

TOPiN-Cloud

DORA-Addendum

ICT third-party service provider keretkiegészítés

pénzügyi szervezet (EU 2022/2554 — DORA) ügyfelek részére
az ÁSZF elválaszthatatlan részét képező kiegészítés

Szolgáltató: TOPiN-HUB Kft.

2161 Csomád, József Attila utca 1. — Cg. 13-09-223835

Hatályos: 2026. május 1. napjától

Verzió: v1.0

1. BEVEZETŐ ÉS ALKALMAZÁSI KÖR

1.1. Jogszabályi keret

A jelen DORA-Addendum (a továbbiakban: „Addendum”) az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2554 rendeletének a pénzügyi szektor digitális működési rezilienciájáról (a továbbiakban: „DORA”) 28. és 30. cikkére, valamint az ezeket kiegészítő, a Bizottság által kibocsátott technikai szabályozási és végrehajtási standardokra (különösen az (EU) 2024/1773, az (EU) 2024/1772 rendeletekre) tekintettel készült.

Az Addendum a TOPiN-Cloud Általános Szerződési Feltételek (a továbbiakban: „ÁSZF”) elválaszthatatlan részét képező kiegészítő szerződési feltétel-csomag, amely automatikusan alkalmazandó valamennyi olyan Ügyfélre, amely a DORA 2. cikk (1) bekezdése szerinti pénzügyi szervezetnek („DORA-ügyfél”) minősül, és e minőségét a TOPiN-HUB Kft. (a továbbiakban: „Szolgáltató”) részére a szerződéskötéskor — vagy a DORA-alá-esés bekövetkeztekor — írásban bejelenti.

1.2. A Szolgáltató pozíciója

A Szolgáltató az Addendum céljára a DORA 3. cikk (19) bekezdése szerinti „ICT third-party service provider”-nek (ICT harmadik fél szolgáltatónak) minősül. A Szolgáltató maga nem pénzügyi szervezet, nem DORA-entitás, a DORA kötelezettségei közvetlenül rá nem, hanem kizárólag a DORA-ügyfelei közvetítésével — szerződéses úton — telepítődnek. Ezen szerződéses kötelezettségek teljességét az ÁSZF és a jelen Addendum együttesen fedi le.

1.3. Kritikus vagy fontos funkció

A DORA-ügyfél feladata a szolgáltatás DORA 3. cikk (22) bekezdése szerinti „kritikus vagy fontos funkció” (critical or important function) minőségének önálló meghatározása. A Szolgáltató e minősítést magáévá teszi, a DORA-ügyfél általi bejelentéstől függően megfelelő SLA-szintet és működési intézkedéseket biztosít.

A Szolgáltató tájékoztató jelleggel rögzíti: a TOPiN-Cloud CoreVM csomag a 99,5%-os éves rendelkezésre állási vállalása miatt DORA-ügyfél kritikus vagy fontos funkciójához nem ajánlott. Kritikus vagy fontos funkció esetén a GeoVM (99,9%) vagy Regional csomag javasolt, megfelelő Managed DB + HA kiegészítéssel és a 14. pontban rögzített exit-tesztelés tényleges lefuttatásával.

2. FOGALOMMEGHATÁROZÁSOK

A jelen Addendumban használt nagybetűs kifejezések jelentése megegyezik az ÁSZF I. fejezetében rögzítettel, az alábbi kiegészítésekkel:

- „DORA”: az Európai Parlament és a Tanács (EU) 2022/2554 rendelete a pénzügyi szektor digitális működési rezilienciájáról.

- „DORA-ügyfél”: a DORA 2. cikk (1) bekezdése szerinti pénzügyi szervezet, amely a TOPiN-Cloud szolgáltatást DORA-hatály alatt veszi igénybe; ide értendő különösen a hitelintézet, a fizetési és elektronikuspénz-kibocsátó szolgáltató, a befektetési vállalkozás, a biztosító, a viszontbiztosító, a kriptoeszköz-szolgáltató, az ABAK, a KBFT, a hatálykezelő és minden egyéb, a 2. cikkben felsorolt entitás.
- „ICT-szolgáltatás” vagy „ICT-service”: a DORA 3. cikk (21) bekezdése szerinti, a TOPiN-Cloud keretében nyújtott digitális és adatalapú szolgáltatás.
- „Major ICT-related incident”: a DORA 18. cikke szerint besorolt jelentős ICT-incidens.
- „Register of Information”: a DORA 28. cikk (3) bekezdése és az (EU) 2024/1772 végrehajtási szabvány szerinti, TOPiN által vezetett ICT-alvállalkozói nyilvántartás, amelyből a DORA-ügyfél kivonatot kérhet a saját Register of Information-ja összeállításához.

3. A SZOLGÁLTATÁS TELJES ÉS PONTOS LEÍRÁSA

A DORA 30. cikk (2) bekezdés a) pontja szerinti kötelezettség teljesítéseként a Szolgáltató a jelen Addendumban kiegészítő részletességgel mutatja be a DORA-ügyfélnek nyújtott szolgáltatás funkcióit és konfigurációját, az ÁSZF II. és VI. fejezeteire, az 1. sz. (Csomagok), 2. sz. (Díjak), 3. sz. (SLA) és 4. sz. (AUP) mellékleteire, valamint a külön Szolgáltatási Szint Megállapodásra (SLA v2) épülő teljességgel.

3.1. A nyújtott ICT-szolgáltatások

- Virtuális privát szerver (VPS) szolgáltatás CoreVM, GeoVM és Regional csomag-szinteken, KVM/QEMU alapú virtualizációval, saját fejlesztésű Proxmox-stackre épülő control-plane-nel.
- Managed adatbázis-szolgáltatás (Managed DB) alap és HA konfigurációban (PostgreSQL, MySQL/MariaDB).
- Automatikus napi backup szolgáltatás 7 napos alap-megőrzéssel; Ügyfélportálon megrendelhető Backup-bővítés (30–90 napos megőrzés).
- SFTP-alapú offline tárolási lehetőség.
- 24/7 biztonsági ügyelet és támogatási csatorna (support@topin.cloud, security@topin.cloud).
- A szolgáltatás-igénybevételhez kapcsolódó Ügyfélportál, számlázási és kommunikációs rendszer.

3.2. Fizikai és logikai lokáció

A Szolgáltatás a 3-2-1 backup-elv mentén felépített, három EU-tagállami adatközpont-helyszín kombinációjában fut:

- Elsődleges (PROD) adatközpont: Birintech Solution által biztosított adatközpont, Budapest, Magyarország (EU-tagállam). Kialakítás: Tier III-egyenértékű (concurrent

maintainability). Minden termelési workload és a lokális napi backup-másolat egyik példánya itt helyezkedik el.

- Másodlagos (HA/failover) magyar adatközpont: VIVAnet adatközpont, Budapest, Magyarország (≈14,5 km légvonalban a PROD helyszíntől). Tier III-egyenértékű kialakítás. Site-szintű Proxmox HA / PostgreSQL streaming replication a GeoVM és a HA Managed DB add-on-okkal rendelkező szolgáltatásokra; a lokális backup-másolat másik példányát is itt tároljuk.
- Offsite Sovereign Backup: OVHcloud SAS, Roubaix (RBX), Franciaország (EU-tagállam). Kizárólag titkosított backup-adatok napi 1x delta + rotációs teljes mentéssel; nincs ügyfél-workload futtatás. A titkosítás AES-256, ügyfélspecifikus kulcshierarchiával, amelyet az OVH nem fejt meg.

Valamennyi DORA-ügyfél termelési (production) környezete és annak teljes adatállománya — beleértve a backup-adatokat is — az Európai Gazdasági Térség területén kerül tárolásra és feldolgozásra. Az EGT-n kívüli adatfeldolgozás nem történik, kivéve az Ügyfél által önállóan igénybe vett harmadik féltől származó integrációk (pl. Stripe fizetési csatorna, ha a DORA-ügyfél használja) esetén, amelyek kockázati profilját maga az Ügyfél értékeli.

3.3. A TOPiN-HUB oldali adatfeldolgozási rétegek

A TOPiN-HUB Kft. mint adatfeldolgozó — az Adatfeldolgozási Szerződés (DPA v2) szerint — az alábbi tevékenységeket végzi a DORA-ügyfél adatain:

- infrastruktúra-szintű kezelés (hypervisor, hálózat, storage);
- automatizált backup-rotáció és helyreállítási műveletek az ÁSZF 3.6. pontja szerinti retenció mellett;
- monitoring- és log-gyűjtés kizárólag üzemeltetési és biztonsági célból;
- támogatási ticket-kezelés, amely során az ügyfél-adatokhoz történő hozzáférés kizárólag az Ügyfél kifejezett jóváhagyásával, audit-logolt módon történik.

A vendég operációs rendszer és a benne futó alkalmazásszintű adatok kezelése (titkosítási kulcsok, alkalmazás-logika, adatbázis-tartalom) a DORA-ügyfél felelőssége.

4. SZOLGÁLTATÁSI SZINT ÉS MINŐSÉGI VÁLLALÁSOK

A Szolgáltató a DORA 30. cikk (2) bekezdés b) pontja szerinti kötelezettség teljesítéseként az alábbi szolgáltatási szinteket vállalja a DORA-ügyfelek részére:

Mérőszám	CoreVM	GeoVM / Managed DB HA	Regional
Éves uptime	99,5%	99,9%	99,5%
RTO (helyreállítási idő)	24 óra	4 óra	24 óra
RPO (adat-veszteség)	8 óra	1 óra	72 óra

Mérőszám	CoreVM	GeoVM / Managed DB HA	Regional
Kritikus / fontos funkcióra ajánlott?	NEM	IGEN	Feltételesen

A fenti szolgáltatási szintek mérésének módszertana, a service credit kalkuláció és a kompenzációs mechanizmus a Szolgáltatási Szint Megállapodás (SLA v2) szerint alkalmazandó. A DORA-ügyfél jogosult az SLA-paraméterek ellenőrzésére és kérheti a mérési módszertan dokumentált bemutatását.

4.1. Testing a resilience és BCP-elemek

A Szolgáltató évente egyszer „recovery drill” gyakorlatot hajt végre, amely magában foglalja a backup-visszaállítás teljes körű tesztelését egy reprezentatív VPS-re és egy Managed DB-re. A gyakorlat eredményéről a Szolgáltató anonimizált, aggregált összefoglalót tesz elérhetővé a DORA-ügyfelek részére kérésre. A DORA-ügyfél saját exit-tesztelését a 14. pont szabályozza.

5. INCIDENSJELENTÉSI KÖTELEZETTSÉG

A Szolgáltató a DORA 30. cikk (2) bekezdés d) pontja szerinti kötelezettség teljesítéseként vállalja, hogy minden ICT-incidensről — a DORA 18. cikke szerinti osztályozás szerinti súlyosságtól függően — a következő határidővel értesíti a DORA-ügyfelet:

Súlyosság	Első értesítés	Részletes jelentés	Végleges root-cause jelentés
Major / Critical (DORA 18. cikk)	4 órán belül	24 órán belül	72 órán belül + 30 napos végső jelentés
Moderate	8 órán belül	72 órán belül	14 napon belül
Low	Havi aggregált jelentésben	Havi riportban	Negyedéves review-ban

5.1. Értesítési csatornák

- Elsődleges csatorna: security@topin.cloud e-mail a DORA-ügyfél által nevesített biztonsági-technikai kontaktra, valamint párhuzamosan az Ügyfélportál Incidens-fül értesítés.
- Kritikus / Major esetén kiegészítő hangértesítés a DORA-ügyfél 24/7 kijelölt technikai kontaktjának a szerződésben rögzített telefonszámon.
- A Szolgáltató 24/7 incident management kontaktja: security@topin.cloud, +36 20 479 4000.

5.2. Az értesítés minimum-tartalma

- incidens-azonosító, osztályozás és súlyosság a Szolgáltató belső osztályozási szabályzata szerint;
- érintett szolgáltatás-elemek, VPS- vagy DB-azonosítók;
- észlelés időpontja (UTC), hatás-időszak tól–ig;
- előzetes root-cause, ha ismert, különben „under investigation”;
- mitigációs lépések, amelyek már megtörténtek;
- a DORA-ügyféltől szükséges közreműködés, ha van;
- következő kommunikáció várható időpontja.

5.3. Kooperáció a DORA-ügyfél saját jelentési kötelezettségeiben

A DORA 19. cikke szerinti jelentési kötelezettség a DORA-ügyfelet terheli, annak teljesítését a Szolgáltató nem helyettesíti. A Szolgáltató azonban a DORA-ügyfél kifejezett kérésére — és ésszerű határidőn belül — ICT-technikai adatokat, időbélyegeket, log-részleteket és forensic-adatokat bocsát rendelkezésre, amelyek a DORA-ügyfél illetékes hatóságának (MNB, EU-ESA-k) történő bejelentéséhez szükségesek. Az együttműködés külön díjat nem keletkeztet.

6. ADATLOKALIZÁCIÓ ÉS ADATHOZZÁFÉRÉS

6.1. Lokalizáció

A Szolgáltató kifejezetten vállalja, hogy a DORA-ügyfél által kezelt valamennyi személyes és operatív adat kizárólag az EGT területén kerül tárolásra és feldolgozásra. A Szolgáltató ettől eltérést csak a DORA-ügyfél kifejezett, írásbeli, előzetes jóváhagyásával kezdeményezhet, ilyenkor a Transfer Impact Assessment és az EU sztenderd szerződéses kikötések (SCC) alkalmazandók.

6.2. Hatósági adathozzáférés

Amennyiben harmadik ország hatósága (ide értve bármely USA-alapú bírói vagy végrehajtó hatóság rendelkezését a CLOUD Act keretében is) a DORA-ügyfél adatainak kiadására vagy feltárására kötelezi a Szolgáltatót vagy annak bármely alvállalkozóját, a Szolgáltató vállalja, hogy:

- az ilyen megkeresést haladéktalanul — és a jogszabályilag megengedett maximumig részletezve — megosztja a DORA-ügyféllel, kivéve, ha ezt bíróság vagy jogszabály kifejezetten tiltja;
- minden rendelkezésére álló jogi eszközt (pl. kihívási eljárást, csökkentési indítványt) igénybe vesz a kért kiadás korlátozására;
- csak a jogilag legszűkebben értelmezett adatkört adja ki;
- a kiadást követően utólagos tájékoztatást nyújt a DORA-ügyfélnek.

A Szolgáltató megerősíti, hogy valamennyi infrastruktúra-alvállalkozója (Birintech Solutions Hungary Kft által biztosított adatközpont — HU; VIVAnet adatközpont — HU; OVHcloud SAS — FR) EU-tagállami székhelyű entitás, amelyekre USA-alapú extraterritoriális adatkérési rendelkezések közvetlenül nem terjednek ki; ezzel együtt a fenti eljárásrend minden olyan hipotetikus helyzetre alkalmazandó, amikor ilyen megkeresés mégis megérkezik.

7. ALVÁLLALKOZÓK (ICT SUBCONTRACTORS)

7.1. Jelenlegi alvállalkozói lista

A Szolgáltató a DORA 30. cikk (2) bekezdés e) pontja szerinti kötelezettség teljesítéseként az alábbi jelenlegi ICT-alvállalkozói láncot teszi átláthatóvá a DORA-ügyfelek felé (a teljes, naprakész lista a Register of Information-ban található):

Alvállalkozó	Funkció	Lokáció	Kritikusság
Birintech Solution Hungary Kft.	Elsődleges adatközpont (PROD colocation)	Budapest, Magyarország (EU)	Kritikus — szolgáltatás-nélkülözhetetlen
VIVAnet adatközpont	Másodlagos adatközpont (HA/failover GeoVM és HA Managed DB add-on esetén; lokális backup-replika)	Budapest, Magyarország (EU)	Kritikus — szolgáltatás-nélkülözhetetlen az érintett add-onokra
OVHcloud SAS	Offsite Sovereign Backup (napi 1x delta + rotációs teljes mentés; nincs ügyfél-workload futtatás)	Roubaix (RBX), Franciaország (EU)	Kritikus — DR-szenárió esetén; normál üzemre nem befolyásoló
Proxmox Server Solutions GmbH	Hypervisor és Backup Server platform-szoftver (licenz + Enterprise Repository)	Wien, Ausztria (EU)	Kritikus — szoftveres egy pontú dependencia
Cloudflare, Inc. (opcionális)	DDoS-védelem és CDN — kizárólag megrendelt add-on esetén	EU-s feldolgozás; USA-s anyavállalat (SCC + TIA)	Fontos — de ügyfél-választható
Stripe Payments Europe Ltd.	Fizetési feldolgozás (ügyfél-adatok körében csak billing adat)	Írország (EU); USA-s anyavállalat	Fontos — számlázási alvállalkozó, ügyfél-workloadot nem érint
Wise Europe SA	Banki szolgáltatás a TOPiN részére (ügyfél-adat nincs az alvállalkozónál)	Belgium (EU)	Nem kritikus

Alvállalkozó	Funkció	Lokáció	Kritikusság
Google Ireland Ltd. (Google Workspace)	Belső e-mail, dokumentumkezelés, TOPiN üzemeltetési ops (nem ügyfél-workload)	Írország (EU); USA-s anyavállalat (SCC + TIA)	Fontos — belső ops folytonossága

7.2. Alvállalkozó-változtatás (DORA Art. 30(2)(a) és 30(3))

A Szolgáltató vállalja, hogy minden olyan tervezett ICT-alvállalkozó-változást — amely kritikus vagy fontos funkciót érint, vagy amely új entitás bevezetését jelenti a szolgáltatási láncba —

- legalább 30 nappal a tervezett változás előtt írásban bejelent valamennyi DORA-ügyfél kijelölt kontaktjának;
- a bejelentés tartalmazza az új/megváltozott alvállalkozó nevét, a kiváltott funkciót, a hatály alá vont adat-kategóriákat, a lokációt, és az átvilágítás főbb eredményeit;
- a DORA-ügyfelet megilleti a tiltakozás joga a változtatással szemben, amelyet a bejelentéstől számított 14 napon belül írásban közölhet. Alapos indok (pl. a DORA-követelményeknek való nem-megfelelés, lokációs eltérés, jelentős biztonsági kockázat-növekedés) fennállása esetén a DORA-ügyfél jogosult a Szerződést a változás hatályba lépésének napjával rendkívüli felmondással felmondani, a 14. pont szerinti exit-együttműködés mellett.

7.3. Teljes láncra kiterjedő felelősség

A Szolgáltató a jelen Addendum szerinti kötelezettségek vonatkozásában úgy felel a DORA-ügyfél felé bármely alvállalkozó eljárásáért, mintha saját maga járt volna el. A Szolgáltató biztosítja, hogy az alvállalkozói szerződésai tartalmazzák mindazon minimum-klauszulákat (incidensjelentés, audit jog, lokalizáció, exit-támogatás), amelyek a DORA Art. 30 teljesítéséhez a lánc végéig szükségesek.

7.4. Concentration risk

A Szolgáltató elismeri, hogy a szolgáltatói láncának használata a DORA-ügyfél szempontjából közvetett concentration risk-et (a DORA 29. cikk értelmében) hordozhat. A Szolgáltató a DORA-ügyfél kérésére együttműködik a concentration risk-értékelésben. A Szolgáltató ICT Third-Party Risk Management Policy-ja (6. §) az alábbi koncentrációs kockázati vektorokat ismeri el és kezeli: (a) geográfiai koncentráció — az elsődleges (Birintech Solution Hungary Kft által biztosított) és a HA (VIVAnet) adatközpont egyaránt Budapesten, egymástól ≈14,5 km-re található, amit az OVH Roubaix-beli offsite Sovereign Backup ellensúlyoz; (b) szoftveres monokultúra — a Proxmox hypervisor egy pontú upstream dependencia, amit KVM-alapú, portábilis VM-formátumok és dokumentált alternatív hypervisor-exit-terv csökkent; (c) offsite backup szolgáltatói koncentráció — az OVH mint egyetlen offsite backup-szolgáltató, ügyfélspecifikus kulcsos AES-256 titkosítással, amely lehetővé teszi gyors S3-kompatibilis áttelepítést (Scaleway, Hetzner,

Backblaze B2 EU). A Szolgáltató ugyanezen 6. §-ban megnevezett alternatív providerpool-t tart karban a DORA-ügyfél saját concentration risk-elemzéséhez.

8. HOZZÁFÉRÉSI, VIZSGÁLATI ÉS AUDITJOG

8.1. A DORA-ügyfelet megillető jogok

A DORA 30. cikk (3) bekezdés e) pontja alapján a DORA-ügyfél — és a DORA-ügyfél illetékes felügyeleti hatósága, illetve az ezek által kijelölt harmadik fél auditor — jogosult a Szolgáltatónál ICT-audit, inspekción és vizsgálati jog gyakorlására a DORA-ügyfél által igénybe vett Szolgáltatás tekintetében. Az audit-jog magában foglalja:

- az auditra vonatkozó dokumentációhoz (policy-k, eljárásrendek, teszt-jegyzőkönyvek, incidenstörténet) való ésszerű hozzáférést;
- a Szolgáltató tárgyi és humán erőforrásaival történő, ésszerű együttműködést az audit lefolytatása során;
- a belső vizsgálati eredmények és a korrekciós intézkedések ellenőrzését;
- a megállapításokra adott válaszok és határidős akció-tervek megvitatását.

8.2. Eljárási szabályok

- A helyszíni audit szándékát a DORA-ügyfél legalább 30 naptári nappal előre írásban jelenti be. Sürgős — regulatórikus kötelezettségből fakadó — auditnál a határidő 10 naptári napra csökkenthető.
- Egy DORA-ügyfél évente egy rutin-audit-ra jogosult, korlátozás nélkül azonban jogosult felügyeleti hatósági utasítás alapján bármikor auditra.
- A Szolgáltató más DORA-ügyfelek által futtatott párhuzamos auditok koordinálásához „pooled audit” megoldást ajánl fel (ahol több DORA-ügyfél közös auditorral egyszerre vizsgál). A DORA-ügyfél nem köteles pooled auditot elfogadni, ha az üzleti vagy bizalmas okok ezt nem teszik lehetővé.
- A Szolgáltató biztosítja, hogy alvállalkozói szerződéseiben ugyanezen audit-jogok érvényesítését a DORA-ügyfél számára lehetővé tegye (pass-through audit).

8.3. Felügyeleti hatóság hozzáférése

A Szolgáltató kifejezetten hozzájárul ahhoz, hogy a DORA-ügyfél illetékes hatósága (MNB vagy az adott ESA), valamint az EU-szinten kritikus ICT-third-party provider esetén kijelölendő Lead Overseer (DORA 31–44. cikk) a DORA 33. cikk szerinti vizsgálatot közvetlenül is lefolytathassa a Szolgáltatónál a DORA-ügyfél tekintetében érintett szolgáltatási láncban. A Szolgáltató e vizsgálatokkal teljes mértékben együttműködik.

9. SZERZŐDÉS MEGSZŪNÉSE ÉS KILÉPÉS

9.1. DORA-indokú rendkívüli felmondás

A DORA 28. cikk (7) bekezdése alapján a DORA-ügyfelet a Szerződésre nézve megilleti a rendkívüli felmondás joga — az általános felmondási szabályokon felül — az alábbi esetekben:

- a Szolgáltató alkalmazandó jogszabályok, szerződéses előírások súlyos megsértése, különösen a DORA vagy a GDPR megsértése esetén;
- a Szolgáltató részéről olyan körülmények, amelyek megváltoztatják a szerződéses funkció teljesítését — beleértve a 3. rész szerinti szolgáltatás-leírás lényeges megváltozását;
- a Szolgáltató hiányosságai a DORA-ügyfél általános ICT-kockázatkezelésében, különösen, ha a szolgáltatás folyamatossága és minősége veszélyben;
- az illetékes felügyeleti hatóság azt a körülményt észleli, hogy a Szolgáltatót érintő kockázatok miatt a DORA-ügyfélnek a Szerződést meg kell szüntetnie.

A rendkívüli felmondási nyilatkozat írásban, a Szolgáltató legal@topin.cloud címére küldött e-mailben közölhető, a felmondási ok konkrét megjelölésével. A Szolgáltató a 14. pont szerinti exit-támogatási kötelezettsége a felmondás közlésével egyidejűleg aktiválódik.

9.2. Szolgáltató-oldali szerződés-megszüntetés

A Szolgáltató a Szerződést DORA-ügyfél esetén rendes felmondással kizárólag azonos vagy hosszabb előzetes értesítéssel szüntetheti meg, mint az az ÁSZF-ben a nem-DORA ügyfélre vonatkozik, minimum azonban 180 nappal előre. A Szolgáltató e felmondási jogot csak komoly üzleti ok fennállása esetén gyakorolja, különösen nem gyakorolja csődhelyzeti fenyegetettség konkrét bizonyítéka vagy felmondhatatlan üzleti stratégia-változás nélkül.

10. EXIT-TÁMOGATÁS ÉS BUSINESS CONTINUITY

A jelen pont a DORA 30. cikk (3) bekezdés f) pontja szerinti „exit strategy” implementálása. Az exit teljes, részletes menetrendje a külön Exit Strategy and Business Continuity for Financial Clients dokumentumban található. A jelen pont a kulcselemeket rögzíti.

10.1. Exit-időkeretek

- a Szerződés-megszüntetés bejelentésétől számított 30 naptári napon belül a Szolgáltató és a DORA-ügyfél közös exit-tervet hagy jóvá;
- az exit-terv keretében a Szolgáltató együttműködő magatartást és ésszerű mértékű technikai és koordinációs kapacitást biztosít;
- az aktív szolgáltatás — a DORA-ügyfél kérésére — a bejelentéstől 90 napig (kivételesen 180 napig, ha a DORA-ügyfél és a Szolgáltató ebben írásban megállapodik) tovább üzemel, hogy a DORA-ügyfél zavartalanul migrálhasson;
- az adat-átadás befejeztével a Szolgáltató a T+30 napon belül beleértve a backup-rotációt véglegesen törli az adatokat, és erről igazolást állít ki;
- a szolgáltatás folyamatossága az exit-időszak alatt a Szerződés szerinti SLA alá tartozik.

10.2. Átadott adatok formátuma

- VPS-ek: OVA (Open Virtualization Appliance) formátumban, teljes virtuális lemez-képpel;
- Managed DB: szabványos SQL dump (pg_dump / mysqldump) teljes export, feldolgozatlan tömörített formában;
- Backup-fájlok: standard tömörített tar + SHA-256 aláírás;
- Konfigurációs adatok: gépolvasható JSON/YAML formátumban;
- Az átadás SFTP-n keresztül, külön megállapodás esetén fizikai adathordozón is történhet.

10.3. Exit-tesztelés

A DORA 11. cikk (6) bekezdésére tekintettel a DORA-ügyfél köteles legalább évente egy alkalommal tényleges exit-gyakorlatot végrehajtani. A Szolgáltató évente egyszer — 60 napos előzetes koordinációval — teljes körű, ingyenes exit-dry-run-t biztosít, amelynek keretében a DORA-ügyfél egy reprezentatív környezetben kipróbálhatja a migrációs folyamatot.

11. DÍJAZÁS DORA-SCOPE-BAN

Az ÁSZF 2. sz. mellékletében rögzített díjtétel DORA-ügyfélre is alkalmazandó. A DORA-megfelelőséggel összefüggő ICT-együttműködés (incidenstámogatás, audit-közreműködés évi 1 alkalomig, exit-gyakorlat évi 1 alkalomig, DPIA-input) a szerződéses díj részét képezi, külön díjat nem vonz.

A fentiekén túli, rendkívüli mértékű igénybevétel (pl. felügyeleti hatóság rendkívüli auditja a DORA-ügyfél oldali kiváltó ok miatt, amely több mint 5 munkanapos dedikált támogatást igényel) esetén a Szolgáltató önköltség-alapú díjazásra jogosult, amelyet előzetesen írásban egyeztet a DORA-ügyféllel.

12. TITOKTARTÁSI ÉS INFORMÁCIÓBIZTONSÁGI ALAPELVEK

A Szolgáltató a DORA-ügyfél üzleti és ügyfél-adataira vonatkozóan a jelen Addendum hatálya alatt titoktartási kötelezettség terheli, amely a Szerződés megszűnését követően is határozatlan ideig fennáll, kivéve a szabadon elérhető, a DORA-ügyfél által nyilvánosságra hozott információkat. A személyes adatok vonatkozásában az Adatfeldolgozási Szerződés (DPA v2) szerinti szabályok alkalmazandók.

13. SZELLEMI TULAJDON

Az ÁSZF X. fejezete szerinti szellemi tulajdoni szabályok változatlanul alkalmazandók. A DORA-ügyfél által a Szolgáltatás keretében elhelyezett tartalom és adat kizárólagos tulajdonjoga a DORA-ügyfelet illeti meg. A Szolgáltatás-szintű szoftverelemek, konfigurációk és know-how a

Szolgáltató tulajdonát képezik; a DORA-ügyfélnek azokra a Szerződés hatálya alatt felhasználási jog van.

14. KAPCSOLATTARTÁS

A DORA-ügyfél — az Addendum hatályának fennállása alatt — megjelöli a következő szerepekre kijelölt kontaktot:

- Primary DORA business contact;
- ICT risk management contact;
- Security / incident response contact (24/7 elérhetőség);
- Audit és compliance contact.

A Szolgáltató oldalán valamennyi DORA-szemponjú kommunikáció primer csatornája: dora@topin.cloud. Konkrét funkciókra: security@topin.cloud (incidens), legal@topin.cloud (szerződéses ügyek), privacy@topin.cloud (adatvédelem).

15. AZ ADDENDUM FELÜLVIZSGÁLATA ÉS MÓDOSÍTÁSA

A jelen Addendumot a Szolgáltató évente legalább egyszer — illetve a DORA alkalmazására vonatkozó uniós jogszabály, technikai standard, vagy NBI-iránymutatás jelentős módosulása esetén soron kívül — felülvizsgálja. A módosítás tervezett tartalmáról a Szolgáltató a hatálybalépést megelőzően minimum 45 naptári nappal értesíti a DORA-ügyfeleket. Amennyiben a módosítás a DORA-ügyfélre nézve hátrányos változást jelent, a DORA-ügyfél jogosult a Szerződést a módosítás hatályba lépésének napjával rendes felmondással — a módosulás átvételére vonatkozó kifogásként — megszüntetni, az exit-támogatási kötelezettségek hatálya alatt.

16. ALKALMAZANDÓ JOG ÉS VITARENDEZÉS

A jelen Addendumra a magyar anyagi jog, kiegészítésként a DORA és kapcsolódó uniós rendeletek közvetlenül alkalmazandók. A DORA-ügyféllel felmerülő jogvitákra az ÁSZF XVII. fejezete szerinti békéltető eljárási + bírósági szabályok érvényesek, azzal, hogy DORA-ügyfél és Szolgáltató közötti vita esetén elsődlegesen szakmai szintű egyeztetés (30 napos tárgyalási időszak) vállalt.

17. ZÁRÓ RENDELKEZÉSEK

A jelen Addendum és az ÁSZF, a DPA v2, a SLA v2 és a kapcsolódó mellékletek közötti esetleges értelmezési kollízió esetén a DORA-ügyfél tekintetében a jelen Addendum elsőbbséget élvez mindazon kérdésekben, amelyek a DORA-megfelelőséget közvetlenül érintik.

Az Addendum elfogadása az ÁSZF szerinti elfogadással történik; a DORA-ügyfél a DORA-jogállásának a Szolgáltató felé történő írásbeli bejelentésével egyúttal az Addendumot is magára nézve kötelezőnek ismeri el.

Hatályos: 2026. május 1. napjától — v1.0.