ADATVÉDELMI SZABÁLYZAT

BitNet Group Kft

	BitNet Group Kft
Székhely	Budapest, Magyarország
Üzleti tevékenység	Mobilalkalmazás-fejlesztés, webprogramozás és egyéni szoftverfejlesztés
Weboldal	https://bitnet.hu
Dokumentum felelős	[Adatvédelmi Koordinátor / Vezetőség]
Besorolás	Belső – Bizalmas

Verziótörténet

Verzió	Dátum	Szerző	Fejezet	Leírás
1.0	[Dátum]	[Monogram]	Mind	Eredeti változat

Jóváhagyás

	Funkció	Név / Aláírás	Dátum
Készítette	Adatvédelmi Koordinátor	[Név]	[Dátum]
Ellenőrizte	[Funkció]	[Név]	[Dátum]
Jóváhagyta	Ügyvezető	[Név]	[Dátum]

Tartalomjegyzék

Tartalomjegyzék 2
1. Bevezetés 4
2. Cél és hatály 4
2.1 Cél 4
2.2 Hatály és alkalmazhatóság 5
3. Fogalommeghatározások 5
4. Szerepek és felelősségek 6
4.1 Vezetőség 6
4.2 Adatvédelmi Koordinátor 6
4.3 Valamennyi Felhasználó 7
4.4 A Társaság GDPR szerinti szerepe 7
5. Adatvédelmi alapelvek 7
6. Az adatkezelés jogalapjai 8
6.1 Hozzájárulás-kezelés 8
7. Érintetti jogok 9
7.1 A kérelmek kezelésének eljárása 9
7.2 Jogok áttekintése 9
7.3 Adatfeldolgozói kötelezettségek az érintetti jogok tekintetében 10
8. Technikai és szervezeti biztonsági intézkedések 10
8.1 Technikai intézkedések 10
8.2 Szervezeti intézkedések 10
8.3 Beépített és alapértelmezett adatvédelem 11
8.4 Beépített adatvédelem a szoftverfejlesztési életciklusban 11
8.4.1 Projektindítási fázis 11
8.4.2 Tervezési és architektúra fázis 11
8.4.3 Fejlesztési és tesztelési fázis 12
8.4.4 Üzembe helyezési és karbantartási fázis 12
8.4.5 Dokumentáció 12
9. Adatvédelmi incidenskezelés 12
9.1 Incidensészlelés és bejelentés 12
9.2 Értékelés és válaszintézkedések 13
9.3 Bejelentés a felügyeleti hatóságnak (33. cikk) 13
9.4 Az érintettek tájékoztatása (34. cikk) 13
9.5 Adatfeldolgozói kötelezettségek incidens esetén 13
9.6 Incidensnyilvántartás 13

10. Adatkezelési tevékenységek nyilvántartása és hatásvizsgálatok 13
10.1 Adatkezelési tevékenységek nyilvántartása (30. cikk) 13
10.2 Adatvédelmi hatásvizsgálat (35. cikk) 14
11. Adatmegőrzés 14
11.1 Általános elvek 14
11.2 Megőrzés adatkezelői minőségben 15
11.3 Megőrzés adatfeldolgozói minőségben 15
11.4 Fejlesztési projektadatok megőrzése 15
11.5 Rendszeres törlési eljárások 16
12. Harmadik fél és beszállító kezelése 16
12.1 Adatfeldolgozók megbízása 16
12.2 AI-adatfeldolgozók kezelése és átvilágítás 16
12.3 Nemzetközi adattovábbítás 17
13. Adatvédelmi kapcsolattartási pont 17
14. Képzés és tudatosság 17
15. Nyomon követés, felülvizsgálat és folyamatos fejlesztés 18
15.1 Éves megfelelési felülvizsgálat 18
15.2 Jelentés a vezetőségnek 18
15.3 A Szabályzat felülvizsgálatát kiváltó események 18
16. Szabályzatsértés 19
17. Dokumentumkezelés 19
17.1 Hatálybalépés 19
17.2 Kivételek 19
1. számú melléklet – Adatmegőrzési Nyilvántartás 20
2. számú melléklet – Jogszabályi hivatkozások 24
Jóváhagyás és aláírások 25

1. Bevezetés

2018. május 25. óta 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 (az „Általános Adatvédelmi Rendelet" vagy „GDPR") közvetlenül alkalmazandó az Európai Unió valamennyi tagállamában, beleértve Magyarországot is.

A BitNet Group Kft (a továbbiakban: „Társaság") elkötelezett amellett, hogy az általa kezelt személyes adatokat a GDPR-nak, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek (a továbbiakban: „Infotörvény"), valamint minden egyéb vonatkozó adatvédelmi jogszabálynak maradéktalanul megfelelően kezelje.

A 2003-ban alapított Társaság mobilalkalmazás-fejlesztéssel, webprogramozással és egyéni szoftverfejlesztéssel foglalkozik, több mint 150 befejezett projekttel és 1,8 millió alkalmazásletöltéssel. Működése során a Társaság különböző érintetti kategóriákba tartozó személyes adatokat gyűjt és kezel, beleértve:

- Jelenlegi és korábbi munkavállalók
- Álláspályázók és jelentkezők
- Ügyfélkapcsolattartók (projektmenedzserek, műszaki kapcsolattartók, számlázási kapcsolattartók)
- Weboldal-látogatók és potenciális ügyfelek
- Beszállítók és üzleti partnerek

Emellett adatfeldolgozói minőségében a Társaság ügyfelei számára olyan alkalmazásokat és szoftverrendszereket fejleszt, amelyek magában foglalhatják az ügyfelek saját érintettjeinek – beleértve a fejlesztett alkalmazások végfelhasználóit – személyes adataihoz való hozzáférést, azok kezelését vagy feldolgozását.

2. Cél és hatály

2.1 Cél

Jelen Adatvédelmi Szabályzat (a továbbiakban: „Szabályzat") belső irányítási dokumentum, amely meghatározza azokat az elveket, szabályokat és szervezeti kereteket, amelyeken keresztül a Társaság biztosítja az alkalmazandó adatvédelmi jogszabályoknak való megfelelést. Célja:

- A Társaság adatvédelmi elveinek és elkötelezettségeinek rögzítése
- Az adatvédelemmel kapcsolatos szerepek és felelősségek meghatározása
- Az adatkezelési tevékenységek és jogalapjaik áttekintése
- Az érintettek jogainak és a kérelmek kezelésére vonatkozó eljárásoknak a leírása
- A személyes adatok védelmét szolgáló biztonsági intézkedések meghatározása
- A magyar jogszabályi követelményeknek megfelelő adatmegőrzési időtartamok rögzítése
- Adatvédelmi incidens-bejelentési eljárások létrehozása
- A beépített és alapértelmezett adatvédelem elveinek beépítése a szoftverfejlesztési életciklusba
- Az adatkezelési tevékenységek nyilvántartásának és az adatvédelmi hatásvizsgálatoknak az alkalmazása
- Folyamatos megfelelési felülvizsgálati mechanizmus kialakítása

2.2 Hatály és alkalmazhatóság

Jelen Szabályzat hatálya kiterjed minden olyan rendszerre, alkalmazásra, adatbázisra, eszközre, személyre és folyamatra, amely a Társaság információs rendszereinek részét képezi vagy azokkal kapcsolatba kerül. Ez magában foglalja az összes munkavállalót, a vezetőséget, a vállalkozókat, tanácsadókat, beszállítókat és egyéb harmadik feleket, akik hozzáférnek a Társaság által kezelt személyes adatokhoz.

A jelen Szabályzat hatálya alá tartozó személyeket a továbbiakban „Felhasználók"-nak nevezzük. A Szabályzatot minden Felhasználó számára elérhetővé kell tenni, és az új munkavállalók bevezetési (onboarding) dokumentációjának részét képezi.

3. Fogalommeghatározások

Jelen Szabályzat alkalmazásában az alábbi fogalmak a következő jelentéssel bírnak:

Személyes adat: azonosított vagy azonosítható természetes személyre (érintettre) vonatkozó bármely információ. Azonosítható az a természetes személy, aki közvetlenül vagy közvetve azonosítható, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján.

Személyes adatok különleges kategóriái: faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre, szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok, valamint a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó adatok.

Adatkezelés: a személyes adatokon végzett bármely művelet vagy műveletek összessége, amelyet automatizált vagy nem automatizált módon végeznek, például gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

Adatkezelő: az a szervezet, amely önállóan vagy másokkal együtt meghatározza a személyes adatok kezelésének céljait és eszközeit.

Adatfeldolgozó: az a szervezet, amely az adatkezelő nevében és utasításai alapján személyes adatokat kezel.

Al-adatfeldolgozó: az adatfeldolgozó által megbízott szervezet, amely az adatkezelő nevében meghatározott adatkezelési tevékenységeket végez, az adatkezelő jóváhagyásával.

Érintett: az a természetes személy, akinek személyes adatait a Társaság kezeli.

Hozzájárulás: az érintett akaratának önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel nyilatkozat vagy egyértelmű megerősítő cselekedet útján jelzi, hogy beleegyezését adja személyes adatainak kezeléséhez.

Adatvédelmi incidens: a biztonság sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Adatvédelmi Koordinátor („AVK"): a Társaság vezetősége által kijelölt személy, aki folyamatosan felügyeli az adatvédelmi megfelelést, és belső és külső kapcsolattartó pontként szolgál adatvédelmi kérdésekben. (Lásd 4. fejezet.)

Adatvédelmi hatásvizsgálat („adatvédelmi hatásvizsgálat"): olyan folyamat, amely segít azonosítani és minimálisra csökkenteni egy projekt vagy adatkezelési tevékenység adatvédelmi kockázatait.

Adatkezelési tevékenységek nyilvántartása („adatkezelési nyilvántartás"): a szervezet által végzett valamennyi adatkezelési tevékenység hivatalos nyilvántartása a GDPR 30. cikke szerint. A Társaság számára jelenleg nem kötelező (lásd 10.1 pont).

NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság, a magyarországi felügyeleti hatóság.

4. Szerepek és felelősségek

4.1 Vezetőség

A Társaság ügyvezetője viseli az adatvédelmi megfelelésért való átfogó felelősséget. A vezetőség jóváhagyja jelen Szabályzatot, megfelelő erőforrásokat biztosít annak végrehajtásához, és gondoskodik arról, hogy az adatvédelem beépüljön a Társaság üzleti működésébe és szoftverfejlesztési tevékenységeibe.

4.2 Adatvédelmi Koordinátor

Bár a Társaság jogilag nem köteles adatvédelmi tisztviselőt (DPO) kinevezni a GDPR 37–39. cikkei alapján – mivel nem közhatóság, nem végez nagymértékű rendszeres megfigyelést, és nem kezel különleges adatkategóriákat nagymértékben –, a Társaság felismeri az adatvédelmi elszámoltathatóság egyetlen, egyértelmű pontjának fontosságát.

Ennek megfelelően a Társaság Adatvédelmi Koordinátort (AVK) jelöl ki, akinek feladatai:

- A vezetőség és valamennyi Felhasználó tájékoztatása az adatvédelmi jogszabályok szerinti kötelezettségeikről
- A GDPR-nak, az Infotörvénynek és jelen Szabályzatnak való megfelelés nyomon követése
- Az érintetti kérelmek kezelésének felügyelete és az időben történő válaszadás biztosítása
- A dedikált adatvédelmi e-mail cím kezelése és az összes beérkező kommunikáció azonnali áttekintése
- Az adatvédelmi incidensek értékelésének, kezelésének és bejelentési eljárásainak koordinálása
- Az adatkezelési tevékenységek nyilvántartására (adatkezelési nyilvántartás) vonatkozó kötelezettség időszakos felülvizsgálata és szükség esetén annak bevezetése
- Adatvédelmi hatásvizsgálatokra (adatvédelmi hatásvizsgálat) vonatkozó iránymutatás nyújtása
- A beépített adatvédelem elveinek integrálása a Társaság fejlesztési életciklusába
- Időszakos megfelelési felülvizsgálatok és auditok lefolytatása vagy koordinálása
- Adatvédelmi tudatossági képzések megszervezése valamennyi munkatárs számára
- Kapcsolattartás a NAIH képviselőivel és az ügyfelekkel adatvédelmi kérdésekben

Ez a Társaság méretére tekintettel részmunkaidős szerep is lehet egyéb feladatok mellett. Az AVK-t időben és megfelelő módon be kell vonni minden személyes adatok védelmével kapcsolatos ügybe. Az AVK elérhetőségét valamennyi munkatársnak, érintettnek és a felügyeleti hatóságnak elérhetővé kell tenni.

4.3 Valamennyi Felhasználó

Minden Felhasználó felelős azért, hogy a feladatai során általa elért vagy kezelt személyes adatokat jelen Szabályzattal és az alkalmazandó jogszabályokkal összhangban kezelje. A Felhasználók kötelességei:

- Személyes adatokat kizárólag engedélyezett célokra és dokumentált utasítások szerint kezelni
- Bármely feltételezett vagy tényleges adatvédelmi incidenst haladéktalanul jelenteni az AVK-nak
- Bármely beérkező érintetti kérelmet azonnal továbbítani az AVK-nak
- A személyes adatok bizalmas kezelése és jogosulatlan személyek számára történő kiadás tilalma
- Beépített adatvédelmi elvek alkalmazása személyes adatokat kezelő szoftverek vagy rendszerek fejlesztésekor
- A kötelező adatvédelmi képzések elvégzése

4.4 A Társaság GDPR szerinti szerepe

A GDPR alapján a Társaság kettős minőségben működik:

Adatkezelőként (24. cikk): saját munkavállalói, ügyfélkapcsolattartói, weboldal-látogatói, potenciális ügyfelei és beszállítói személyes adatainak kezelésekor, saját meghatározott céljaira.

Adatfeldolgozóként (28. cikk): szoftveralkalmazások fejlesztésekor ügyfelek számára, karbantartás, tesztelés és IT-szolgáltatások nyújtása során, ahol az ügyféladatok az ügyfél saját érintettjeinek – beleértve a fejlesztett alkalmazások végfelhasználóit – személyes adatait tartalmazhatják. Ebben a minőségben a Társaság kizárólag az adatkezelő (ügyfél) utasításai alapján és a vonatkozó Adatfeldolgozási Szerződésnek megfelelően kezeli a személyes adatokat.

Ez a kettős szerep megköveteli mind az adatkezelői kötelezettségekre (transzparencia, jogszerű adatkezelés, érintetti jogok), mind az adatfeldolgozói kötelezettségekre (kizárólag dokumentált utasítások alapján való eljárás, megfelelő biztonság biztosítása, bizalmas kezelés, az adatkezelő megfelelésének támogatása) való fokozott odafigyelést.

5. Adatvédelmi alapelvek

A Társaság biztosítja, hogy valamennyi személyesadat-kezelési tevékenysége megfelel a GDPR 5. cikkében foglalt következő alapelveknek:

- **Jogszerűség, tisztességesség és átláthatóság:** A személyes adatokat jogszerűen, tisztességesen és az érintett számára átlátható módon kell kezelni.
- **Célhoz kötöttség:** A személyes adatokat meghatározott, egyértelmű és jogszerű célból kell gyűjteni, és azokat nem szabad e célokkal össze nem egyeztethető módon tovább kezelni.
- **Adattakarékosság:** A személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek, relevásnak és a szükségesre korlátozottnak kell lenniük.
- **Pontosság:** A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük. Minden ésszerű intézkedést meg kell tenni annak érdekében, hogy a pontatlan adatok haladéktalanul törlésre vagy helyesbítésre kerüljenek.
- **Korlátozott tárolhatóság:** A személyes adatokat olyan formában kell tárolni, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges

ideig teszi lehetővé. A Társaságra vonatkozó konkrét megőrzési időtartamokat a 11. fejezet és az 1. számú melléklet tartalmazza.
- **Integritás és bizalmas jelleg:** A személyes adatokat úgy kell kezelni, hogy megfelelő biztonságuk garantált legyen, beleértve a jogosulatlan vagy jogellenes adatkezeléssel, valamint a véletlen elvesztéssel, megsemmisítéssel vagy károsodással szembeni védelmet, megfelelő technikai és szervezeti intézkedések alkalmazásával.
- **Elszámoltathatóság:** A Társaság felelős a fenti elveknek való megfelelésért, és képesnek kell lennie ennek igazolására.

6. Az adatkezelés jogalapjai

A Társaság biztosítja, hogy minden adatkezelési tevékenység a GDPR 6. cikk (1) bekezdésében meghatározott jogalapok legalább egyikén alapuljon:

- **Hozzájárulás:** az érintett egyértelmű hozzájárulását adta személyes adatainak egy vagy több meghatározott célból történő kezeléséhez.
- **Szerződés:** az adatkezelés az érintettel kötött szerződés teljesítéséhez, vagy a szerződéskötést megelőző lépések meghozatalához szükséges.
- **Jogi kötelezettség:** az adatkezelés a Társaságra vonatkozó jogi kötelezettség teljesítéséhez szükséges (pl. magyar munkajog, adójog, számviteli kötelezettségek).
- **Létfontosságú érdekek:** az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges.
- **Közérdek:** az adatkezelés közérdekű feladat végrehajtásához szükséges.
- **Jogos érdek:** az adatkezelés a Társaság vagy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett érdekei, jogai és szabadságai.

A személyes adatok különleges kategóriáinak kezelése kizárólag a GDPR 9. cikkében meghatározott további feltételek teljesülése esetén megengedett, beleértve azt az esetet, amikor az adatkezelés a foglalkoztatás és a szociális biztonság területén fennálló kötelezettségek teljesítéséhez szükséges, vagy az érintett kifejezett hozzájárulását adta.

Az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról szóló 2003. évi CXXV. törvény (Egyenlő bánásmód tv.) 8. §-a alapján a különleges adatkategóriák gyűjtése sokszínűségi monitoring céljából nem megengedett, mivel az diszkriminatívnak minősülhet. A NAIH Foglalkoztatási iránymutatása továbbá rögzíti, hogy munkavállalóktól és pályázóktól kizárólag a munkakörrel kapcsolatos információk gyűjthetők, amelyek nem terjedhetnek ki a magánéletre, kapcsolatokra, családi életre vagy vallásra.

Adatfeldolgozói minőségben a Társaság a személyes adatokat kizárólag az adatkezelő (ügyfél) dokumentált utasításai alapján kezeli. Az adatkezelés jogalapjáért ilyen esetekben az adatkezelő felel.

6.1 Hozzájárulás-kezelés

Amennyiben az adatkezelés jogalapja a hozzájárulás, a Társaság biztosítja, hogy:

- A hozzájárulás egyértelmű, tevőleges cselekedettel történik és dokumentált
- Az érintettet tájékoztatják arról, hogy hozzájárulását bármikor visszavonhatja, és a visszavonás ugyanolyan egyszerű, mint a hozzájárulás megadása
- 16. életévüket be nem töltött kiskorúak esetén a hozzájárulást a szülői felelősséget viselő személy adja meg vagy hagyja jóvá
- A hozzájárulási űrlapokat használatuk előtt az AVK hagyja jóvá

Adatfeldolgozói minőségben a hozzájárulás beszerzése az adatkezelő feladata. A Társaság e tekintetben az adatkezelő utasításait követi.

7. Érintetti jogok

A Társaság tiszteletben tartja és biztosítja a GDPR szerinti érintetti jogokat. Az érintettek jogaikat a dedikált adatvédelmi e-mail címen keresztül az AVK-hoz intézett kérelemmel gyakorolhatják. Bármely érintetti kérelmet – akár Felhasználó, akár a Társaság nevében adatot kezelő harmadik fél érkeztetett – haladéktalanul tovább kell ítani az AVK-nak.

7.1 A kérelmek kezelésének eljárása

Érintetti kérelem beérkezésekor az AVK:

- Szükség esetén ellenőrzi az érintett személyazonosságát
- Nyilvántartásba veszi a kérelmet és koordinál az érintett szervezeti egységekkel az összes érintett személyes adat azonosítása érdekében
- A kérelem kézhezvételétől számított egy hónapon belül írásban válaszol
- Komplex vagy nagyszámú kérelem esetén a válaszadási határidőt további két hónappal meghosszabbíthatja, erről az érintettet az első egy hónapon belül tájékoztatva
- A választ díjmentesen adja meg, kivéve ha a kérelem nyilvánvalóan megalapozatlan, túlzott vagy ismétlődő, amely esetben ésszerű díj számítható fel, vagy a kérelem indokolt megtagadására kerülhet sor

Az AVK valamennyi érintetti kérelmet és azok eredményét nyilvántartja és dokumentálja.

7.2 Jogok áttekintése

Hozzáféréshez való jog (15. cikk): Az érintett jogosult arra, hogy visszajelzést kapjon arról, hogy személyes adatainak kezelése folyamatban van-e, és ha igen, jogosult a személyes adatokhoz és az adatkezeléssel kapcsolatos információkhoz való hozzáféréshez, beleértve az adatkezelés céljait, az érintett adatkategóriákat, a címzetteket, a megőrzési időtartamokat és az adatok forrását. Az érintett kérheti adatai másolatát elektronikus formátumban.

Helyesbítéshez való jog (16. cikk): Az érintett kérheti a pontatlan személyes adatok helyesbítését vagy a hiányos adatok kiegészítését.

Törléshez való jog (17. cikk): Az érintett kérheti személyes adatainak törlését, amennyiben azok a gyűjtés céljához már nem szükségesek, a hozzájárulását visszavonja, tiltakozással él, az adatkezelés jogellenes, vagy a törlést jogszabály írja elő. Ez a jog nem érvényesülhet, ha a megőrzés jogi kötelezettség teljesítéséhez vagy jogi igények előterjesztéséhez, érvényesítéséhez, illetőleg védelméhez szükséges.

Az adatkezelés korlátozásához való jog (18. cikk): Az érintett kérheti az adatkezelés korlátozását, ha a pontosságot vitatja, az adatkezelés jogellenes, a Társaságnak már nincs szüksége az adatokra, de az érintett jogi igényekhez igényli azokat, vagy tiltakozást nyújtott be.

Adathordozhatósághoz való jog (20. cikk): Az érintett jogosult arra, hogy a rá vonatkozó személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, és kérheti ezek közvetlen továbbítását másik adatkezelőnek, amennyiben az adatkezelés hozzájáruláson vagy szerződésen alapul és automatizált módon történik.

Tiltakozáshoz való jog (21. cikk): Az érintett jogosult tiltakozni a jogos érdeken vagy közérdeken alapuló adatkezelés ellen, beleértve a profilalkotást. A Társaság megszünteti az adatkezelést,

kivéve, ha kényszerítő erejű jogos okokat igazol, amelyek elsőbbséget élveznek az érintett érdekeivel szemben.

Automatizált döntéshozatal alóli mentesülés joga (22. cikk): Az érintett jogosult arra, hogy ne terjedjen ki rá olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy hasonlóképpen jelentősen érintené.

7.3 Adatfeldolgozói kötelezettségek az érintetti jogok tekintetében

Adatfeldolgozói minőségben a Társaság segíti az adatkezelőt az érintetti kérelmek megválaszolására vonatkozó kötelezettségeinek teljesítésében. Ha a Társaság közvetlenül kap érintetti kérelmet az adatkezelő nevében kezelt adatokkal kapcsolatban, az AVK haladéktalanul tájékoztatja az érintett adatkezelőt, és a kérelemre nem válaszol közvetlenül, kivéve, ha erre az adatkezelő utasítja.

8. Technikai és szervezeti biztonsági intézkedések

A Társaság a kockázatnak megfelelő szintű biztonságot biztosító megfelelő technikai és szervezeti intézkedéseket hajt végre, figyelembe véve a tudomány és technológia állását, a megvalósítás költségeit, az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint az érintettek jogait és szabadságait érintő kockázat valószínűségét és súlyosságát.

8.1 Technikai intézkedések

A Társaság technikai biztonsági intézkedései közé tartoznak, de nem korlátozódnak az alábbiakra:

- Hozzáférés-szabályozás, amely biztosítja, hogy a rendszerekhez és adatokhoz kizárólag arra jogosult személyzet férjen hozzá egyedi azonosítókkal
- Többtényezős hitelesítés a kritikus rendszerekhez való hozzáféréshez, ahol alkalmazható
- Adatok titkosítása továbbítás során és szükség esetén nyugalmi állapotban
- Hálózati biztonsági intézkedések, beleértve a tűzfalakat, behatolásérzékelést és forgalomellenőrzést
- Biztonságos szoftverfejlesztési gyakorlatok, beleértve a kódátvizsgálást és sebezhetőségi tesztelést
- Biztonsági mentési és katasztrófa-helyreállítási eljárások
- Eszközbiztonsági intézkedések, beleértve a végponti védelmet és távoli törlési képességet
- Fejlesztési környezetek és forráskód-tárolók biztonságos konfigurálása
- Rendszeres biztonsági frissítések és javítócsomag-kezelés

8.2 Szervezeti intézkedések

A Társaság szervezeti biztonsági intézkedései:

- Hozzáférés-szabályozási irányelvek, amelyek biztosítják, hogy a személyes adatokhoz kizárólag az arra jogosult Felhasználók férjenek hozzá a szükséges mértékben (need-to-know elv)
- Titoktartási kötelezettség valamennyi munkavállaló és vállalkozó számára
- Rendszeres adatvédelmi tudatossági képzés valamennyi munkatárs részére

- Biztonságos tárolás: a személyes adatokat tartalmazó dokumentumokat biztonságosan kell tárolni; az íróasztalokat érzékeny dokumentumoktól meg kell tisztítani, ha felügyelet nélkül maradnak
- Személyes adatok személyes eszközökre, magán e-mail fiókokba vagy engedélyezetlen felhőtárhelyre való átvitelének tilalma az AVK engedélye nélkül
- A Társaság vagy ügyfelek tevékenységével kapcsolatos dokumentumok, információk vagy adatok fényképezésének vagy filmezésének tilalma
- A már nem szükséges személyes adatok biztonságos megsemmisítési és törlési eljárásai
- Fejlesztési, tesztelési és éles környezetek elkülönítése a személyes adatok kitételének minimálisra csökkentése érdekében
- Incidens-kezelési eljárások a jelen Szabályzat 9. fejezetének megfelelően

8.3 Beépített és alapértelmezett adatvédelem

A GDPR 25. cikkével összhangban a Társaság az adatvédelmi szempontokat az új rendszerek, szolgáltatások és folyamatok tervezésébe kezdettől fogva integrálja (beépített adatvédelem). Alapértelmezés szerint kizárólag az egyes konkrét adatkezelési célokhoz szükséges személyes adatok kezelésére kerül sor (alapértelmezett adatvédelem). Ez vonatkozik a gyűjtött adatok mennyiségére, az adatkezelés terjedelmére, a tárolás időtartamára és az adatok hozzáférhetőségére.

8.4 Beépített adatvédelem a szoftverfejlesztési életciklusban

Tekintettel a Társaság fő tevékenységére (mobilalkalmazás-fejlesztés és egyéni szoftver), a beépített adatvédelmet a teljes fejlesztési életciklus során érvényesíteni kell. Az alábbi gyakorlatok alkalmazandók:

8.4.1 Projektindítási fázis

- Minden új projekt elején Adatvédelmi Ellenőrzőlista kitöltése annak megállapítására, hogy az alkalmazás vagy rendszer személyes adatokat fog-e kezelni
- Személyes adatok kezelése esetén az AVK-val való egyeztetés az adatvédelmi hatások felmérésére
- A Társaság (mint adatfeldolgozó) és az ügyfél (mint adatkezelő) adatvédelmi felelősségének tisztázása és dokumentálása a projekt hatókörében és az Adatfeldolgozási Szerződésben
- Előzetes értékelés arról, hogy szükséges-e adatvédelmi hatásvizsgálat a projekthez

8.4.2 Tervezési és architektúra fázis

- Az adattakarékosság legyen alapvető tervezési elv: az alkalmazások kizárólag a funkcióhoz szigorúan szükséges személyes adatokat gyűjtsék
- A célhoz kötöttség beépítése az architektúrába: az egyik célra gyűjtött adatok ne legyenek műszakilag elérhetők összeegyeztethetetlen célokra további szabályozás nélkül
- A hozzáférés-szabályozás kezdettől való beépítése az alkalmazásba, szerepalapú hozzáférés és legkisebb jogosultság elvével
- Adatmegőrzési mechanizmusok beépítése a tervezésbe, beleértve az automatizált törlési vagy anonimizálási funkciókat
- Titkosítási és álnevezési technikák értékelése és alkalmazása

8.4.3 Fejlesztési és tesztelési fázis

- Valós személyes adatok fejlesztési vagy tesztelési környezetben való használata kizárólag feltétlenül szükséges esetben, az AVK és az ügyfél engedélyével
- Tesztadatok szükségessége esetén lehetőség szerint anonimizált vagy szintetikus adatok használata
- Forráskód átvizsgálata adatvédelmi sebezhetőségekre: túlzott adatgyűjtés, nem megfelelő hozzáférés-szabályozás, nem biztonságos adattárolás és személyes adatok naplózása
- Biztonsági tesztelés a személyes adatok kezelésének értékelésével, beleértve az injekciós sebezhetőségeket, hitelesítési gyengeségeket és adatkitételi kockázatokat

8.4.4 Üzembe helyezési és karbantartási fázis

- A projekt befejezését vagy megszűnését követően az ügyfél által fejlesztéshez és teszteléshez biztosított valamennyi személyes adatot biztonságosan törölni kell vagy vissza kell adni az AFSZ-nek megfelelően
- A fejlesztési környezeteket, staging szervereket és tárolókat felül kell vizsgálni és meg kell tisztítani a megmaradt személyes adatoktól
- A folyamatos karbantartási tevékenységekre ugyanazon beépített adatvédelmi elvek vonatkoznak, és a személyes adatok kezelését érintő változtatásokat adatvédelmi hatás szempontjából értékelni kell

8.4.5 Dokumentáció

A fejlesztési életciklus során hozott adatvédelmi döntéseket és szempontokat a projektdokumentációban kell rögzíteni. Ez támogatja az elszámoltathatóság elvét, és lehetővé teszi a Társaság számára, hogy ügyfelei felé igazolja a beépített adatvédelem alkalmazását a projekt egészében.

9. Adatvédelmi incidenskezelés

9.1 Incidensészlelés és bejelentés

Valamennyi Felhasználó köteles bármely feltételezett vagy megerősített adatvédelmi incidenst indokolatlan késedelem nélkül bejelenteni az AVK-nak a dedikált adatvédelmi e-mail címen. A bejelentésnek a lehetőségekhez mérten tartalmaznia kell:

- Az incidens jellegének leírását
- Az érintett érintetti kategóriákat és közelítő számukat
- Az érintett személyesadat-nyilvántartások kategóriáit és közelítő számukat
- Az incidens várható következményeinek leírását
- Az incidens kezelésére és hatásainak enyhítésére tett vagy javasolt intézkedések leírását

Adatvédelmi incidensek példái közé tartoznak, de nem korlátozódnak a következőkre: személyes adatokat tartalmazó rendszerekhez való jogosulatlan hozzáférés; adatok véletlen továbbítása nem szándékolt címzettnek; személyes adatokat tartalmazó eszközök vagy dokumentumok elvesztése vagy eltulajdonítása; személyes adatokat érintő malware- vagy zsarolóvírus-incidensek; személyes adatokat tartalmazó forráskód-tárolók kompromittálódása; rosszindulatú szoftver telepítése a Társaság eszközeire; valamint bármely kötelező biztonsági kontroll megsértése, amely személyes adatok elvesztéséhez vagy kompromittálódásához vezethet.

9.2 Értékelés és válaszintézkedések

Az incidensbejelentés beérkezésekor az AVK:

- Értékelést indít annak megállapítására, hogy az esemény a GDPR szerinti adatvédelmi incidensnek minősül-e
- Dokumentálja az értékelést, beleértve az incidenssel kapcsolatos valamennyi tényt, annak hatásait és a megtett korrekciós intézkedéseket
- Ha az esemény nem minősül incidensnek, az előzetes értékelést a nyilvántartás számára dokumentálja
- Ha az esemény incidensnek minősül, kockázatértékelést végez az érintettek jogait és szabadságait érintő kockázat valószínűségének és súlyosságának megállapítására

9.3 Bejelentés a felügyeleti hatóságnak (33. cikk)

Amennyiben az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a Társaság indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb az incidensről való tudomásszerzést követő 72 órán belül bejelenti azt a NAIH képviselőinek. Ha a bejelentés nem történik meg 72 órán belül, a késedelem okát is meg kell adni.

9.4 Az érintettek tájékoztatása (34. cikk)

Amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a Társaság indokolatlan késedelem nélkül, világos és közérthető nyelven tájékoztatja az érintetteket.

9.5 Adatfeldolgozói kötelezettségek incidens esetén

Adatfeldolgozói minőségben a Társaság indokolatlan késedelem nélkül értesíti az érintett adatkezelőt, amennyiben ügyféladatokat érintő adatvédelmi incidensről tudomást szerez. A felügyeleti hatóság és az érintettek felé történő bejelentési kötelezettség az adatkezelőt terheli; a Társaság azonban az AFSZ-ben előírtak szerint minden szükséges segítséget és információt megad.

9.6 Incidensnyilvántartás

Az AVK nyilvántartást vezet valamennyi adatvédelmi incidensről, beleértve azokat is, amelyek nem igényeltek bejelentést a felügyeleti hatóság felé. A nyilvántartás tartalmazza az incidenssel kapcsolatos tényeket, annak hatásait és a megtett korrekciós intézkedéseket. A nyilvántartás frissítését a vezetőség vizsgálja felül és hagyja jóvá.

10. Adatkezelési tevékenységek nyilvántartása és hatásvizsgálatok

10.1 Adatkezelési tevékenységek nyilvántartása (30. cikk)

A GDPR 30. cikk (5) bekezdése értelmében az adatkezelési tevékenységek nyilvántartásának (adatkezelési nyilvántartás) vezetésére vonatkozó kötelezettség nem vonatkozik a 250 főnél kevesebb személyt foglalkoztató szervezetekre, kivéve, ha az adatkezelés valószínűsíthetően kockázatot jelent az érintettek jogaira és szabadságaira, az adatkezelés nem alkalmi jellegű, vagy

az adatkezelés különleges adatkategóriákra vagy bűncselekményekre vonatkozó adatokra terjed ki.

A Társaság jelenlegi méretére (9–15 fő), tevékenységeinek jellegére és adatkezelési tevékenységeinek hatókörére tekintettel jelenleg nem köteles formális adatkezelési nyilvántartást vezetni. Amennyiben a Társaság körülményei megváltoznak – különösen létszámnövekedés, az adatkezelési tevékenységek bővülése vagy különleges adatkategóriákat érintő adatkezelés bevezetése esetén –, az AVK újraértékeli ezt a kötelezettséget és szükség esetén bevezeti az adatkezelési nyilvántartást.

A fentiektől függetlenül a Társaság megfelelő belső dokumentációt vezet adatkezelési tevékenységeiről jelen Szabályzaton, az Adatmegőrzési Nyilvántartáson (1. sz. melléklet), az Adatvédelmi Tájékoztatón és az ügyfelekkel kötött Adatfeldolgozási Szerződéseken keresztül.

10.2 Adatvédelmi hatásvizsgálat (35. cikk)

Amennyiben egy adatkezelési típus – különösen új technológiák alkalmazása esetén – valószínűsíthetően magas kockázatot jelent a természetes személyek jogaira és szabadságaira, a GDPR előírja, hogy a Társaság az adatkezelést megelőzően adatvédelmi hatásvizsgálatot (adatvédelmi hatásvizsgálat) végezzen. A Társaság jelenlegi adatkezelési tevékenységei alapján jelenleg nem szükséges adatvédelmi hatásvizsgálat.

Azonban a Társaság szoftverfejlesztői szerepe miatt előfordulhat, hogy az ügyfelek számára fejlesztett alkalmazások igényelnek adatvédelmi hatásvizsgálatot. Az AVK tájékoztatja az ügyfeleket a adatvédelmi hatásvizsgálati követelményeiről és szükség esetén segítséget nyújt az AFSZ-nek megfelelően.

Amennyiben a jövőben adatvédelmi hatásvizsgálat elvégzése szükségessé válik, a Társaság a francia adatvédelmi hatóság (Commission Nationale de l'Informatique et des Libertés – CNIL) által közzétett adatvédelmi hatásvizsgálati sablont használja, amely szabadon elérhető és az EU-ban széles körben elismert referenciamódszertanként. Az AVK koordinálja az adatvédelmi hatásvizsgálat lefolytatását, és amennyiben a vizsgálat magas maradékkockázatot jelez, az adatkezelést megelőzően egyeztet a NAIH képviselőivel.

11. Adatmegőrzés

11.1 Általános elvek

A személyes adatokat kizárólag az adatkezelés céljához szükséges ideig, vagy az alkalmazandó magyar és uniós jogszabályok által előírt ideig kell megőrizni. A Társaság a korlátozott tárolhatóság elvét alkalmazza, biztosítva, hogy a személyes adatok ne legyenek azonosítható formában a szükségesnél tovább tárolva.

A Társaság által kezelt személyes adatok egyes kategóriáira vonatkozó konkrét megőrzési időtartamokat az 1. számú melléklet – Adatmegőrzési Nyilvántartás tartalmazza. Az 1. sz. melléklet képezi a Társaság végleges megőrzési nyilvántartását, és egyetlen alkalmazandó megőrzési időtartamot határoz meg minden egyes nyilvántartási típushoz. A nyilvántartás a magyar jogszabályi követelményeken alapul, különösen:

- 2000. évi C. törvény a számvitelről (Számviteli tv.) – 8 éves megőrzés számviteli bizonylatokra
- 2017. évi CL. törvény az adózás rendjéről (Art.) – adómegállapítási elévülési idők

- 2012. évi I. törvény a munka törvénykönyvéről (Mt.) – 3 éves elévülési idő munkajogi igényekre
- A társadalombiztosításról szóló törvény – nyugdíjjal kapcsolatos dokumentumok megőrzése
- 1993. évi XCIII. törvény a munkavédelemről (Mvt.) és az 5/1993. (XII. 26.) MüM rendelet – baleseti nyilvántartások és kitettségi nyilvántartások
- 33/1998. (VI. 24.) NM rendelet az orvosi vizsgálatokról – 30/40 éves megőrzés orvosi nyilvántartásokra
- 1997. évi CLV. törvény a fogyasztóvédelemről (Fgytv.) – ügyfélpanaszok és levelezés
- 2013. évi V. törvény a Polgári Törvénykönyvről (Ptk.) – 5 éves általános elévülési idő polgári jogi igényekre
- 2008. évi XLVIII. törvény a gazdasági reklámtevékenységről (Reklámtv.) – direkt marketing hozzájárulási nyilvántartások
- 2017. évi LXXVIII. törvény az ügyvédi tevékenységről (Ügyvédi tv.) – társasági iratok megőrzése
- 2003. évi CXXV. törvény az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról (Egyenlő bánásmód tv.) – különleges adatgyűjtés korlátozásai
- NAIH Munkahelyi adatkezelési követelmények iránymutatása – munkavállalói és pályázói adatkezelésre vonatkozó iránymutatás

Amennyiben ugyanazon adatra több megőrzési időtartam is vonatkozik, a leghosszabb alkalmazandó időtartamot kell alkalmazni.

11.2 Megőrzés adatkezelői minőségben

Az AVK felelős a személyes adatok egyes kategóriáira vonatkozó megőrzési időtartam meghatározásáért, a megőrzési időtartamok dokumentálásáért és az érintett szervezeti egységek tájékoztatásáért, az érintett szervezeti egységekkel való koordinációért annak biztosítása érdekében, hogy a lejárt megőrzési idejű személyes adatokat már ne használják működési célokra, valamint a személyes adatok biztonságos törléséért vagy anonimizálásáért a vonatkozó megőrzési időtartam lejártakor.

11.3 Megőrzés adatfeldolgozói minőségben

Adatfeldolgozói minőségben a Társaság az ügyfél személyes adatait kizárólag az adott adatkezelővel kötött Adatfeldolgozási Szerződésben (AFSZ) meghatározott ideig őrzi meg. Az AFSZ megszűnésekor vagy az adatkezelő utasítására a Társaság az összes személyes adatot visszaadja az adatkezelőnek vagy biztonságosan törli, kivéve, ha jogszabály megőrzést ír elő.

11.4 Fejlesztési projektadatok megőrzése

A Társaság szoftverfejlesztési alaptevékenységére tekintettel különös figyelmet kell fordítani a fejlesztési környezetekben, tesztadatbázisokban, forráskód-tárolókban, staging szervereken és projektdokumentációkban található személyes adatokra. A következő elvek érvényesek:

- Az ügyfelek által fejlesztési vagy tesztelési célra biztosított személyes adatokat feldolgozói adatként kell kezelni, és kizárólag a projekt időtartamára vagy az AFSZ-ben meghatározott ideig őrizhetők meg
- A projekt befejezését, átadását vagy megszűnését követően az ügyfél által biztosított valamennyi személyes adatot biztonságosan törölni kell a fejlesztési környezetekből, tesztadatbázisokból, staging szerverekről és mentésekből, kivéve, ha az AFSZ másként rendelkezik

- A forráskód-tárolókat felül kell vizsgálni annak biztosítására, hogy azok nem tartalmaznak személyes adatokat a kódban, konfigurációs fájlokban vagy commit-történetben
- A személyes adatokat tartalmazó projektdokumentációt a projekt lezárásakor felül kell vizsgálni, és a személyes adatokat törölni vagy anonimizálni kell
- A projektadatok törlését dokumentálni kell, és az ügyfelet értesíteni kell

11.5 Rendszeres törlési eljárások

A Társaság rendszeres eljárásokat vezet be a személyes adatok felülvizsgálatára és törlésére, beleértve:

- A megőrzött adatok éves felülvizsgálatát a megőrzési nyilvántartás alapján
- Automatizált emlékeztetőket vagy jelzési mechanizmusokat, ahol megvalósítható
- Dokumentált törlési vagy anonimizálási eljárásokat igazoló nyilvántartásokkal
- Fizikai dokumentumok biztonságos megsemmisítését és elektronikus adatok végleges törlését szolgáló módszereket

12. Harmadik fél és beszállító kezelése

12.1 Adatfeldolgozók megbízása

Amikor a Társaság adatkezelői minőségben személyes adatokhoz hozzáférő harmadik felet bíz meg (például bérszámfejtés, könyvelés, felhő/tárhely-szolgáltatók, IT-támogatás vagy fejlesztőeszközök/platformok), a Társaság:

- Ellenőrzi, hogy a harmadik fél megfelelő garanciákat nyújt az adatvédelmi jognak való megfelelésre, beleértve a megfelelő technikai és szervezeti intézkedéseket
- A GDPR 28. cikkével összhangban Adatfeldolgozási Szerződést köt bármely adatkezelés megkezdése előtt
- Időszakos értékelést végez az adatfeldolgozó folyamatos megfeleléséről, legalább évente
- Az összes AFSZ másolatát az AVK felügyelete alatt őrzi

Személyes adatok Társaság nevében történő kezelését magában foglaló szerződés nem köthető meg az AVK előzetes írásbeli jóváhagyása nélkül.

12.2 Al-adatfeldolgozók kezelése és átvilágítás

Amikor a Társaság adatfeldolgozói minőségben al-adatfeldolgozót bíz meg (pl. felhőszolgáltatások, fejlesztőeszközök, szakosított vállalkozók vagy harmadik fél API-k), a Társaság:

- Előzetes általános vagy eseti engedélyt szerez az adatkezelőtől
- Az al-adatfeldolgozó átvilágítását végzi el a Társaság Al-adatfeldolgozói Átvilágítási Ellenőrzőlistája alapján, értékelve: adatvédelmi irányelveket és gyakorlatokat; AFSZ-kötési hajlandóságot; megvalósított biztonsági intézkedéseket; az adatkezelés és tárolás helyét (EU/nem EU); incidensbejelentési képességeket; valamint releváns tanúsítványokat vagy megfelelési igazolásokat
- Ugyanazon adatvédelmi kötelezettségeket rója az al-adatfeldolgozóra írásbeli megállapodás útján
- Nyilvántartást vezet a jóváhagyott al-adatfeldolgozókról, és kérésre elérhetővé teszi az adatkezelők számára

- Teljes mértékben felel az adatkezelő felé az al-adatfeldolgozó adatvédelmi kötelezettségeinek teljesítéséért

Az éves felülvizsgálatok során kiemelt figyelmet kell fordítani az al-adatfeldolgozói tevékenységekre. Amennyiben egy al-adatfeldolgozó nem teljesíti adatvédelmi kötelezettségeit, a Társaság megfelelő korrekciós intézkedéseket tesz, beleértve szükség esetén az al-adatfeldolgozási jogviszony megszüntetését.

12.3 Nemzetközi adattovábbítás

Személyes adatok az Európai Gazdasági Térségen (EGT) kívülre kizárólag a GDPR V. fejezetében előírt megfelelő garanciák megléte esetén továbbíthatók, például:

- Az Európai Bizottság megfelelőségi határozata
- Az Európai Bizottság által jóváhagyott Általános Szerződési Feltételek (ÁSZF-ek)
- Kötelező erejű vállalati szabályok
- A GDPR 49. cikke szerinti eltérések

Az IT-fejlesztési munka jellegére és a nemzetközi felhőszolgáltatások, fejlesztési platformok és együttműködési eszközök lehetséges használatára tekintettel az AVK Adattovábbítási Feltérképezést végez az összes olyan szolgáltatás és eszköz azonosítására, amely adatokat továbbíthat az EGT-n kívülre, és biztosítja a megfelelő garanciák meglétét.

Adatfeldolgozói minőségben a Társaság tisztázza az ügyfelekkel az adatok tárolási helyére vonatkozó korlátozásokat, és biztosítja, hogy az AFSZ-ek megfelelő továbbítási rendelkezéseket tartalmazzanak. Harmadik országbeli al-adatfeldolgozók igénybevétele esetén a Társaság megfelelő garanciákat (pl. ÁSZF-eket) biztosít.

13. Adatvédelmi kapcsolattartási pont

A Társaság dedikált e-mail címet tart fenn minden adatvédelmi kommunikáció számára: adatvedelem@bitnet.hu.

Az AVK kezeli ezt az e-mail címet, biztosítva az összes beérkező kommunikáció – beleértve az érintetti kérelmeket, az ügyfelek adatvédelmi kérdéseit és a belső bejelentéseket – azonnali áttekintését és feldolgozását.

A munkavállalók és vállalkozók ezt a címet használják bármely adatvédelemmel kapcsolatos kérelemhez vagy bejelentéshez.

14. Képzés és tudatosság

A Társaság adatvédelmi képzési és tudatossági programot valósít meg annak biztosítására, hogy valamennyi Felhasználó ismerje kötelezettségeit. A program magában foglalja:

- Kötelező adatvédelmi tudatossági képzés valamennyi új munkavállaló számára a bevezetési (onboarding) folyamat részeként
- Időszakos ismétlő képzés valamennyi munkatárs részére, legalább évente
- Szerepspecifikus iránymutatás a fejlesztő munkatársaknak, akik szoftverfejlesztési projektek során ügyfél személyes adataihoz férhetnek hozzá, beleértve a beépített adatvédelmi elveket, biztonságos kódolási gyakorlatokat és az anonimizált vagy szintetikus tesztadatok használatát
- Képzés a lehetséges adatvédelmi incidensek felismeréséről és bejelentéséről

- Valamennyi megtartott képzés dokumentálása, beleértve a részvételi nyilvántartást

A képzésnek a Társaság méretére tekintettel nem kell kiterjedtnek lennie, de ki kell terjednie a GDPR alapelveire, a Társaság adatvédelmi irányelveire és az egyes munkavállalók szerepéhez kapcsolódó gyakorlati iránymutatásra. Az AVK felelős a képzési program megtervezéséért, lebonyolításáért és dokumentálásáért.

15. Nyomon követés, felülvizsgálat és folyamatos fejlesztés

15.1 Éves megfelelési felülvizsgálat

Az AVK legalább évente átfogó felülvizsgálatot végez a Társaság adatvédelmi megfeleléséről. A felülvizsgálat kiterjed:

- Jelen Szabályzat és az összes kapcsolódó eljárás megfelelőségére és hatékonyságára
- Az adatkezelési nyilvántartási kötelezettséget vagy adatvédelmi hatásvizsgálati követelményt kiváltó feltételek esetleges változásaira
- A megőrzési időtartamoknak való megfelelésre és a törlési eljárások hatékonyságára
- Az elvégzett adatvédelmi hatásvizsgálatok eredményeire
- A képzések teljesítési arányára és a tudatosság szintjére
- A felülvizsgálati időszak során bekövetkezett adatvédelmi incidensekre és a levont tanulságokra
- Az alkalmazandó jogszabályok, szabályozási iránymutatások vagy hatósági döntések változásaira
- A harmadik felekkel, al-adatfeldolgozókkal és nemzetközi adattovábbításokkal kapcsolatos megfelelésre
- A beépített adatvédelmi gyakorlatok hatékonyságára a fejlesztési életciklusban

15.2 Jelentés a vezetőségnek

Az éves felülvizsgálatot követően, valamint sürgős esetekben (pl. jelentős adatvédelmi incidens), az AVK jelentést nyújt be az ügyvezetőnek, amely kiterjed az azonosított vagy lehetséges meg nem felelésekre és a megtett vagy javasolt korrekciós intézkedésekre, az adatvédelemmel kapcsolatos jelentős kockázatokra vagy problémákra, az elvégzett és ajánlott adatvédelmi hatásvizsgálatokra, az új projektekre vagy adatkezelési tevékenységekre és azok adatvédelmi elveknek való megfelelésére, valamint a szabályzat frissítésére vagy eljárási javításokra vonatkozó javaslatokra.

15.3 A Szabályzat felülvizsgálatát kiváltó események

Az éves felülvizsgálaton túl jelen Szabályzatot a következő események bármelyikét követően felül kell vizsgálni és frissíteni:

- Az alkalmazandó adatvédelmi jogszabályok vagy szabályozási iránymutatások lényeges változásai
- A Társaság üzleti működésének, szolgáltatásainak vagy IT környezetének jelentős változásai
- Jelentős adatvédelmi incidens vagy biztonsági esemény
- Auditok vagy hatósági vizsgálatok megállapításai vagy ajánlásai
- A Társaság kockázati profiljának vagy fenyegetési környezetének változásai
- Bármely egyéb esemény, amelyet az AVK felülvizsgálatot igénylőnek ítél

16. Szabályzatsértés

Jelen Szabályzat megsértését az AVK a vezetőséggel együttműködve vizsgálja ki. A szabályzatsértés a sértés súlyosságával arányos fegyelmi intézkedést vonhat maga után, beleértve, de nem korlátozva:

- Írásbeli figyelmeztetés
- A személyes adatokhoz és információs rendszerekhez való hozzáférés ideiglenes vagy végleges korlátozása
- Kötelező további adatvédelmi képzés
- Munkaviszony vagy szerződéses jogviszony megszüntetése
- Jogi lépések, amennyiben indokolt

17. Dokumentumkezelés

17.1 Hatálybalépés

Jelen Szabályzat az ügyvezető általi jóváhagyás napján lép hatályba.

17.2 Kivételek

A jelen Szabályzat alóli kivételeket az AVK ajánlására az ügyvezető hagyja jóvá írásban. Valamennyi kivételt dokumentálni kell, időbeli korláttal kell ellátni, és felülvizsgálat alá kell vetni.

1. számú melléklet – Adatmegőrzési Nyilvántartás

Az alábbi táblázat meghatározza a Társaság által kezelt személyes adatok valamennyi kategóriájára vonatkozó végleges megőrzési időtartamokat. Amennyiben magyar jogszabály előírja a megőrzési időtartamot, azt alkalmazzák. Amennyiben nincs jogszabályi előírás, a megőrzési időtartam az alkalmazandó elévülési időkön és szabályozási iránymutatásokon alapul. Amennyiben több kötelezettség átfedi egymást, a leghosszabb alkalmazandó időtartamot választottuk.

Ez a melléklet képezi a Társaság mérvadó adatmegőrzési nyilvántartását. Az AVK biztosítja a személyes adatok ezen időtartamok szerinti törlését vagy anonimizálását.

Nyilvántartás típusa	Megőrzési időtartam	Időtartam kezdete	Jogszabályi alap
A. FOGLALKOZTATÁS – SZEMÉLYES ADATOK			
Személyes elérhetőségek (cím, telefon, e-mail)	3 év	Munkaviszony megszűnése	Mt. 286. § (1) bek.
Bankszámla adatok	3 év	Munkaviszony megszűnése	Mt. 286. § (1) bek.
Személyazonosító adatok (teljes név, foglalkozás)	3 év	Munkaviszony megszűnése	Mt. 286. § (1) bek.
Munkavállalási jogosultságra vonatkozó iratok	3 év	Munkaviszony megszűnése	Mt. 286. § (1) bek.
Személyi azonosító számok (TAJ, szem. ig., útlevél)	3 év	Munkaviszony megszűnése	Mt. 286. § (1) bek.
Munkahelyi elérhetőségek (munkakör, e-mail, telefon)	3 év	Munkaviszony megszűnése	Mt. 286. § (1) bek.
Hozzátartozók és vészhelyzeti elérhetőségek	Törlés a munkav. megszűnésekor	Munkaviszony megszűnése	GDPR 5. cikk (1) e) pont
B. FOGLALKOZTATÁS – NAPLÓK ÉS JELENLÉT			
Jelenléti nyilvántartás	3 év	Munkaviszony megszűnése	Mt. 134. § és 286. § (1) bek.
Helyszíni belépési nyilvántartások	3 év	Munkaviszony megszűnése	Mt. 134. § és 286. § (1) bek.
Éves szabadság nyilvántartás	3 év	Munkaviszony megszűnése	Mt. 134. § és 286. § (1) bek.
Munkabaleseti jelentések	5 év	A baleset bekövetkezése	Mvt. 64/A. §; 5/1993. MüM r. 5. §
C. FOGLALKOZTATÁS – EGÉSZSÉGÜGYI NYILVÁNTARTÁSOK			
Orvosi igazolások (foglalkozási alkalmasság)	30 év; 40 év biológiai kitettség	A nyilvántartás létrehozása	33/1998. NM r. 14. § (5)-(6) bek.
Orvosi jelentések	30 év; 40 év biológiai kitettség	A nyilvántartás létrehozása	33/1998. NM r. 14. § (5)-(6) bek.
Munkahelyi alkalmazkodások nyilvántartása	30 év; 40 év biológiai kitettség	A nyilvántartás létrehozása	33/1998. NM r. 14. § (5)-(6) bek.
D. FOGLALKOZTATÁS – BÉR ÉS ADÓ			
Társadalombiztosítási járulékok	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Tb. tv. 99/A. §*
Bérjegyzékek	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Tb. tv. 99/A. §*
Bérekből történő levonások nyilvántartása	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Tb. tv. 99/A. §*

Bruttó és nettó bér nyilvántartás	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Tb. tv. 99/A. §*
Jogszabályi (adó)kedvezmények nyilvántartása	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Tb. tv. 99/A. §*
E. FOGLALKOZTATÁS – NYUGDÍJ			
Eltartottak és kedvezményezettek adatai	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Tb. tv. 99/A. §*
Nyugdíj bérjegyzékek és bérkártyák	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Tb. tv. 99/A. §*
Munkaviszony megszűnését követő választások	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Tb. tv. 99/A. §*
Járulékszint változások nyilvántartása	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Tb. tv. 99/A. §*
Nyugdíjszolgáltatói választások nyilvántartása	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Tb. tv. 99/A. §*
Munkáltatói hozzájárulások nyilvántartása	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Tb. tv. 99/A. §*
F. FOGLALKOZTATÁS – TELJESÍTMÉNY			
Prémiumok	3 év	Munkaviszony megszűnése	Mt. 286. § (1) bek.
Fegyelmi nyilvántartások	3 év	Munkaviszony megszűnése	Mt. 286. § (1) bek.
Panaszok	3 év	Munkaviszony megszűnése	Mt. 286. § (1) bek.
Teljesítménymenedzsment nyilvántartás	3 év	Munkaviszony megszűnése	Mt. 286. § (1) bek.
Előléptetési nyilvántartások	3 év	Munkaviszony megszűnése	Mt. 286. § (1) bek.
G. FOGLALKOZTATÁS – PÁLYÁZÓI ADATOK			
Sikeres pályázók – felvételi dokumentumok	3 év	Munkaviszony megszűnése	Mt. 286. § (1) bek.
Sikeres pályázók – háttérellenőrzés	Törlés az ellenőrzés után	Az ellenőrzés lezárása	Mt. 11. § (3), 44/A. §; NAIH
Sikertelen pályázók – hozzájárulás nélkül	Törlés az elutasításkor	Az elutasítás dátuma	GDPR 5. cikk (1) e); NAIH
Sikertelen pályázók – háttérellenőrzés	Törlés az ellenőrzés után	Az ellenőrzés lezárása	Mt. 11. § (3), 44/A. §; NAIH
Különleges adatok sokszínűségi monitoringhoz	NEM MEGENGEDETT	–	Egyenlő bánásmód tv. 8. §; NAIH
H. MUNKAVÉDELEM			
Munkavédelmi audit jelentések	5 év	Az értékelés időpontja	Mvt. 54. § (5) bek.
Kábítószer/alkohol teszt – pozitív	3 év	A munkaviszony megszűnése	Mt. 286. § (1) bek.
Kábítószer/alkohol teszt – negatív	1 év	A jegyzőkönyv aláírása	Mt. 286. § (1) bek.
Munkavédelmi szabályzatok	3 év	A nyilvántartás létrehozása	Mt. 286. § (1) bek.
Baleseti bejelentések	5 év	A baleset bekövetkezése	Mvt. 64/A. §; 5/1993. MüM r.
Vizsgálati jelentések	5 év	A baleset bekövetkezése	Mvt. 64/A. §; 5/1993. MüM r.

Egészségügyi/orvosi vizsgálatok	30 év; 40 év biol. kitettség	A nyilvántartás létrehozása	33/1998. NM r. 14. § (5)-(6)
Munkavédelmi képviselői egyeztetések	3 év	A nyilvántartás létrehozása	Mt. 286. § (1) bek.
Egészségi állapoton alapuló munkaszervezés	3 év	A munkaviszony megszűnése	Mt. 286. § (1) bek.
Veszélyes anyagok kitettségi nyilvántartás	10 év; 50 év rákkeltő	Megszűnés / utolsó kitettség napja	Mvt. 63/A. § (3), 63/B. § (3)
Kockázatértékelések	5 év	Az értékelés időpontja	Mvt. 54. § (5) bek.
Rutin munkavállalói egészségügyi dok.	3 év	A munkaviszony megszűnése	Mt. 286. § (1) bek.
I. TÁRSASÁGI ÉS PÉNZÜGYI			
Számviteli bizonylatok – pénzügyi kimutatások	8 év	Az üzleti év vége	Számviteli tv. 169. § (2) bek.
Könyvvizsgálati dokumentáció	8 év	Az üzleti év vége	Számviteli tv. 169. § (2) bek.
Alapító okirat / Társasági szerződés	Állandó; majd 10 év	A társaság megszűnése	Ügyvédi tv. 46. § (5)-(6); Ptk. 6:22. §
Igazgatósági ülések jegyzőkönyvei	10 év	A létrehozás dátuma	Ügyvédi tv. 46. § (5)-(6); Ptk. 6:22. §
Vezető tisztségviselők szerződései	5 év	Az igény esedékessé válása	Ptk. 6:22. §
Tagjegyzék / tagi nyilvántartás	10 év	A létrehozás dátuma	Ügyvédi tv. 46. § (5)-(6); Ptk. 6:22. §
Taggyűlési jegyzőkönyvek és határozatok	10 év	A létrehozás dátuma	Ügyvédi tv. 46. § (5)-(6); Ptk. 6:22. §
J. ADÓNYILVÁNTARTÁSOK			
Társasági adó iratok	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Art.
Általános adónyilvántartások	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Art. 202. §
Adóbevallásokhoz kapcsolódó nyilvántartások	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Art.
ÁFA nyilvántartások	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Art.
K. ÉRTÉKESÍTÉS, MARKETING ÉS ÜGYFÉL			
Ügyfélszerződések	5 év	Az igény esedékessé válása	Ptk. 6:22. §
Ügyfélpanasz-napló	3 év	A beérkezés / jegyzőkönyv készítése	Fgytv. 17/A. § (7) bek.
Hívás- és levelezési nyilvántartások	5 év	A nyilvántartás létrehozása	Fgytv. 17/B. § (3) bek.
Direkt marketing adatok – ügyfél	A hozzájárulás visszavonásáig	A hozzájárulás megadása	Reklámtv. 6. § (5) bek.
Direkt marketing adatok – érdeklődő	A hozzájárulás visszavonásáig	A hozzájárulás megadása	Reklámtv. 6. § (5) bek.
Érintetti kérelmek nyilvántartása	5 év	Az igény esedékessé válása	Ptk. 6:22. §; GDPR elszámoltathatóság
Jogalapok nyilvántartása (hozzájárulás, jogos érdek)	5 év	Az igény esedékessé válása	Ptk. 6:22. §
L. ADATFELDOLGOZÓI NYILV. – SZOFTVERFEJLESZTÉS			

Ügyféladatok fejlesztési szerződés alapján	Az adatkezelési megállapodásban meghat. szerint	Az adatkezelés megszűnése	GDPR 28. cikk; vonatkozó AFSZ
Tesztadatok személyes adattal (ügyféltől)	Törlés a projekt befejezésekor	Projekt befejezésétől / Az adatkezelés megszűnése	GDPR 28. cikk; vonatkozó AFSZ
Fejlesztési környezet adatai (adatbázis, staging)	Törlés a projekt befejezésekor	Projekt befejezésétől / Az adatkezelés megszűnése	GDPR 28. cikk; vonatkozó AFSZ
Forráskód-tárolók beágyazott személyes adattal	Felülvizsgálat és törlés a projekt zárásakor	A projekt befejezésétől	GDPR 5. cikk (1) e); beépített adatvéd.
Projektdokumentáció személyes adattal	Felülvizsg. és törlés/anonimiz. a záráskoz	A projekt befejezésétől	GDPR 5. cikk (1) e); vonatkozó AFSZ

* A bér- és nyugdíjnyilvántartásoknál a Számviteli törvény szerinti 8 éves számviteli megőrzési időtartamot alkalmazzuk standard megőrzési időtartamként, mivel az magában foglalja a rövidebb 3 éves munkajogi igények elévülési idejét. Megjegyzés: a társadalombiztosításról szóló törvény 99/A. §-a alapján a 2024. december 31. előtt keletkezett, nyugdíjellátások megállapításához szükséges dokumentumokat a munkavállaló nyugdíjkorhatárának elérésétől számított legalább 5 évig meg kell őrizni. Amennyiben ez 8 évnél hosszabb megőrzési időtartamot eredményez, a hosszabb időtartam az irányadó.

A fent nem szereplő nyilvántartások esetében a megőrzési időtartamot az AVK határozza meg az adatkezelés célja, az alkalmazandó jogszabályi követelmények és a GDPR korlátozott tárolhatóság elvének figyelembevételével. Valamennyi megőrzési döntést dokumentálni kell.

2. számú melléklet – Jogszabályi hivatkozások

Az alábbi magyar és uniós jogszabályok képezik a jelen Szabályzatban és az Adatmegőrzési Nyilvántartásban hivatkozott jogi keretrendszert:

Rövidítés	Teljes megnevezés	Főbb szakaszok	Relevanciája
Számviteli tv.	2000. évi C. törvény a számvitelről	169. § (2) bek.	Számviteli bizonylatok megőrzése (8 év)
Art.	2017. évi CL. törvény az adózás rendjéről	202. §	Adónyilvántartások megőrzése; elévülési idők
Mt.	2012. évi I. törvény a munka törvénykönyvéről	11. § (3), 44/A. §, 134. §, 286. § (1) bek.	Foglalkoztatási nyilvántartások, jelenlét, elévülési idők
Ügyvédi tv.	2017. évi LXXVIII. törvény az ügyvédi tevékenységről	46. § (5) és (6) bek.	Jogi szakemberek által őrzött dokumentumok megőrzése
Ptk.	2013. évi V. törvény a Polgári Törvénykönyvről	6:22. §	Általános polgári jogi igények elévülése (5 év)
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról	Több szakasz	Magyar adatvédelmi törvény
Mvt.	1993. évi XCIII. törvény a munkavédelemről	54. § (5), 63/A. §, 63/B. §, 64/A. §	Munkabaleseti nyilvántartások, veszélyes anyagok
Mvt. vhr.	5/1993. (XII. 26.) MüM rendelet	5. §	Munkabaleseti nyilvántartás végrehajtása
Orvosi vizsg. r.	33/1998. (VI. 24.) NM rendelet az orvosi vizsgálatokról	14. § (5) és (6) bek.	Foglalkozási alkalmasságra vonatkozó orvosi nyilvántartások
Tb. tv.	A társadalombiztosításról szóló törvény	99/A. §	Nyugdíjmegállapításhoz szükséges foglalkoztatási dokumentumok
Egyenlő bánásmód tv.	2003. évi CXXV. tv. az egyenlő bánásmódról	8. §	Diszkriminatív adatgyűjtés tilalma
GDPR	(EU) 2016/679 rendelet (általános adatvédelmi rendelet)	5. cikk (1) e) pont	Adattakarékosság és korlátozott tárolhatóság elve
NAIH Fogl. iránymutatás	NAIH Munkahelyi adatkezelési követelmények iránymutatása	II. rész, 1.2., 1.3. pont	Útmutatás a munkavállalói adatkezeléshez
Reklámtv.	2008. évi XLVIII. tv. a gazdasági reklámtevékenységről	6. § (5) bek.	Direkt marketing hozzájárulási követelmények
Fgytv.	1997. évi CLV. törvény a fogyasztóvédelemről	17/A. § (7), 17/B. § (3) bek.	Ügyfélpanaszok kezelése és megőrzése

Jóváhagyás és aláírások

Dátum: _____

Aláírás: _____

Név: _____