4999/1/2025

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:

- **Gyengébb titok (belső titok):** Minden olyan információ, amely ugyan nem minősül üzleti titoknak vagy minősített adatnak, de az Intézmény működése szempontjából jelentőséggel bír, illetéktelen személy általi megismerése vagy nyilvánosságra hozatala az Intézményre nézve hátrányos következményekkel járhat. Gyengébb titok lehet például a belső szabályzat, utasítás, eljárásrend vagy szervezeti működéshez kapcsolódó, nem nyilvános információ. Ezen adatok kezelésének célja a szervezet belső érdekeinek

5. Adatkezelési és titokvédelmi alapelvek

Saját működése során az intézmény nem keletkeztet üzleti titkoknál 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

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)

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 katasztrófahelyreállítási 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

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

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

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

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.