek és partnerek bizalmát is.
- **Külső szakértelem:** Az adatvédelmi terület speciális szakértelem és szakmai tapasztalatot igényel. Amennyiben a szervezetnek nincs megfelelő belső szakembere a hibák javítására, külső tanácsadó bevonása javasolt.

8. Adatvédelmi incidensek kezelése és bejelentése

8.1. Definíció és azonosítás

Adatvédelmi incidensnek minősül minden olyan biztonsági esemény, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan nyilvánosságra hozatalát vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

8.2. Incidenskezelési eljárás

Az Intézmény részletes eljárásokat dolgoz ki az incidensek azonnali azonosítására, kivizsgálására, elhárítására és a károk mérséklésére. Ez magában foglalja az előzetes értékelési mintát, amely alapján az incidens jelentősége megállapítható (pl. érintett adatok köre, érintettek száma, azonnali intézkedés szükségessége, partneradatok érintettsége, hatás, büntetőjogi következmények).

8.3. Bejelentési Kötelezettség

Az adatvédelmi incidenseket haladéktalanul, de legkésőbb 72 órán belül be kell jelenteni a Nemzeti Adatvédelmi és Információszabadság Hatóságnak (NAIH), amennyiben az incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

8.4. Naplózás és dokumentáció

Az összes adatvédelmi incidenst dokumentálni kell egy belső nyilvántartásban, rögzítve az incidens tényét, hatásait és az elvégzett intézkedéseket. Az adatkezelőnek naplózási rendet kell bevezetnie és folyamatosan ellenőriznie kell az adatvédelmi incidensek megelőzése és felderítése céljából.

9. Az üzleti titok kezelése

- Az üzleti titokhoz és védett ismerethez kizárólag azok férhetnek hozzá, akiknek ez a munkájukhoz feltétlenül szükséges. Az információkhoz való hozzáférést dokumentálni kell, és minden érintettet írásban, igazolható módon tájékoztatni kell a titoktartási kötelezettségről.
- Az üzleti titkot és a védett ismeretet csak az Intézmény előzetes írásbeli hozzájárulásával lehet harmadik fél tudomására hozni vagy nyilvánosságra hozni. A titoktartásra

kötelezett személy sem közvetve, sem közvetlenül nem teheti közzé, nem reprodukálhatja, nem terjesztheti, nem továbbíthatja, nem visszafejtheti vagy nem ruházhatja át az üzleti titkot semmilyen formában.

10. Külső féltől származó, üzleti titokként minősített adatok kezelése

10.1. Átvétel

- Külső féltől származó, üzleti titokként megjelölt adatokat kizárólag írásban, dokumentált módon szabad átvenni, a minősítés egyértelmű feltüntetésével (pl. „Üzleti titok" jelölés az iraton).
- Az átvétel során minden esetben rögzíteni kell az átadó fél nevét, az adat pontos megnevezését, az átvétel időpontját, valamint az üzleti titok minősítés indokát (átvételi elismervény vagy jegyzőkönyv).
- Az átvételről átvételi elismervényt vagy jegyzőkönyvet kell készíteni, amelyet mindkét fél aláír.
- A közbeszerzési eljárás az ajánlattevő által, az EKR felületre feltöltött, üzleti titkot tartalmazó dokumentum esetén az átvétel dokumentálása az EKR-en keresztül, az ajánlati dokumentációval közösen történik.

10.2. Feldolgozás

- Az adatokat kizárólag a kijelölt, titoktartási kötelezettséggel rendelkező foglalkoztatottak dolgozhatják fel, a külső fél által meghatározott feltételek és célok szerint.
- A feldolgozás során tilos az adatokat a szerződésben vagy titoktartási megállapodásban rögzített célokon túl felhasználni, továbbítani vagy másolni.
- A feldolgozás minden lépése dokumentálandó, a hozzáférések naplózása kötelező (betekintési nyilvántartás).

10.3. Tárolás

- Az üzleti titokként minősített adatokat elkülönítetten, zárt, biztonságos fizikai vagy elektronikus tárolóban kell elhelyezni, amelyhez csak az arra jogosultak férhetnek hozzá.
- Elektronikus tárolás esetén jelszóval védett, hozzáférés-szabályozott rendszer használata kötelező.
- A tárolás során biztosítani kell, hogy az adatokhoz illetéktelen személy ne férhessen hozzá, és az adatok integritása ne sérüljön.

10.3.1 Továbbítás 3. személy részére és másolás

1) Védendő információ továbbítása csak biztonságos csatornán történhet.
2) E-mailben csak titkosítva vagy jelszóval védve küldhető.
3) Fénymásolás csak engedéllyel, nyilvántartással végezhető.
4) Külső félnek történő átadás csak titoktartási nyilatkozat aláírása után lehetséges.
5) A továbbítás során minden esetben ellenőrizni kell a címzett jogosultságát és a továbbítás szükségességét.
6) A digitális továbbítás esetén előnyben kell részesíteni a végponttól végpontig titkosított kommunikációs csatornákat.

10.4. Selejtezés (külön intézkedések)

- Selejtezéskor a dokumentumokat megsemmisítés előtt jegyzőkönyvezni kell

(selejtezési jegyzőkönyv), a selejtezés tényét és módját rögzíteni kell.

10.5. Megismerhetőség módja

- Az ilyen adatokhoz kizárólag azok a foglalkoztatottak férhetnek hozzá, akiknek a munkaköri leírása, illetve a titoktartási megállapodás ezt kifejezetten lehetővé teszi.
- A megismerés minden esetben naplózandó (hozzáférési napló), a hozzáférési jogosultságokat rendszeresen felül kell vizsgálni.
- Harmadik félnek az adatokat csak a külső fél előzetes, írásbeli engedélyével lehet átadni.
- A betekintés, másolás, továbbítás vagy bármilyen egyéb hozzáférés kizárólag a titoktartási kötelezettség vállalása mellett történhet, amelyet írásban kell rögzíteni.
- Közérdekű adatigénylés esetén az üzleti titokként minősített adatok csak akkor adhatók ki, ha a hatályos jogszabályok ezt kifejezetten előírják, és az aránytalan sérelem kizárható.

11. Adatok minősítése, felülvizsgálata

- Az adat minősítése akkor indokolt, ha az adat a minősítéssel védhető közérdekek körébe tartozik, nyilvánosságra hozatala károsítja a minősítéssel védhető közérdeket, és szükséges az adat nyilvánosságának meghatározott ideig történő korlátozása.
- A minősítő a felterjesztés kézhezvételétől számított 30 napon belül dönt az adat minősítéséről, a jelölésnek tartalmaznia kell a minősítési szintet és az érvényességi időt, a javaslat indokolását, a szükséges tényeket és körülményeket.
- Az Intézményben jellemzően csak üzleti titok minősítés alkalmazott, amelyet a készítő, illetve az Intézmény vezetője jogosult elrendelni.
- A minősítő köteles rendszeresen, de legalább 5 évente felülvizsgálni az általa vagy jogelődje által minősített adatokat, és dönthet a minősítés fenntartásáról, szintjének csökkentéséről, érvényességi idejének módosításáról vagy megszüntetéséről.

12. Selejtezés

Az iratok selejtezésére vonatkozóan külön szabályzat rendelkezik, melynek általános rendelkezései a jelen szabályzat hatálya alá tartozó iratokra is vonatkoznak.

12.1. Selejtezés alapelvei

- Selejtezni csak olyan iratot lehet, amelynek megőrzési ideje lejárt, azonos típusú iratokra a leghosszabb megőrzési idő az irányadó.

12.2. Megsemmisítési módok

1) Papír dokumentumok: iratmegsemmisítő vagy aprítás alkalmazásával.
2) Elektronikus adatok: biztonságos törlés speciális szoftverrel.
3) Adathordozók: fizikai tönkretétel.
4) Megsemmisítési jegyzőkönyv készítése minden esetben kötelező.
5) A megsemmisítés során biztosítani kell, hogy az adatok véglegesen és visszaállíthatatlanul törlődjenek.
6) A megsemmisítési folyamat szakszerű végrehajtása kulcsfontosságú a teljes titokvédelmi rendszer hatékonyságának szempontjából.

13. Használt és kötelező dokumentumok

A szabályzat végrehajtásához az alábbi dokumentumok alkalmazása kötelező:

- Átvételi elismervény vagy jegyzőkönyv

  Külső féltől származó, üzleti titokként minősített adat átvételekor készül, tartalmazza az átadó fél nevét, az adat pontos megnevezését, az átvétel időpontját és a minősítés indokát.

- Selejtezési jegyzőkönyv

  Az iratok, adatok selejtezésekor készül, rögzíti a selejtezés tényét, okát, módját, a selejtezésben résztvevők nevét, valamint a jóváhagyást.

- Megsemmisítési jegyzőkönyv

  Selejtezett dokumentumok megsemmisítésekor készül, a megsemmisítést végző személy aláírja.

- Betekintési nyilvántartás

  Az üzleti titokként minősített adatokhoz való hozzáféréseket, megismeréseket, feldolgozási lépéseket naplózni kell.

- Oktatási igazolás

  A titokvédelmi szabályzat oktatásán részt vett foglalkoztatottak aláírásával igazolják annak megismerését.

14. Záró Rendelkezések

14.1. A Szabályzat felülvizsgálata és aktualizálása

A jelen Titokvédelmi Szabályzat nem statikus dokumentum; rendszeres felülvizsgálatra és aktualizálásra szorul. Javasolt a szabályzatot legalább évente, vagy jogszabályi változások, technológiai fejlődés, illetve az Intézmény működésében bekövetkező jelentős változások esetén azonnal felülvizsgálni és aktualizálni, biztosítva annak folyamatos relevanciáját és hatékonyságát. Világos eljárásokat kell kidolgozni a szabályzat frissítésére és a változások kommunikálására minden érintett felé.

14.2. Jogkövetkezmények

A jelen Titokvédelmi Szabályzat be nem tartása súlyos jogkövetkezményekkel járhat mind az egyének, mind az Intézmény számára. A foglalkoztatottak esetében fegyelmi eljárásokra, akár munkaviszony megszüntetésére is sor kerülhet.

A jelen szabályzat az Intézmény valamennyi foglalkoztatottjára és szerződéses partnerére kötelező érvényű. A szabályzatban nem szabályozott kérdésekben a mindenkor hatályos jogszabályok az irányadók. A szabályzat hatálybalépésével egyidejűleg minden korábbi, ezzel ellentétes rendelkezés hatályát veszti. A szabályzatot az Intézményvezető hagyja jóvá, és az Intézmény faliújságján, valamint belső kommunikációs csatornáin keresztül kell közzétenni, biztosítva annak minden érintett számára történő megismerését.

Kelt: Budapest, 2025. augusztus 11.

Fővárosi Önkormányzat Vázsonyi Vilmos Idősek Otthona

Intézményvezető

1. számú melléklet

Üzleti titok felmerülése esetén az alábbi alkalmazható utasítások adhatók:

- Saját kezű felbontásra!
- Más szervnek nem adható át!
- Nem másolható!
- Kivonat nem készíthető!
- Elolvasás után visszaküldendő!
- Zárt borítékban tárolandó!
- Különösen fontos!
- Csak kijelölt személyek férhetnek hozzá!
- Nem vihető ki az intézmény területéről!
- Elektronikus másolat nem készíthető!
- Egyéb, az adathordozó sajátosságától függő utasítás

A különleges kezelési utasításokat minden érintett dokumentumon jól látható helyen kell feltűntetni. Ezek az utalások növelik a titkos információk védelmét, és megszegésük fegyelmi vagy jogi következményekkel járhat. A cél, hogy a dokumentumok sorsa minden pillanatban nyomon követhető legyen.