ADATVÉDELMI SZABÁLYZAT

BitMessaging

Cégnév	BitMessaging
Székhely	Budapest, Magyarország
Üzleti tevékenység	Tömeges SMS-átjáró és üzenetküldő szolgáltatások
Weboldal	https://sms.bitnet.hu
Dokumentum felelős	[Adatvédelmi tisztviselő / Vezetőség]
Besorolás	Belső – Bizalmas

Verzió	Dátum	Szerző	Fejezet	Leírás
1.0	[Dátum]	[Kezdőbetűk]	Mind	Kezdeti verzió

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

Tartalomjegyzék

1. Bevezetés

2018. május 25-től az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete 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 BitMessaging (a továbbiakban: „Társaság”) elkötelezett amellett, hogy az általa kezelt személyes adatokat a GDPR-rel, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénnyel (a továbbiakban: „Infotv.”), valamint minden egyéb vonatkozó adatvédelmi jogszabállyal teljes összhangban kezelje.

A Társaság tömeges SMS-átjáró és üzenetküldő szolgáltatásokat nyújt, beleértve a tranzakciós üzenetküldést, promociós SMS-eket, kétfaktoros hitelesítési (2FA) kódokat, ügyfél-értesítéseket és rendelés-visszaigazolásokat. A Társaság szolgáltatásait HTTP API, SMPP, UCP és CIMD2 protokollokon keresztül nyújtja, VPN és dedikált vonali kapcsolat támogatással. Működése során a Társaság az érintettek különböző kategóriáinak személyes adatait gyűjti és kezeli, beleértve:

- jelenlegi és korábbi munkavállalók;
- álláspályázók és jelentkezők;
- ügyfélkapcsolattartók (fióktulajdonosok, műszaki kapcsolattartók, számlázási kapcsolattartók);
- weboldal-látogatók és érdeklődők (sms.bitnet.hu);
- beszállítók és üzleti partnerek.

Továbbá, és legjelentősebb módon, adatfeldolgozói minőségében a Társaság nagy mennyiségű személyes adatot kezel ügyfelei nevében, beleértve mobiltelefonorszámokat, üzenettartalmat, kézbesítési jelentéseket és hitelesítési kódokat, amelyek az ügyfelek saját érintettjeihez (SMS-címzettekhez és végfelhasználókhoz) tartoznak. Az adatkezelés nagymértékű jellege különös GDPR-követelményeket indukál, beleértve az adatvédelmi tisztviselő kötelező kinevezését (lásd a 4.2. pontot).

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 megállapítása;
- az adatvédelmi szerepek és felelősségek meghatározása;
- az adatkezelési tevékenységek és azok jogalapjainak áttekintése;
- az érintetti jogok és a kérelmek kezelésére vonatkozó eljárások leírása;
- a személyes adatok védelmét szolgáló biztonsági intézkedések meghatározása;
- a magyar jogi követelményekhez igazított adatmegőrzési időtartamok meghatározása;
- adatvédelmi incidensértesítési eljárások megállapítása;
- a kötelező adatkezelési tevékenységek nyilvántartásának és az adatvédelmi hatásvizsgálatoknak a szabályozása;

- a nagymértékű SMS-üzenetküldési műveletekből eredő különleges adatvédelmi szempontok kezelése; és
- folyamatos megfelelőségi felülvizsgálati mechanizmus létrehozása.

2.2 Hatály és alkalmazhatóság

Jelen Szabályzat vonatkozik minden olyan rendszerre, alkalmazásra, adatbázisra, eszközre, személyre és folyamatra, amely a Társaság információs rendszereinek részét képezi, vagy azokkal kapcsolatba kerül. Ide tartozik minden munkavállaló, vezető, szerződéses partner, tanácsadó, beszállító és egyéb harmadik fél, aki hozzáféréssel rendelkezik a Társaság által kezelt személyes adatokhoz.

A jelen Szabályzat hatálya alá tartozó személyeket a továbbiakban „Felhasználók”-nak nevezzük. A Szabályzatot valamennyi Felhasználó számára hozzáférhetővé kell tenni, és az új munkavállalók bevezető dokumentációjának részét képezi.

3. Fogalommeghatározások

Jelen Szabályzat alkalmazásában az alábbi fogalmak a következő jelentéssel bírnak:

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

A személyes adatok különleges kategóriái: a 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 és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó adatok.

Adatkezelés: a személyes adatokon végzett bármely művelet vagy műveletek összessége, így a 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 természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza.

Adatfeldolgozó: az a személy vagy szerv, amely az adatkezelő nevében és utasításai alapján személyes adatokat kezel.

Al-adatfeldolgozó: az adatfeldolgozó által az adatkezelő nevében végzett meghatározott adatkezelési tevékenységekre megbízott szervezet, az adatkezelő jóváhagyásával. A Társaság működésében az al-adatfeldolgozók közé tartoznak a mobilhálózati operátorok (MNO-k) és a felhőinfrastruktúra-szolgáltatók.

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

Hozzájárulás: az érintett akaratának önkéntes, konkrét, megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel nyilatkozat vagy egyértelmű megerősítő cselekedet útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok 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 tisztviselő („DPO”): a Társaság által a GDPR 37–39. cikkei alapján kinevezett személy, aki felügyeli az adatvédelmi megfelelőséget, tanácsot ad a Társaságnak kötelezettségei teljesítésében, és kapcsolattartóként szolgál az érintettek és a felügyeleti hatóság számára. A DPO kinevezése a Társaság számára kötelező (lásd a 4.2. pontot).

Adatvédelmi hatásvizsgálat (DPIA): Adatvédelmi hatásvizsgálat, amely egy projekt vagy adatkezelési tevékenység adatvédelmi kockázatainak azonosítását és minimalizálását szolgáló eljárás.

Adatkezelési tevékenységek nyilvántartása (ROPA): a szervezet által végzett valamennyi adatkezelési tevékenység hivatalos nyilvántartása a GDPR 30. cikke szerint. A Társaság számára kötelező (lásd a 10.1. pontot).

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

4. Szerepek és felelősségek

4.1 Vezetőség

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

4.2 Adatvédelmi tisztviselő (kötelező kinevezés)

A GDPR 37. cikk (1) bekezdés b) pontja értelmében a Társaság köteles adatvédelmi tisztviselőt kinevezni, mivel főtevékenységei olyan adatkezelési műveletekből állnak, amelyek jellegüknél, hatókörüknél és céljaiknál fogva az érintettek rendszeres és szisztematikus, nagyméretű megfigyelését teszik szükségessé. A Társaság tömeges SMS-üzenetküldési műveletei potenciálisan milliónyi mobiltelefonszám és üzenet kezelését foglalják magukban, ami nagyméretű adatkezelésnek minősül és kiindukálja a kötelező DPO-kinevezést. Ez a követelmény független a Társaság létszámától, és az adatkezelés jellege és mérete indokolja.

A Társaság olyan DPO-t nevez ki, aki megfelel a GDPR 37–39. cikkeiben foglalt követelményeknek. A DPO lehet belső munkavállaló vagy szolgáltatási szerződés alapján megbízott külső szolgáltató. A DPO:

- szakértelmmel rendelkezik az adatvédelmi jog és gyakorlat terén (37. cikk (5) bekezdés);
- megfelelően és időben bevonásra kerül a személyes adatok védelmével kapcsolatos valamennyi kérdésbe (38. cikk (1) bekezdés);
- közvetlenül a legfelső szintű vezetésnek jelent (38. cikk (3) bekezdés);
- feladatait függetlenként látja el, anélkül, hogy utasításokat kapna e feladatok ellátásával kapcsolatban (38. cikk (3) bekezdés);
- nem bocsátható el és nem szankcionálható DPO-feladatai ellátása miatt (38. cikk (3) bekezdés);
- elérhető az érintettek és a felügyeleti hatóság számára (38. cikk (4) bekezdés);
- titoktartási vagy bizalmassági kötelezettség köti feladatai ellátása során (38. cikk (5) bekezdés);

- tájékoztatja és tanácsot ad a Társaságnak és munkavállalóinak az adatvédelmi jogszabályokból eredő kötelezettségeikről;
- figyelemmel kíséri a GDPR-nak, az Infotv.-nek és jelen Szabályzatnak való megfelelést;
- felügyeli az érintetti kérelmek kezelését és biztosítja az időben történő válaszadást;
- kezeli a kijelölt adatvédelmi e-mail címet és biztosítja valamennyi beérkező kommunikáció haladéktalan áttekintését;
- koordinálja az adatvédelmi incidensek értékelését, kezelését és bejelentési eljárásait;
- karbantartja és felülvizsgálja a kötelező adatkezelési tevékenységek nyilvántartását;
- iránymutatást ad az adatvédelmi hatásvizsgálatokhoz, és szükség esetén elvégzi vagy felügyeli azokat;
- időszakos megfelelőségi felülvizsgálatokat és auditokat végez vagy koordinál;
- adatvédelmi tudatossági képzést szervez vagy biztosít valamennyi munkavállaló számára; és
- elsődleges kapcsolattartóként szolgál a NAIH képviselői és az ügyfelek felé adatvédelmi kérdésekben.

A DPO-t a GDPR 37. cikk (7) bekezdése szerint be kell jelenteni az illetékes hatóságnál, mely hatóság Magyarországon a NAIH. A DPO elérhetőségeit közzé kell tenni a Társaság weboldalán, szerepeltetni kell minden adatkezelési tájékoztatóban, közölni kell valamennyi munkatárssal, valamint hozzáférhetővé kell tenni az érintettek és a felügyeleti hatóság számára.

A DPO egyéb feladatokat és kötelezettségeket is elláthat, feltéve, hogy ezek nem eredményeznek összeférhetetlenséget (38. cikk (6) bekezdés).

4.3 Valamennyi Felhasználó

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

- személyes adatokat kizárólag engedélyezett célokra és dokumentált utasításoknak megfelelően kezelni;
- bármely feltételezett vagy tényleges adatvédelmi incidenst haladéktalanul jelenteni a DPO-nak;
- bármely érintetti kérelmet azonnal továbbítani a DPO-nak;
- a személyes adatok bizalmasságát megőrizni és azokat jogosulatlan személyek számára nem hozzáférhetővé tenni; és
- elvégezni a kötelező adatvédelmi képzéseket.

4.4 A Társaság GDPR szerinti szerepe

A GDPR értelmében a Társaság kettős minőségben működik:

Adatfeldolgozóként (elsődleges szerep – 28. cikk): amikor az ügyfelek által megadott mobiltelefonszámokat kezeli SMS-kézbesítés céljából; üzenettartalmat továbbít az ügyfelek nevében a végső címzetteknek; kézbesítési jelentéseket, üzenetküldési naplókat és továbbítási adatokat tárol; és hitelesítési kódokat (2FA/OTP) kezel ügyfeleinek rendszereihez. Ebben a minőségben a Társaság kizárólag az adatkezelő (ügyfél) utasításai alapján és a vonatkozó adatfeldolgozói megállapodásnak megfelelően kezel személyes adatokat.

Adatkezelőként (másodlagos szerep – 24. cikk): amikor saját munkavállalóinak, ügyfélkapcsolattartóinak (fióktulajdonosok, számlázási kapcsolattartók, műszaki kapcsolattartók), weboldal-látogatóinak, érdeklődőinek és beszállítóinak személyes adatait kezeli saját céljaira.

E kettős szerep megköveteli mind az adatkezelői kötelezettségek (láthatóság, jogszerű adatkezelés, érintetti jogok), mind az adatfeldolgozói kötelezettségek (kizárólag dokumentált utasítás alapján történő eljárás, megfelelő biztonság biztosítása, bizalmasság fenntartása, az adatkezelő megfelelőségének támogatása) teljesítését. A Társaság adatfeldolgozói tevékenységének nagymértékű jellege miatt az adatfeldolgozói kötelezettségek különös jelentőséggel bírnak.

5. Adatvédelmi elvek

A Társaság biztosítja, hogy minden személyes adatkezelési tevékenysége megfelel a GDPR 5. cikkében meghatározott következő elveknek:

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 ezekkel a célokkal össze nem egyeztethető módon tovább kezelni.

Adattakarékosság: A személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lenniük, és a szükségesre kell korlátozódniuk.

Pontosság: A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük. Minden ésszerű intézkedést meg kell tenni annak biztosítására, hogy a pontatlan adatok haladéktalanul törlésre vagy helyesbítésre kerüljenek.

Korlátozott tárolhatóság: A személyes adatokat olyan formában kell tárolni, amely az érintettek azonosítását csak addig teszi lehetővé, amíg az az adatkezelés céljai szempontjából szükséges. A Társaságra vonatkozó konkrét megőrzési időtartamokat a 11. pont és az 1. melléklet tartalmazza.

Integritás és bizalmasság: A személyes adatokat úgy kell kezelni, hogy megfelelő biztonság garantált legyen, beleértve a jogosulatlan vagy jogellenes adatkezelés, valamint a véletlen elvesztés, megsemmisítés vagy károsodás elleni védelmet, megfelelő technikai és szervezeti intézkedések alkalmazásával.

Elszámoltathatóság: A Társaság felelős a fenti elveknek való megfelelésért, és képesnek kell lennie annak 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 konkrét célból történő kezeléséhez.

Szerződés: az adatkezelés az érintettel kötött szerződés teljesítéséhez szükséges, vagy az érintett kérésére szerződéskötést megelőző lépések megtételéhez szükséges.

Jogi kötelezettség: az adatkezelés a Társaságra vonatkozó jogi kötelezettség teljesítéséhez szükséges (pl. magyar munkajogi, adójogi, 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 vagy szabadságai.

A személyes adatok különleges kategóriáinak kezelése kizárólag a GDPR 9. cikkében meghatározott további feltételek mellett megengedett, beleértve azt az esetet, amikor az adatkezelés a foglalkoztatási és szociális biztonsági jog területén fennálló kötelezettségek teljesítéséhez szükséges, vagy ha az érintett kifejezett hozzájárulását adta.

Az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról szóló 2003. évi CXXV. törvény 8. §-a alapján különleges adatok gyűjtése sokszínűségi monitoring céljára nem megengedett, mivel az diszkriminációnak minősülhet. A NAIH Foglalkoztatási iránymutatása továbbá előírja, hogy munkavállalóktól és pályázóktól csak a munkakörrel kapcsolatos információk gyűjthetők, kizárva a magánéletre, kapcsolatokra, családi életre vagy vallásra vonatkozó adatokat.

Adatfeldolgozóként eljárva a Társaság kizárólag az adatkezelő (ügyfél) dokumentált utasításai alapján kezel személyes adatokat. Az ilyen esetekben az adatkezelés jogalapja az adatkezelőnél van.

6.1 Hozzájárulás-kezelés

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

- a hozzájárulást egyértelmű, megerősítő cselekedeten keresztül szerzik meg, és azt dokumentálják;
- az érintettet tájékoztatják a hozzájárulás bármikori visszavonásának jogáról, és a visszavonás ugyanolyan egyszerű, mint a hozzájárulás megadása;
- 16 év alatti kiskorúak esetében a hozzájárulást a szülői felelősséget viselő személy adja meg vagy engedélyezi; és
- a hozzájárulási űrlapokat használat előtt a DPO jóváhagyja.

Adatfeldolgozóként a hozzájárulás beszerzése az adatkezelő kötelezettsége. A Társaság az adatkezelő e tekintetben adott utasításait követi.

7. Érintetti jogok

A Társaság tiszteletben tartja és érvényesíti a GDPR által biztosított érintetti jogokat. Az érintettek jogaikat a DPO-nak a kijelölt adatvédelmi e-mail címre küldött megkereséssel gyakorolhatják. Bármely érintetti kérelmet, amelyet Felhasználó vagy a Társaság nevében adatokat kezelő harmadik fél kap, haladéktalanul továbbítani kell a DPO-nak.

7.1 A kérelmek kezelésének eljárása

Érintetti kérelem beérkezésekor a DPO:

- szükség esetén igazolja az érintett személyazonosságát;
- nyilvántartásba veszi a kérelmet és az érintett részlegekkel egyeztetve azonosítja az összes érintett személyes adatot;
- a kérelem beérkezésétől számított egy hónapon belül írásbeli választ ad;
- amennyiben a kérelem összetett, vagy nagyszámú kérelem érkezett, a válaszadási határidőt további két hónappal meghosszabbítja, erről az érintettet az első egy hónapos időszakon belül tájékoztatja; és

- a választ díjmentesen adja meg, kivéve, ha a kérelem nyilvánvalóan megalapozatlan, túlzó vagy ismétlődő, amely esetben ésszerű díj számítható fel, vagy a kérelem indokolással megtagadható.

Valamennyi érintetti kérelmet és annak eredményét a DPO nyilvántartja és dokumentálja.

7.2 Jogok áttekintése

Hozzáféréshez való jog (15. cikk): Az érintetteknek jogában áll visszaigazolást kapni arra vonatkozóan, hogy személyes adataik kezelése folyamatban van-e, és ha igen, hozzáférést az adatokhoz és az adatkezelésre vonatkozó információkhoz. Az érintett kérheti adatainak másolatát elektronikus formátumban.

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

Törléshez való jog (17. cikk): Az érintettek kérhetik személyes adataik törlését, ha azok a gyűjtés céljához már nem szükségesek, ha a hozzájárulást visszavonják, ha az adatkezelés jogellenes volt, vagy ha a törlést jogszabály írja elő. Ez a jog nem alkalmazandó, ha a megőrzés jogi kötelezettség teljesítéséhez vagy jogi igények előterjesztéséhez, érvényesítéséhez, illetőleg védelméhez szükséges.

Az adatkezelés korlátozásához való jog (18. cikk): Az érintettek kérhetik az adatkezelés korlátozását, ha a pontosságot vitatják, az adatkezelés jogellenes, a Társaságnak már nincs szüksége az adatokra, de az érintett jogi igényekhez igényli azokat, vagy ha az érintett tiltakozott az adatkezelés ellen.

Adathordozhatósághoz való jog (20. cikk): Az érintettek kérhetik személyes adataik tagolt, széles körben használt, géppel olvasható formátumban történő kiadását, és kérhetik azok közvetlen továbbítását másik adatkezelőhöz, ahol az adatkezelés hozzájáruláson vagy szerződésen alapul és automatizált módon történik.

Tiltakozáshoz való jog (21. cikk): Az érintettek tiltakozhatnak a jogos érdeken vagy közérdeken alapuló adatkezelés ellen, beleértve a profilalkotást. A Társaság köteles az adatkezelést megszüntetni, kivéve, ha kényszerítő erejű jogos érdekeket igazol, amelyek elsőbbséget élveznek az érintett érdekeivel szemben.

Automatizált döntéshozatal elleni jog (22. cikk): Az érintetteknek jogában áll, hogy ne terjedjen ki rájuk kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés, amely rájuk nézve joghatással jár vagy őket hasonlóképpen jelentős mértékben érinti.

7.3 Adatfeldolgozói kötelezettségek az érintetti jogokkal kapcsolatban

Adatfeldolgozóként a Társaság segítséget nyújt az adatkezelőnek az érintetti kérelmek megválaszolására vonatkozó kötelezettségeinek teljesítésében. Ha a Társaság közvetlenül kap kérelmet egy érintettől az adatkezelő nevében kezelt adatokkal kapcsolatban (például egy SMS-címzett kéri a telefonszámának törlését), a DPO haladéktalanul értesíti az érintett adatkezelőt, és nem válaszol közvetlenül a kérelemre, kivéve, ha az adatkezelő erre utasítja.

8. Technikai és szervezeti biztonsági intézkedések

A Társaság a kockázat mértékének megfelelő biztonsági szintet biztosító megfelelő technikai és szervezeti intézkedéseket hajt végre, figyelembe véve a technika állását, a megvalósítás költségeit, az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint az érintettek jogait és szabadságait fenyegető kockázat valószínűségét és súlyosságát. Tekintettel a Társaság nagymértékű adatkezelési tevékenységeire és az üzenetküldési adatok érzékenységére (beleértve a banki és pénzügyi szolgáltatásokhoz használt hitelesítési kódokat), a hatékony biztonsági intézkedések elengedhetetlenek.

8.1 Technikai intézkedések

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

- titkosított kommunikáció minden adattovábbításnál, beleértve a VPN-kapcsolatokat és a HTTPS-támogatást az API-integrációkhoz;
- biztonságos üzenetküldési protokollok támogatása, beleértve az SMPP, UCP és CIMD2 protokollokat titkosított API-kapcsolatokkal;
- redundáns felhőalapú infrastruktúra, amely magas rendelkezésre állást biztosít (0–24 órás működés magas SLA-garanciával);
- hálózati biztonsági intézkedések, beleértve a tűzfalakat, behatolásészlelést és forgalomfigyelést;
- hozzáférés-szabályozás, amely biztosítja, hogy a rendszerekhez és adatokhoz kizárólag jogosult személyzet férhet hozzá egyedi hitelesítő adatokkal;
- többfaktoros hitelesítés a kritikus rendszerekhez és az ügyfeleink webes felületéhez való hozzáférésnél;
- tárolt adatok titkosítása;
- biztonsági mentési és katasztrófa-helyreállítási eljárások;
- rendszeres biztonsági frissítések és javításkezelés; és
- rendszertevékenység és üzenetkézbesítési műveletek monitorozása és naplózása.

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 szükségességi alapon;
- titoktartási kötelezettség valamennyi munkavállaló és szerződéses partner számára;
- rendszeres adatvédelmi tudatossági képzés valamennyi munkatárs számára;
- biztonságos tárolás: a személyes adatokat tartalmazó dokumentumokat biztonságosan kell tárolni; az íróasztalokat felügyelet nélkül meg kell tisztítani az érzékeny dokumentumoktól;
- tilos a személyes adatok személyes eszközökre, magán e-mail fiókokba vagy nem engedélyezett felhőtárhely-szolgáltatásokba való továbbítása a DPO jóváhagyása nélkül;
- tilos a Társaság vagy ügyfelek tevékenységéhez kapcsolódó dokumentumok, információk vagy adatok fényképezése vagy filmezése;
- a már nem szükséges személyes adatok biztonságos megsemmisítési és törlési eljárásai; és
- a jelen Szabályzat 9. pontjában foglalt incidenskezelési eljárások.

8.3 Beépített és alapértelmezett adatvédelem

A GDPR 25. cikkével összhangban a Társaság már a tervezés fázisában beépíti az adatvédelmi szempontokat az új rendszerek, szolgáltatások és folyamatok kialakításába (beépített adatvédelem). Alapértelmezés szerint kizárólag az egyes konkrét adatkezelési célokhoz szükséges személyes adatok kerülnek kezelésre (alapértelmezett adatvédelem).

Az üzenetküldési szolgáltatások és API-interfészek fejlesztésekor vagy módosításakor a Társaság az adattakarékosság elvét alkalmazza, biztosítva, hogy kizárólag az SMS-kézbesítéshez feltétlenül szükséges személyes adatok (címzett telefonszáma és üzenettartalom) kerüljenek kezelésre, és az üzenetküldési naplók és kézbesítési adatok csak a szükséges ideig kerüljenek megőrzésre.

9. Adatvédelmi incidensek kezelése

Tekintettel a Társaság nagymértékű adatkezelési tevékenységeire és az üzenetküldési adatok érzékenységére (beleértve a banki és pénzügyi szolgáltatásokhoz használt hitelesítési kódokat), az incidensek észlelésére és kezelésére való képesség kritikus fontosságú. Az üzenetküldési infrastruktúrát érintő incidens akár milliónyi végfelhasználóra hatással lehet, és bejelentési kötelezettséget válthat ki több ügyfél-adatkezelő, valamint a felügyeleti hatóság felé.

9.1 Incidensek észlelése és bejelentése

Valamennyi Felhasználó köteles bármely feltételezett vagy megerősített adatvédelmi incidenst indokolatlan késedelem nélkül bejelenteni a DPO-nak a kijelölt adatvédelmi e-mail címen. A bejelentésnek lehetőség szerint tartalmaznia kell:

- az incidens jellegének leírását;
- az érintett érintetti kategóriákat és hozzávetőleges számukat;
- az érintett személyes adatok kategóriáit és hozzávetőleges mennyiségét;
- az incidens valószínű következményeinek leírását; és
- az incidens kezelésére tett vagy javasolt intézkedések leírását és hatásainak enyhítését.

9.2 Értékelés és válaszintézkedések

Az incidensbejelentés beérkezésekor a DPO:

- értékelést kezdeményez annak megállapítására, hogy az eset a GDPR szerinti adatvédelmi incidensnek minősül-e;
- dokumentálja az értékelést, beleértve az incidenssel kapcsolatos valamennyi tényt, annak hatásait és a megtett korrekciós intézkedéseket;
- amennyiben az eset nem minősül incidensnek, a kezdeti értékelést nyilvántartja; és
- amennyiben az eset incidensnek minősül, kockázatértékelést végez az érintettek jogait és szabadságait fenyegető kockázat valószínűségének és súlyosságának meghatározására.

9.3 Bejelentés a felügyeleti hatóságnak (33. cikk)

Amennyiben az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a Társaság az incidensről való tudomásszerzést követően indokolatlan késedelem nélkül, lehetőség szerint 72 órán belül bejelenti azt a hatóságnál. Amennyiben a bejelentés nem történik meg 72 órán belül, a késedelem okait is közölni kell.

9.4 Az érintettek értesítése (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 érintett érintetteket.

9.5 Adatfeldolgozói incidensbejelentési kötelezettségek

Adatfeldolgozóként a Társaság az ügyféladatokat érintő adatvédelmi incidensről való tudomásszerzést követően indokolatlan késedelem nélkül értesíti az érintett adatkezelőt. Tekintettel arra, hogy egyetlen üzenetküldési infrastruktúrát érintő incidens potenciálisan nagyszámú ügyfél-adatkezelőt érinthet, a Társaság naprakész kapcsolattartási adatokat tart nyilván minden ügyfél adatvédelmi vagy biztonsági kapcsolattartójáról a gyors értesítés érdekében. A felügyeleti hatóságnak és az érintetteknek szóló bejelentési kötelezettség az adatkezelőt terheli; a Társaság azonban az adatfeldolgozói megállapodás szerinti szükséges segítséget és információt biztosítja.

9.6 Incidensnyilvántartás

A DPO nyilvántartást vezet valamennyi adatvédelmi incidensről, beleértve azokat is, amelyek nem tették szükségessé a felügyeleti hatóság értesítését. A nyilvántartás tartalmazza az incidenssel kapcsolatos tényeket, annak hatásait és a megtett korrekciós intézkedéseket. A nyilvántartás bármely frissítését a vezetőség felülvizsgálja és jóváhagyja.

10. Adatkezelési tevékenységek nyilvántartása és hatásvizsgálatok

10.1 Adatkezelési tevékenységek nyilvántartása (30. cikk) – Kötelező

A GDPR 30. cikke értelmében a Társaság köteles adatkezelési tevékenységeinek nyilvántartását vezetni. A 30. cikk (5) bekezdésében foglalt, a 250 főnél kevesebb munkavállalót foglalkoztató szervezetekre vonatkozó mentesség a Társaságra nem alkalmazandó, mivel az adatkezelés nem alkalomszerű (az üzenetküldési szolgáltatás folyamatosan működik), az adatkezelés az érintettek jogaira és szabadságaira nézve kockázattal járhat (telefonszámok, üzenettartalom, hitelesítési kódok), ezért a nyilvántartás vezetése kötelező.

A Társaság külön adatkezelési nyilvántartást vezet adatkezelői tevékenységeihez (30. cikk (1) bekezdés) és adatfeldolgozói tevékenységeihez (30. cikk (2) bekezdés). A nyilvántartás dokumentálja:

- az elvégzett adatkezelési tevékenységek kategóriáit;
- az adatkezelés céljait;
- az érintettek és személyes adatok kategóriáit;
- a személyes adatok címzettjeit, beleértve a mobilhálózati operátorokat;
- a nemzetközi adattovábbításokat és az alkalmazott garanciákat;
- a megőrzési időtartamokat; és
- a technikai és szervezeti biztonsági intézkedések általános leírását.

A DPO felelős az adatkezelési nyilvántartás karbantartásáért, felülvizsgálatáért és folyamatos frissítéséért, legalább évente. Az adatkezelési nyilvántartást kérésre a NAIH képviselői rendelkezésére kell bocsátani.

10.2 Adatvédelmi hatásvizsgálat (35. cikk)

Amennyiben egy adatkezelési típus – különösen új technológiák alkalmazásával – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a GDPR előírja, hogy a Társaság az adatkezelést megelőzően adatvédelmi hatásvizsgálatot végezzen.

A személyes adatok (telefonszámok, üzenettartalom, hitelesítési kódok) nagymértékű kezelése és az adatkezelés jellege (elektronikus kommunikáció) miatt egyes adatkezelési tevékenységek a 35. cikk alapján hatásvizsgálatot igényelhetnek. A DPO értékeli, hogy szükséges-e az adatvédelmi hatásvizsgálat a Társaság alapvető üzenetküldési tevékenységeihez, valamint bármely új szolgáltatáshoz vagy az adatkezelés jelentős módosításához.

Amennyiben az adatvédelmi hatásvizsgálat szükséges, a Társaság a francia adatvédelmi hatóság (Commission Nationale de l'Informatique et des Libertés – CNIL) által közzétett sablont használja, amely ingyenesen elérhető és az EU-ban széles körben elismert referencia-módszertannak számít. A DPO koordinálja az adatvédelmi hatásvizsgálat elvégzését, és amennyiben az értékelés magas maradványkockázatot jelez, a NAIH képviselőit az adatkezelés megkezdése előtt megkeresi.

Adatfeldolgozóként a Társaság segítséget nyújt az adatkezelőknek saját adatvédelmi hatásvizsgálataik elvégzéséhez az alkalmazandó adatfeldolgozói megállapodásnak megfelelően.

11. Adatmegőrzés

11.1 Általános elvek

A személyes adatokat kizárólag addig szabad megőrizni, ameddig az a gyűjtés céljaihoz szükséges, vagy ameddig az alkalmazandó magyar és uniós jogszabályok előírják. A Társaság a korlátozott tárolhatóság elvét alkalmazza, biztosítva, hogy a személyes adatokat nem őrzik azonosítható formában a szükségesnél hosszabb ideig.

A Társaság által kezelt egyes adatkategóriákra vonatkozó konkrét megőrzési időtartamokat az 1. melléklet – Adatmegőrzési menetrend tartalmazza. Az 1. melléklet a Társaság mérvadó megőrzési menetrendjét képezi, és minden irattípusra egyetlen alkalmazandó megőrzési időtartamot állapít meg. A magyar jogszabályok követelményein alapul, beleértve, de nem kizárólagosan:

- a számvitelről szóló 2000. évi C. törvény (Számviteli tv.) – 8 éves megőrzési kötelezettség a számviteli bizonylatokra;
- az adózás rendjéről szóló 2017. évi CL. törvény (Art.) – adómegállapítási elévülési idők;
- a munka törvénykönyvéről szóló 2012. évi I. törvény (Mt.) – 3 éves elévülési idő a munkajogi igényekre;
- a társadalombiztosításról szóló törvény – nyugdíjjal kapcsolatos dokumentumok megőrzése;
- a munkavédelemről szóló 1993. évi XCIII. törvény (Mvt.) és az 5/1993. (XII. 26.) MüM rendelet – baleseti nyilvántartások és kitettségi nyilvántartások;
- a 33/1998. (VI. 24.) NM rendelet az orvosi vizsgálatokról – 30/40 éves megőrzés az orvosi nyilvántartásokra;
- a fogyasztóvédelemről szóló 1997. évi CLV. törvény (Fgytv.) – ügyfélpanaszok és levelezések;
- a Polgári Törvénykönyvről szóló 2013. évi V. törvény (Ptk.) – 5 éves általános elévülési idő polgári jogi igényekre;

- a gazdasági reklámtevékenységről szóló 2008. évi XLVIII. törvény (Reklámtv.) – direkt marketing hozzájárulási nyilvántartások;
- az ügyvédi tevékenységről szóló 2017. évi LXXVIII. törvény (Ügyvédi tv.) – társasági iratok megőrzése;
- az egyenlő bánásmódról szóló 2003. évi CXXV. törvény (Egyenlő bánásmód tv.) – különleges adatok gyűjtésének korlátozásai; és
- a NAIH Foglalkoztatási iránymutatása – útmutatás a munkavállalói és pályázói adatkezeléshez.
- a 2003. évi C. törvény az elektronikus hírközlésről – útmutatás a bűnüldözési, nemzetbiztonsági és honvédelmi célú adatmegőrzési kötelezettsékről.

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

11.2 Megőrzés adatkezelőként

A DPO felelős az egyes személyesadat-kategóriákra vonatkozó megőrzési időtartam azonosításáért, a megőrzési időtartamok dokumentálásáért és az érintett részlegekkel való közléséért, az érintett részlegekkel való koordinációért annak biztosítása érdekében, hogy a megőrzési idejét letöltött személyes adatokat ne használják működési célokra, valamint a személyes adatok biztonságos törléséért vagy anonimizálásáért a vonatkozó megőrzési időtartam lejártát követően.

Valamennyi Felhasználó köteles a megőrzési időtartam lejártát követően a személyes adatokat használatától elzárkózni, és tájékoztatni a DPO-t minden olyan adatról, amelyet törölni vagy anonimizálni kellett volna, de ez nem történt meg.

11.3 Megőrzés adatfeldolgozóként

Adatfeldolgozóként a Társaság az ügyfél személyes adatait kizárólag az adott adatkezelővel kötött adatfeldolgozói megállapodásban meghatározott időtartamig őrzi meg. A megállapodás megszűnésekor vagy az adatkezelő utasítására a Társaság valamennyi személyes adatot visszaszolgáltatja az adatkezelőnek, vagy biztonságosan törli azokat, kivéve, ha a megőrzést alkalmazandó jogszabály írja elő.

11.4 Üzenetküldési adatok megőrzése

Tekintettel a Társaság SMS-üzenetküldési alaptevékenységére, az üzenetküldési naplókban, kézbesítési jelentésekben és kapcsolódó nyilvántartásokban szereplő személyes adatok megőrzésére az alábbi differenciált megőrzési elvek alkalmazandók:

- **SMS-kézbesítési naplók** (telefonszámok, kézbesítési időbélyegek, kézbesítési állapot): az alapértelmezett megőrzési időtartam 12 (tizenkét) hónap a kézbesítés hónapjának végétől számítva, összhangban az Eht. 159/A. § szerinti bűnüldözési célú adatmegőrzési kötelezettséggel. Sikertelen kézbesítési kísérletek adatai legfeljebb 6 (hat) hónapig őrzendők meg. Az ügyféllel kötött adatkezelési megállapodás az adatfeldolgozói jogviszonyban kezelt adatok tekintetében ennél rövidebb megőrzési időtartamot határozhat meg, azzal, hogy a Társaság saját adatkezelői jogalapon fennálló jogszabályi megőrzési kötelezettségeit ez nem érinti.
- **Üzenettartalom**: alapértelmezetten a kézbesítés visszaigazolásától számított 72 (hetvenkettő) órán belül törlendő. Az ügyféllel kötött adatkezelési megállapodás legfeljebb 12 (tizenkét) hónapos kiterjesztett megőrzési időtartamot határozhat meg, amennyiben az ügyfél a tartalommegőrzéshez jogszerű adatkezelési célt és jogalapot igazol (pl. panaszkezelés, fogyasztóvédelmi kötelezettség, pénzügyi audit). A

kiterjesztett megőrzés nem alkalmazható hitelesítési kódokra (2FA/OTP). A kiterjesztett megőrzési időtartamot az adatkezelési nyilvántartásban és az adatvédelmi hatásvizsgálatban rögzíteni kell. A Társaság az üzenettartalmat a megőrzési időtartam lejártát követően haladéktalanul törli, vagy – amennyiben technikai okokból azonnali törlés nem lehetséges – visszafordíthatatlanul anonimizálja.

- **Hitelesítési kódok (2FA/OTP)**: átmeneti adatként kezelendők, és a kézbesítés visszaigazolása után legfeljebb 1 (egy) órán belül automatikusan és visszavonhatatlanul törlendők. Ez alól az ügyféllel kötött adatkezelési megállapodás sem adhat felmentést.
- **Anonimizált és aggregált forgalmi statisztikák**: amennyiben az anonimizálás visszafordíthatatlan és a GDPR 26. preambulumbekezdésének megfelelő mértékű, korlátlan ideig megőrizhetők szolgáltatásfejlesztés és kapacitástervezés céljából.
- Az üzenetküldési adatok megőrzési időtartamait az ügyféllel kötött adatkezelési megállapodásokban tételesen rögzíteni kell, és az adatkezelési nyilvántartásban szerepeltetni szükséges.
- Az automatizált törlési eljárásokat az üzenettartalom és a hitelesítési kódok tekintetében kötelezően, a többi adatkategória tekintetében lehetőség szerint be kell vezetni. A törlési eljárások működését évente felül kell vizsgálni.

11.5 Szisztematikus törlési eljárások

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

- a megőrzött adatok éves felülvizsgálatát a megőrzési menetrendhez képest;
- automatizált emlékeztetőket vagy jelzési mechanizmusokat, ahol megvalósítható;
- az üzenetküldési naplók és kézbesítési adatok automatizált törlését a meghatározott megőrzési időtartamoknak megfelelően;
- dokumentált törlési vagy anonimizálási eljárásokat visszaigazoló nyilvántartásokkal; és
- fizikai dokumentumok biztonságos megsemmisítésének és elektronikus adatok végleges törlésének módszereit.

12. Harmadik felek és beszállítók kezelése

12.1 Adatfeldolgozók megbízása

Amikor a Társaság adatkezelőként harmadik felet bíz meg, amely hozzáférést kap személyes adatokhoz (pl. bérszámfejtő szolgáltatások, könyvelés, felhő/hosting szolgáltatók, IT-támogatás), a Társaság:

- ellenőrzi, hogy a harmadik fél megfelelő garanciákat nyújt az adatvédelmi jogszabályoknak való megfelelésre, beleértve a megfelelő technikai és szervezeti intézkedéseket;
- a GDPR 28. cikkével összhangban adatfeldolgozói megállapodást köt az adatkezelés megkezdése előtt;
- az adatfeldolgozó folyamatos megfelelését legalább évente értékeli; és
- a DPO felügyelete alatt megőrzi valamennyi adatfeldolgozási megállapodás másolatát.

A Társaság nevében személyes adatok kezelésére vonatkozó szerződés kizárólag a DPO előzetes írásbeli jóváhagyásával köthető meg.

12.2 Al-adatfeldolgozók kezelése és átvilágítása

Amikor a Társaság adatfeldolgozóként al-adatfeldolgozót bíz meg (beleértve a mobilhálózati operátorokat, felhőinfrastruktúra-szolgáltatókat, monitoring szolgáltatásokat és egyéb műszaki szolgáltatókat), a Társaság:

- előzetes általános vagy egyedi felhatalmazást szerez az adatkezelőtől;
- átvilágítást végez az al-adatfeldolgozón, értékelve: az adatvédelmi gyakorlatokat és szabályzatokat; a megfelelő adatvédelmi megállapodások megkötésére való hajlandóságot; a végrehajtott biztonsági intézkedéseket; az adatkezelés és -tárolás helyét (EU/nem EU); az incidensbejelentési képességet; valamint a releváns tanúsítványokat vagy megfelelőségi igazolásokat;
- az al-adatfeldolgozóra írásbeli megállapodásban azonos adatvédelmi kötelezettségeket ró;
- nyilvántartást vezet valamennyi jóváhagyott al-adatfeldolgozóról (beleértve a mobilhálózati operátorokat és felhőszolgáltatókat), és azt kérésre az adatkezelők rendelkezésére bocsátja; és
- teljes mértékben felel az adatkezelő felé az al-adatfeldolgozó adatvédelmi kötelezettségeinek teljesítéséért.

A mobilhálózati operátorok GDPR szerinti szerepe és felelőssége (al-adatfeldolgozó, közös adatkezelő vagy önálló adatkezelő) minden operátori kapcsolat esetében egyértelműen meghatározandó és dokumentálandó.

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

12.3 Nemzetközi adattovábbítások

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

- az Európai Bizottság megfelelőségi határozata;
- az Európai Bizottság által jóváhagyott általános szerződési feltételek (SCCs);
- kötelező erejű vállalati szabályok; vagy
- a GDPR 49. cikke szerinti alkalmazandó eltérés.

Az SMS-üzenetküldés jellegéből adódóan a nemzetközi adattovábbítás a Társaság működéséhez szervesen hozzátartozik. Amikor az ügyfelek az EU/EGT-n kívüli címzetteknek küldenek üzeneteket, a személyes adatok (telefonszámok és üzenettartalom) harmadik országbeli mobilhálózati operátorokhoz kerülnek továbbításra. A DPO-nak adattovábbítási feltérképezést kell végeznie az összes harmadik országba irányuló adatáramlás azonosítására a mobilhálózati összekapcsolásokon és a felhőinfrastruktúrán vagy egyéb műszaki szolgáltatásokon keresztül, és biztosítania kell a megfelelő garanciák vagy eltérések meglétét és dokumentálását.

A nemzetközi adattovábbítási mechanizmusokat és az adattovábbítás célországait az adatkezelési nyilvántartásban dokumentálni kell, az ügyfél kötött adatkezelési megállapodásokban szerepeltetni kell, és a Társaság adatkezelési tájékoztatóiban nyilvánosságra kell hozni.

13. Adatvédelmi kapcsolattartási pont

A Társaság kijelölt e-mail címet tart fenn minden adatvédelmi kommunikációra: adatvedelem@bitmessaging.hu.

A DPO figyelemmel kíséri ezt az e-mail címet a beérkező kommunikációk – beleértve az érintetti kérelmeket, az ügyfelek adatvédelmi megkereséseit és a belső bejelentéseket – haladéktalan áttekintése és feldolgozása érdekében.

A munkavállalók és szerződéses partnerek ezt a címet használják adatvédelemmel kapcsolatos kérelmekhez vagy bejelentésekhez. A DPO elérhetőségeit a Társaság weboldalán is közzé kell tenni, és valamennyi adatkezelési tájékoztatóban szerepeltetni kell.

14. Képzés és tudatosság

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

- kötelező adatvédelmi tudatossági képzés valamennyi új munkavállaló számára a beléptetési folyamat részeként;
- időszakos felfrissítő képzés valamennyi munkatárs számára, legalább évente;
- szerepkör-specifikus útmutatás az üzenetküldési műveleteket kezelő munkatársak számára, beleértve az adatok bizalmasságának fontosságát, az ügyfél-adatok (telefonszámok, üzenettartalom, hitelesítési kódok) biztonságos kezelését, és az üzenettartalom hozzáféréséhez és közzétételéhez fűződő tilalmakat, kivéve a műszaki műveletekhez szükséges eseteket;
- képzés a potenciális adatvédelmi incidensek felismeréséről és bejelentéséről; és
- valamennyi megtartott képzés dokumentálása, beleértve a jelenléti nyilvántartásokat.

A DPO felelős a képzési program megtervezéséért, lebonyolításáért és dokumentálásáért.

15. Monitoring, felülvizsgálat és folyamatos fejlesztés

15.1 Éves megfelelőségi felülvizsgálat

A DPO legalább évente átfogó felülvizsgálatot végez a Társaság adatvédelmi megfelelőségéről. A felülvizsgálat kiterjed:

- a jelen Szabályzat és valamennyi kapcsolódó eljárás megfelelőségére és hatékonyságára;
- az adatkezelési tevékenységek nyilvántartásának teljességére és pontosságára;
- a megőrzési időtartamoknak való megfelelésre és a törlési eljárások hatékonyságára, különös tekintettel az üzenetküldési adatokra;
- az elvégzett adatvédelmi hatásvizsgálatok eredményeire;
- a képzésen való részvételi arányokra és a tudatossági szintekre;
- a felülvizsgálati időszakban bekövetkezett adatvédelmi incidensekre és a levont tanulságokra;
- az alkalmazandó jogszabályok, szabályozási iránymutatások vagy felügyeleti hatósági döntések változásaira;
- a harmadik felek, al-adatfeldolgozók (beleértve a mobilhálózati operátorokat) és a nemzetközi adattovábbítási megfelelőség elégségességére; és

- a technikai és szervezeti biztonsági intézkedések hatékonyságára.

15.2 Jelentéstétel a vezetőségnek

Az éves felülvizsgálatot követően, és sürgős esetekben (mint például jelentős adatvédelmi incidens), a DPO jelentést nyújt be az ügyvezetőnek, amely tartalmazza az azonosított vagy potenciális meg nem felelések és a megtett vagy javasolt korrekciós intézkedések ismertetését, az adatvédelemmel kapcsolatos jelentős kockázatokat vagy problémákat, az elvégzett és javasolt adatvédelmi hatásvizsgálatokat, az új szolgáltatásokat vagy adatkezelési tevékenységeket és azok adatvédelmi elveknek való megfelelését, valamint a szabályzat-frissítésekre vagy eljárási fejlesztésekre vonatkozó javaslatokat.

15.3 Szabályzat-felülvizsgálatot kiváltó események

Az éves felülvizsgálat mellett jelen Szabályzatot az alábbi események bármelyikét követően felül kell vizsgálni és szükség szerint frissíteni:

- az alkalmazandó adatvédelmi jogszabályok vagy szabályozási iránymutatások lényeges változásai;
- a Társaság üzleti tevékenységeinek, szolgáltatásainak vagy informatikai környezetének jelentős változásai;
- jelentős adatvédelmi incidens vagy biztonsági esemény;
- auditok vagy felügyeleti hatósági vizsgálatok megállapításai vagy ajánlásai;
- a Társaság kockázati profiljának vagy fenyegetettségi környezetének változásai; és
- bármely egyéb, a DPO által felülvizsgálatot indokolónak minősített esemény.

16. A Szabályzat megsértése

Jelen Szabályzat megsértését a DPO a vezetőséggel együttműködve vizsgálja ki. A megsértés a jogsértés súlyosságával arányos fegyelmi intézkedést vonhat maga után, beleértve, de nem kizárólagosan:

- írásbeli figyelmeztetés;
- a személyes adatokhoz és információs rendszerekhez való hozzáférés ideiglenes vagy végleges korlátozása;
- kötelező kiegészítő adatvédelmi képzés;
- a munkaviszony vagy szerződéses jogviszony megszüntetése; és
- jogi lépések, amennyiben indokoltak.

17. Dokumentumkezelés

17.1 Hatálybalépés

Jelen Szabályzat az ügyvezető általi jóváhagyás napjától hatályos.

17.2 Kivételek

Jelen Szabályzat alóli kivételeket kizárólag az ügyvezető hagyhatja jóvá írásban, a DPO javaslatára. Valamennyi kivételt dokumentálni kell, időbeli hatályt kell szabni, és felülvizsgálat alá kell vonni.

1. melléklet – Adatmegőrzési nyilvántartás

Az alábbi táblázat a Társaság által kezelt valamennyi személyesadat-kategóriára vonatkozó mérvadó megőrzési időtartamokat állapítja meg. Ahol a magyar jogszabály meghatározott megőrzési időtartamot ír elő, azt kell alkalmazni. Ahol nincs jogszabályi előírás, az időtartam az alkalmazandó elévülési időkön és szabályozási iránymutatásokon alapul. Ahol több kötelezettség átfedi egymást, a leghosszabb alkalmazandó időtartam került kiválasztásra.

Jelen melléklet a Társaság mérvadó adatmegőrzési menetrendjét képezi. A DPO biztosítja, hogy a személyes adatok ezen időtartamoknak megfelelően törlésre vagy anonimizálásra kerüljenek.

Irat típusa	Megőrzési időtartam	Időtartam kezdete	Jogszabályi hivatkozás
A. FOGLALKOZTATÁS – SZEMÉLYES ADATOK			
Személyes elérhetőségek (lakcím, 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 jogosultság dokumentumai (munkavállalási engedélyek, vízumok)	3 év	Munkaviszony megszűnése	Mt. 286. § (1) bek.
Személyi azonosító számok (TAJ, személyi ig., útlevél, jogosítvány)	3 év	Munkaviszony megszűnése	Mt. 286. § (1) bek.
Munkahelyi elérhetőségek (munkakör, munkahelyi e-mail, telefon)	3 év	Munkaviszony megszűnése	Mt. 286. § (1) bek.
Hozzátartozók és vészhelyzeti elérhetőségek	Törlés a munkaviszony megszűnésekor	Munkaviszony megszűnése	GDPR 5. cikk (1) bek. e) pont
B. FOGLALKOZTATÁS – NAPLÓK ÉS JELENLÉT			
Jelenléti nyilvántartás	3 év	Munkaviszony megszűnése	Mt. 134. § és Mt. 286. § (1) bek.
Helyszíni belépési nyilvántartások	3 év	Munkaviszony megszűnése	Mt. 134. § és Mt. 286. § (1) bek.
Éves szabadság nyilvántartása	3 év	Munkaviszony megszűnése	Mt. 134. § és Mt. 286. § (1) bek.
Munkahelyi baleseti jelentések	5 év	Baleset bekövetkezése	Mvt. 64/A. §; 5/1993. MüM rend. 5. §
C. FOGLALKOZTATÁS – EGÉSZSÉGÜGYI NYILVÁNTARTÁSOK (FOGLALKOZÁS-EGÉSZSÉGÜGYI)			
Orvosi igazolások (foglalkozási alkalmasság)	30 év; 40 év biológiai kitettség esetén	A nyilvántartás létrehozása	33/1998. NM rend. 14. § (5)–(6) bek.
Orvosi jelentések	30 év; 40 év biológiai kitettség esetén	A nyilvántartás létrehozása	33/1998. NM rend. 14. § (5)–(6) bek.

Munkahelyi alkalmazkodások nyilvántartásai	30 év; 40 év biológiai kitettség esetén	A nyilvántartás létrehozása	33/1998. NM rend. 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 nyilvántartása	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. §*
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 változásainak nyilvántartása	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Tb. tv. 99/A. §*
Nyugdíjszolgáltató 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 nyilvántartások	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 iránymutatás
Sikertelen pályázók – hozzájárulás nélkül	Törlés az elutasításkor	Az elutasítás dátuma	GDPR 5. cikk (1) e); NAIH iránymutatás
Sikertelen pályázók – háttérellenőrzés	Törlés az ellenőrzés után	Az ellenőrzés lezárása	Mt. 11. § (3), 44/A. §; NAIH iránymutatás

Különleges adatok sokszínűségi monitoringra	NEM MEGENGEDETT	–	Egyenlő bánásmód tv. 8. §; NAIH iránymutatás
H. MUNKAVÉDELEM			
Munkavédelmi audit jelentések	5 év	Az értékelés időpontja	Mvt. 54. § (5) bek.
Kábítószer/alkohol tesztek – pozitív	3 év	A munkaviszony megszűnése	Mt. 286. § (1) bek.
Kábítószer/alkohol tesztek – negatív	1 év	A jegyzőkönyv aláírása	Mt. 286. § (1) bek.
Munkavédelmi szabályzatok (nyilvántartások)	3 év	A munkaviszony megszűnése	Mt. 286. § (1) bek.
Munkavédelmi baleseti bejelentések	5 év	A baleset bekövetkezése	Mvt. 64/A. §; 5/1993. MüM rend.
Munkavédelmi vizsgálati jelentések	5 év	A baleset bekövetkezése	Mvt. 64/A. §; 5/1993. MüM rend.
Egyéb egészségügyi/orvosi vizsgálatok	30 év; 40 év biológiai kitettség esetén	A nyilvántartás létrehozása	33/1998. NM rend. 14. § (5)–(6) bek.
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 anyagoknak való kitettség nyilvántartásai	10 év; 50 év rákkeltő anyagok esetén	Megszűnés / utolsó kitettség időpontja	Mvt. 63/A. § (3), 63/B. § (3) bek.
Kockázatértékelések	5 év	Az értékelés időpontja	Mvt. 54. § (5) bek.
Rutin munkavállalói egészségügyi dokumentáció	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	Tartós; majd 10 év	A társaság megszűnése	Ügyvédi tv. 46. § (5)–(6); Ptk. 6:22. §
Igazgatósági ülések jegyzőkönyvei és határozatai	10 év	A létrehozás dátuma	Ügyvédi tv. 46. § (5)–(6); Ptk. 6:22. §
Vezető tisztségviselők szolgálati szerződései	5 év	Az igény esedékessé válása	Ptk. 6:22. §
Tagjegyzék / tagi nyilvántartások	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 végé	Számviteli tv. 169. § (2); Art.
Általános adónyilvántartások	8 év	Az üzleti év végé	Számviteli tv. 169. § (2); Art. 202. §
Adóbevallásokhoz kapcsolódó nyilvántartások	8 év	Az üzleti év végé	Számviteli tv. 169. § (2); Art.

ÁFA nyilvántartások	8 év	Az üzleti év vége	Számviteli tv. 169. § (2); Art.
K. ÉRTÉKESÍTÉS, MARKETING ÉS ÜGYFÉLNYILVÁNTARTÁSOK			
Ügyfélszerződések	5 év	Az igény esedékessé válása	Ptk. 6:22. §
Ügyfélpanasz-napló	3 év	A beérkezés / a 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, JÉÉ)	5 év	Az igény esedékessé válása	Ptk. 6:22. §
L. ADATFELDOLGOZÓI NYILVÁNTARTÁSOK – ÜZENETKÜLDÉSI MŰVELETEK			
Adatfeldolgozási megállapodás keretében kezelt ügyfél-adatok	A megállapodás szerint meghatározva	A megállapodás megszűnésétől/lejártától	GDPR 28. cikk; 5. cikk (1) e); Eht. 159/A. §; megállapodás
SMS-kézbesítési naplók (telefonszámok, kézbesítési állapot, időbélyegek)	A megállapodás szerint; alapértelmezetten 12 hónap, sikertelen kézbesítés esetén 6 hónap, ha nincs meghatározva	Az üzenetkézbesítés dátumától	GDPR 28. cikk; 5. cikk (1) e); megállapodás
Üzenettartalom (ha tárolásra kerül)	Alapértelmezetten 72 órán belül törlendő a kézbesítés visszaigazolásától; a megállapodás legfeljebb 12 hónapos kiterjesztett megőrzést határozhat meg jogszerű cél igazolása esetén. Hitelesítési kódokra (2FA/OTP) a kiterjesztett megőrzés nem alkalmazható.	A kézbesítés visszaigazolásától	GDPR 5. cikk (1) c) és e); vonatkozó megállapodás; kiterjesztett megőrzés esetén DPIA szükséges
Hitelesítési kódok (2FA/OTP)	Legfeljebb 1 órán belül automatikusan és visszavonhatatlanul törlendő a kézbesítés visszaigazolásától. A megállapodás sem adhat felmentést.	A kézbesítés visszaigazolásától	GDPR 5. cikk (1) c) és e); átmeneti adat; megállapodás sem írhatja felül

Számlázási és használati nyilvántartások (összesített)	8 év	Az üzleti év végétől	Számviteli tv. 169. § (2) bek.

***** A bér- és nyugdíjnyilvántartások esetében a Számviteli tv. szerinti 8 éves számviteli megőrzési időtartam kerül alkalmazásra mint általános megőrzési időtartam, mivel ez 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, a nyugdíjellátások megállapításánál figyelembe veendő dokumentumokat a munkavállaló nyugdíjkorhatárának elérésétől számított legalább 5 évig meg kell őrizni. Amennyiben ez 8 évnél hosszabb megőrzési időtartamot eredményez, a hosszabb időtartam alkalmazandó.

A fentiekben nem szereplő nyilvántartások esetében a megőrzési időtartamot a DPO határozza meg az adatkezelés céljára, az alkalmazandó jogi követelményekre és a GDPR korlátozott tárolhatóság elvére tekintettel. Valamennyi megőrzési döntést dokumentálni kell.

2. melléklet – Jogszabályi hivatkozások

Az alábbi magyar és uniós jogszabályok képezik a jelen Szabályzatban és az Adatmegőrzési menetrendben 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, elévülés
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	Különböző	Magyar adatvédelmi jog
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. rend.	33/1998. (VI. 24.) NM rendelet az orvosi vizsgálatokról	14. § (5) és (6) bek.	Orvosi nyilvántartások (30/40 év)
Tb. tv.	A társadalombiztosításról szóló törvény	99/A. §	Nyugdíjmegállapításhoz szükséges dokumentumok
Egyenlő bánásmód tv.	2003. évi CXXV. törvény az egyenlő bánásmódról	8. §	Diszkriminatív adatgyűjtés tilalma
GDPR	Az Európai Parlament és a Tanács (EU) 2016/679 rendelete	Különböző (5–49. cikk)	EU adatvédelmi keretrendszer
NAIH Fogl. iránymutatás	NAIH Munkahelyi adatkezelési követelmények iránymutatása	II. rész, 1.2., 1.3. pont	Munkavállalói és pályázói adatkezelési útmutatás
Reklámtv.	2008. évi XLVIII. törvény 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
Eht.	2003. évi C. törvény az elektronikus hírközlésről	159/A. §	Bűnüldözési, nemzetbiztonsági és honvédelmi célú adatmegőrzési kötelezettség.

Jóváhagyás és aláírások

Dátum: _____

Aláírás: _____

Név: _____