FŐVÁROSI ÖNKORMÁNYZAT
GYULAI IDŐSEK OTTHONA
5700 GYULA, VÉRTANÚK ÚTJA 1-5.
TEL.: +36 66 561 370 FAX: +36 66 561 373
E-MAIL: GYULAOTTHON@GYULAOTTHON.HU

Ikt. sz.: Gy: 23 - 7/2025.

ÜZLETI TITOK SZABÁLYZAT

Tartalom

1 Bevezető rendelkezések

1.1 A szabályzat célja

A szabályzat célja, hogy a Fővárosi Önkormányzat Gyulai Idősek Otthona – 5700 Gyula, Vértanúk útja 1-5. (továbbiakban intézmény) részére egységes eljárásrendet biztosítson az üzleti titok, közadat, valamint a külső féltől származó, üzleti titokként minősített adatok kezelésére, védelmére, selejtezésére és megismerhetőségére.

1.2 A szabályzat tárgya

Minden, az intézményben keletkező, oda érkező, illetve onnan kimenő üzleti titokra, közadatra vonatkozik. Az adatvédelmi és titokvédelmi eljárások minden dokumentumra, elektronikus adatra és szóban átadott információra is kiterjednek.

1.3 A szabályzat személyi hatálya

Az intézmény minden foglalkoztatottjára és szerződéses partnerére kiterjed. Ez magában foglalja a teljes munkaidős, részmunkaidős, megbízási jogviszonyban álló, valamint a külső szolgáltatókat is.

A szabályzat rendelkezései kiterjednek az adatkezelési nyilvántartás titokvédelmi szempontjaira is.

1.4 Jogszabályi alapok

- 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 információs önrendelkezési jogról és az információszabadságról (Infotv.)
- 2013. évi V. törvény a Polgári Törvénykönyvről (Ptk.)
- 2009. évi CLV. törvény a minősített adatok védelméről (Titok tv.)
- 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

2 Értelmező rendelkezések

- **Titok / Bizalmas információ:** Minden olyan információ, amelynek jogosulatlan hozzáférése, módosítása, nyilvánosságra hozatala vagy megsemmisítése kárt okozna a szervezetnek vagy az érintettnek. Ide tartoznak mind az üzleti, valamint a személyes és különleges adatok is. A bizalmas információk védelme kiemelt fontosságú az intézmény működésében, és magába foglalja a gondozottak adatait is.

- **Üzleti titok:** Minden olyan adat, amelyet a készítő üzleti titoknak minősít, vagy amelynek védelme üzleti érdek. Az üzleti titok védelme elősegíti az intézmény versenyképességét, gazdasági érdekeinek megőrzését, és megakadályozza a jogosulatlan felhasználást. 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, titokként minősített adat:** Külső partner által üzleti titokként megjelölt adat. Ezek kezelésére különös figyelmet kell fordítani, és a partner előírásait is be kell tartani. Ezen adatok védelme szerződéses kötelezettség, és betartásuk az intézmény jó hírnevét is védi.

- **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.

3 Általános rendelkezések

3.1 Adatkezelési és titokvédelmi alapelvek

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.
- **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.

3.2 Kapcsolódás a személyesadat-kezeléshez

Az Üzleti Titok Szabályzat személyes adatot csak abban az esetben érint, ha az adott információ egyben üzleti titok. Ekkor a titokvédelmi eljárások mellett a GDPR-ból fakadó kötelezettségek is irányadók.

A személyes adatok kezelésével, valamint az érintettek jogainak gyakorlásával kapcsolatos részletszabályokat a szervezet Adatvédelmi Kódexe és Adatvédelmi Szabályzata tartalmazza.

3.3 Szerepek és felelősségek

3.3.1 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 az Adatvédelmi Kódexet és Adatvédelmi szabályzatot, valamint gondoskodik az adatkezelési nyilvántartás GDPR-nak megfelelő vezetéséről és naprakészen tartásáról. Feladata továbbá, hogy folyamatosan ellenőrizze és figyelemmel kísérje, hogy az intézményben történő adatkezelés megfelel-e a jogszabályokban, valamint a belső dokumentumokban meghatározott szabályoknak.

3.3.2 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. preambulum bekezdés alapján a következők:

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

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

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

helyén jól látható módon, a honlapján, az adatkezelési tájékoztatókban, az adatkezelési tevékenységek nyilvántartásában, az adatvédelmi incidensek nyilvántartásában, valamint az érintett hozzáférési jogával kapcsolatos intézkedések nyilvántartásában.

3.3.3 Foglalkoztatottak és külső partnerek kötelezettségei

Az Intézmény valamennyi foglalkoztatottja és szerződéses partnere köteles betartani a jelen Üzleti Titok 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 az Üzleti Titok Szabályzat és az alkalmazandó adatvédelmi törvények betartására, és megfelelő biztonsági intézkedéseket kell bevezetniük.

3.3.4 Képzés és tudatosság

Kötelező, rendszeres képzést kell biztosítani minden foglalkoztatott számára az Üzleti 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.

3.4 Titok- és adatbiztonsági intézkedések

Az intézmény technikai és szervezeti intézkedésekkel védi az adatokat a jogosulatlan hozzáféréstől, módosítástól, megsemmisüléstől vagy elvesztéstől. A biztonsági intézkedések kiterjednek a fizikai, informatikai és szervezeti védelemre is, beleértve a rendszeres auditokat és kockázatelemzéseket. A folyamatos fejlesztés biztosítja, hogy az intézmény a legújabb technológiai kihívásokra is felkészült legyen.

3.4.1 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.

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

- **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:** Részletes eljárásokat kell bevezetni a papír alapú és elektronikus dokumentumok kezelésére, beleértve a számozást, nyilvántartásba vételt (iktatókönyvek), iktatást, és továbbítást. Kiemelt figyelmet kell fordítani a papír alapú iratkezelési segédletek hitelesítésére, valamint az elektronikus másolatok képi vagy tartalmi megfelelésének biztosítására a papír alapú eredetikkel, hitelesítési záradékkal és elektronikus aláírással ellátva.

3.4.2 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.

3.4.3 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.

3.4.4 Adatvédelmi auditok

Az adatvédelmi audit a leghatékonyabb vizsgálat annak érdekében, hogy egy szervezet teljes körű, átfogó képet kapjon adatkezelési folyamatairól, az adatkezeléshez használt rendszereinek működéséről, illetve arról, hogy ezek mennyire felelnek meg a jogszabályi, adatvédelmi és egyéb előírásoknak.

- **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: háttér-dokumentáció 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.

3.5 Adatvédelmi incidensek kezelése

Az adatvédelmi incidensek azonnali azonosítása, kivizsgálása és kezelése kiemelt jelentőségű. Az incidenseket minden esetben dokumentálni kell, és szükség esetén jelenteni kell a hatóságoknak, illetve értesíteni kell az érintetteket. Az intézmény részletes eljárásrendet dolgozott ki az incidensek megfelelő kezelésére.

3.5.1 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.

3.5.2 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).

3.5.3 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.

3.5.4 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.

3.6 Üzleti titok kezelése

Az üzleti titokhoz csak azok férhetnek hozzá, akiknek ez a munkájukhoz feltétlenül szükséges. Az üzleti titok védelme érdekében minden érintettet írásban, igazolható módon kell tájékoztatni a titoktartási kötelezettségről. Az üzleti titkot 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.

3.7 Külső féltől származó, üzleti titokként minősített adatok kezelése

A nem az adatkezelőnél keletkező adat csak akkor kezelhető üzleti titokként, ha az adat szolgáltatója az adat e jellegét egyértelműen, már az adat szolgáltatásakor, az üzleti titokként kezelendő adatok pontos megjelölésével jelezte, és az adat üzleti titokként kezelése nem nyilvánvalóan ellentétes az üzleti titok védelméről szóló 2018. évi LIV. törvényben foglaltakkal.

3.7.1 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 során az ajánlattevő által, az EKR felületre feltöltött, üzleti titkot tartalmazó dokumentum esetén az átvétel dokumentálása az EKR-en keresztül, az ajánlati dokumentációval közösen történik.
- Szerződésben üzleti titokra vonatkozó rendelkezés esetén az átvétel a szerződés aláírásával valósul meg.

3.7.2 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 (hozzáférési napló).

3.7.3 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.

3.7.4 Selejtezés (külön intézkedések)

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

3.7.5 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.

3.8 Adatok minősítése, felülvizsgálata

Az adatok minősítése során a minősítő indokolja a titokvédelmi szintet, meghatározza az érvényességi időt, és rendszeres felülvizsgálatot ír elő. A minősítési eljárás átlátható és dokumentált, biztosítva a jogszerűséget és a visszakereshetőséget. A felülvizsgálat célja, hogy a minősítés mindig aktuális és indokolt legyen.

- 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.

3.9 Titoktartási kötelezettség időbeli hatálya és megszűnése

3.9.1 Üzleti titok időbeli hatálya

Az üzleti titok védelme **határozatlan ideig** fennáll, amíg az adat megfelel az üzleti titok fogalmi követelményeinek. Az üzleti titok akkor szűnik meg, ha:

- elveszti gazdasági értékét,
- általánosan ismertté válik vagy könnyen hozzáférhetővé,
- a titok jogosultja felmentést ad a titoktartás alól,
- a titok nyilvánosságra kerül jogszerű módon.

Az üzleti titok esetében nincs törvényben meghatározott maximális időtartam, azonban a titok védelmének fenntartása érdekében a jogosultnak folyamatosan biztosítania kell a szükséges védelmi intézkedéseket.

3.10 Selejtezés

Az iratok selejtezésére vonatkozóan külön szabályzat rendelkezik, melynek általános rendelkezései a jelen szabályzat hatálya alá tartozó iratokra is vonatkoznak. Selejtezni csak olyan iratot lehet, amelynek megőrzési ideje lejárt, azonos típusú iratokra a leghosszabb megőrzési idő az irányadó.

3.11 Használt és kötelező dokumentumok

A szabályzat végrehajtásához kötelezően alkalmazandó dokumentumok: átvételi elismervény, selejtezési jegyzőkönyv, megsemmisítési jegyzőkönyv, hozzáférési napló, oktatási igazolás. Ezek a dokumentumok biztosítják a folyamatok átláthatóságát és ellenőrizhetőségét, valamint segítik a jogszerűség bizonyítását. A megfelelő dokumentáció elengedhetetlen a szabályzat betartásához és a jogi megfeleléshez.

4 Záró rendelkezések

4.1 A szabályzatot évente, illetve jogszabályi változás, technológiai fejlődés, az intézmény működésében bekövetkező jelentős változások esetén felül kell vizsgálni és szükség szerint aktualizálni.

4.2 Jelen Üzleti titok szabályzat be nem tartása súlyos jogkövetkezményekkel járhat mind az egyének, mind az intézmény számára. Az üzleti titok megsértése a közalkalmazott jogviszonyából eredő kötelezettség súlyos megsértésének minősül. A foglalkoztatottak esetében fegyelmi eljárásokra, akár közalkalmazotti jogviszony megszüntetésére is sor kerülhet. Az üzleti titok megsértése esetén az üzleti titok védelméről szóló 2018. évi LIV. törvényben foglaltak az irányadók.

4.3 A jelen szabályzat az Intézmény valamennyi foglalkoztatottjára és szerződéses partnerére kötelező érvényű. A szabályzatban nem szabályozott kérdésekben a mindenkor hatályos jogszabályok az irányadók.

4.4 Jelen szabályzat 2025. október 1-jén lép hatályba és visszavonásig érvényes. A szabályzat hatálybalépésével egyidejűleg minden korábbi, ezzel ellentétes rendelkezés hatályát veszti.

Gyula, 2025. szeptember 30.

Hajdu Szilvia

gazdasági vezető

1.melléklet

Minősítési jegyzőkönyv

Készítő szerv neve: Fővárosi Önkormányzat Gyulai Idősek Otthona

Irat tárgya: [Az adat vagy dokumentum pontos megnevezése]

Minősítési javaslatot készítette: [Név, beosztás]

Minősítési javaslat kelte: [Év, hónap, nap]

1. Minősítési javaslat indoka

- Az adat a minősítéssel védhető közérdekek vagy az intézmény működésének rendje körébe tartozik. A minősítés célja, hogy az adat jogosulatlan megismerését vagy nyilvánosságra hozatalát megakadályozza.
- Nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé tétele, illetve az arra jogosult részére hozzáférhetetlenné tétele károsítja a védhető közérdeket. A minősítés indoklásában részletesen meg kell határozni, hogy milyen érdeksérelem következhet be az adat védelme nélkül.
- Az adat nyilvánosságát és az arra feljogosított személyen kívüli megismerhetőségét meghatározott ideig korlátozni szükséges. Az érvényességi idő letelte után a minősítés automatikusan megszűnik, hacsak a minősítő másként nem rendelkezik.

Rövid indoklás: [Pl.: Az adat tartalmazza az intézmény pénzügyi tervét, amely üzleti titoknak minősül, nyilvánosságra hozatala versenyhátrányt okozna.]

2. Minősítési szint

- [ ] Üzleti titok
- [ ] Közadat (nem minősíthető)
- [ ] Egyéb: _____

Érvényességi idő: [Év, hónap, nap – vagy: „meghatározott eseményig”] Az érvényességi idő megállapításánál figyelembe kell venni az adat jellegét és a védelmi szükségletet.

3. Minősítő döntése

Minősítő neve, beosztása: [Név, beosztás]

Döntés kelte: [Év, hónap, nap]

Döntés:

- [ ] A minősítési javaslatot elfogadom
- [ ] A minősítési javaslatot elutasítom

Minősítési jelölés: [Pl.: „Üzleti titok! Érvényes: 2026. június 30-ig” A minősítési jelölést minden példányon jól láthatóan fel kell tüntetni.

4. Különleges kezelési utasítások

[Pl.: „Nem másolható”, „Zárt borítékban tárolandó”, „Csak kijelölt személyek férhetnek hozzá”] Az utasításokat a dokumentum minden példányán rögzíteni kell.

5. Példánysorszám, iktatószám, címzettek

- **Példánysorszám:** [1/2/3...]
- **Iktatószám:** [Iktatószám]
- **Címzettek:** [Név, beosztás]

A példánysorszám segíti a dokumentumok nyomon követését, az iktatószám pedig az iratkezelési rendszerben való azonosítást.

6. Aláírások

Név	Beosztás	Aláírás	Dátum

Megjegyzés: A jegyzőkönyvet minden érintett példányban, az adatkezelési szabályoknak megfelelően kell kezelni és tárolni. A minősítési döntésről az érintetteket írásban kell tájékoztatni, és a jegyzőkönyvet az iratkezelési szabályok szerint kell megőrizni.

2.melléklet

MINŐSÍTÉSI ZÁRADÉK

Ez az irat **üzleti titoknak titoknak** minősül.

- **Minősítési szint:** [Üzleti titok / / Bizalmas! / Korlátozott terjesztésű!]
- **Érvényességi idő:** [Év, hónap, nap vagy „meghatározott eseményig”]
- **Minősítő neve, beosztása:** [Név, beosztás]
- **Minősítés kelte:** [Év, hónap, nap]
- **Különleges kezelési utasítások:** [Pl. „Nem másolható”, „Zárt borítékban tárolandó”, „Csak kijelölt személyek férhetnek hozzá”]

A záradékot minden irat első oldalán, jól látható helyen kell feltüntetni, és szükség esetén minden oldalon megismételni. Ez biztosítja, hogy mindenki számára egyértelmű legyen az irat minősített státusza és a rá vonatkozó kezelési szabályok.

Példa a záradék elhelyezésére:

Üzleti titok! Bizalmas!
Érvényes: ……-ig.
Minősítő: intézményvezető
Kelt: ……..
Különleges utasítás: Nem másolható, csak kijelölt személyek férhetnek hozzá.

3.melléklet

Különleges kezelési utasítások felsorolása

- 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 utasítások célja, hogy a minősített adatok védelme minden helyzetben biztosított legyen. Az utasítások megszegése fegyelmi vagy jogi következményekkel járhat, és minden érintett köteles azokat maradéktalanul betartani. Ezek az utasítások segítik a mindennapi munkát és a szabályok betartását.

A fenti szabályzat és mellékletei részletesen szabályozzák az üzleti titok, valamint minden minősített adat kezelését, védelmét, minősítését, dokumentálását és ellenőrzését az intézményben. A szabályzat alkalmazásával az intézmény biztosítja a jogszabályoknak megfelelő, átlátható és biztonságos adatkezelést, valamint a bizalom fenntartását minden érintett számára.

4.melléklet

Átvételi Elismervény – Üzleti titok

Cél: Az üzleti titok kezelésére jogosult személyek közötti átadás-átvétel dokumentálása a Titok tv. 15. §-a alapján.

Mező	Tartalom	Kitöltési útmutató
Iktatószám		Intézményi iktatási rend szerint
Kelt		Átadás helye és dátuma

Átvétel tárgyát képező anyag

Dokumentum megnevezése	**Minősítés**	**Mennyiség**	**Egyedi azonosító**	**Megjegyzés**

Átadó és átvevő adatai

Átadó:

- **Név:**
- **Beosztás:**
- **Szervezeti egység:**
- **Jogosultsági szint:**
- **Aláírás: _____**

Átvevő:

- **Név:**
- **Beosztás:**
- **Szervezeti egység:**
- **Jogosultsági szint:**
- **Aláírás: _____**

Átadás-átvétel körülményei

- **Átadás célja:**
- **Visszaadási határidő:**
- **Különleges tárolási feltételek:**
- **Felelősségvállalás:**

Záradék: Az átvevő kijelenti, hogy az átadott dokumentumokat kizárólag a megjelölt célra használja, azokat illetéktelen személlyel nem közli, és a visszaadási határidő lejártakor változatlan állapotban visszaszolgáltatja.

5.melléklet

Hozzáférési Napló

Cél: Az üzleti titokhoz való hozzáférések nyomon követése, auditálhatóság biztosítása a GDPR 32. cikke és a Titok tv. alapján.

Naplóvezetési útmutató

- **Kitöltés gyakorisága:** Minden egyes hozzáféréskor azonnal
- **Adatmegőrzés:** 5 év (GDPR követelmény)
- **Felelős:** Az adott szervezeti egység vezetője és a DPO
- **Ellenőrzés:** Havonta a DPO által

Hozzáférési napló

Hónap:
Szervezeti egység:
Adathordozó/rendszer:

Dátum	Idő	Felhasználó	Cél	Érintett adatkör	Jogosultság	Kivétel

Különleges események

Dátum	Esemény	Intézkedés	Felelős	Státusz

Adatvédelmi megfelelőség

Ellenőrző:
Ellenőrzés dátuma:
Megállapítás:
Intézkedés:
Aláírás: _____