

Verzia: 1.0, účinná od **1. augusta 2026** (rozhodnutie objednávateľa 2026-08-05) — tento dokument sa verzuje **samostatne** od Zmluvy o spracúvaní osobných údajov (DPA); tvorí obsah jej prílohy III.

Tento dokument konkrétne opisuje technické a organizačné opatrenia, ktoré spoločnosť **WebHeroes s.r.o.** (sprostredkovateľ, „Klubos“) prijala podľa čl. 32 GDPR na zaistenie bezpečnosti osobných údajov spracúvaných v službe Klubos, ako aj opatrenia, ktorými pomáha prevádzkovateľovi (klubu) pri plnení jeho povinností (doložka 8 písm. d) a doložka 9 DPA).

Model zdieľanej zodpovednosti. Každé opatrenie má určený zodpovedný subjekt: **Klubos** (aplikačná vrstva a prevádzka platformy), **Klub** (prevádzkovateľ — používanie Služby) alebo **Hetzner** (infraštruktúrny sub-sprostredkovateľ). Hetzner Online GmbH zodpovedá **výlučne za fyzickú a infraštruktúrnú vrstvu po hypervízor** (dátové centrá Falkenstein a Norimberg, DE); jeho vlastný TOM dokument označuje správu, údržbu a zabezpečenie cloudových serverov — vrátane aktualizácií, autorizačných postupov a ochrany prenesených dát a softvéru — za **zodpovednosť klienta**. Všetko nad hypervízorom preto zabezpečuje Klubos.

1. Kontrola fyzického prístupu

Opatrenie	Zodpovedný
Fyzické zabezpečenie dátových centier (oplotenie, kamerové systémy, kontrola vstupu, strážna služba) — DC Falkenstein (aplikácia a živé dáta) a DC Norimberg (zálohy)	Hetzner
Preukazovanie úrovne fyzickej bezpečnosti výročnou audítorskou správou TÜV	Hetzner
Žiadne osobné údaje na lokálnych zariadeniach mimo dátových centier; správa výlučne vzdialene cez zabezpečené kanály	Klubos

2. Kontrola elektronického prístupu

Opatrenie	Zodpovedný
Autentifikácia používateľov cez centrálny identitný systém (Keycloak) s riadením relácií	Klubos
Autorizácia na strane servera: každý prístup viazaný na rolu a spôsobilosti (capabilities) v rámci organizácie a klubu	Klubos
Šifrovanie prenášaných údajov (TLS) na všetkých verejných rozhraniach	Klubos
Šifrovanie internej komunikácie medzi uzlami klastra (WireGuard šifrovanie pod-to-pod siete)	Klubos
Dôvernosť prihlasovacích údajov používateľov Klubu; bezodkladné odobratie prístupu osobám, ktoré ho už nemajú mať	Klub

3. Kontrola interného prístupu

Opatrenie	Zodpovedný
Zásada najmenších privilégií pre interný a administrátorský prístup; prístup k produkčným údajom len v rozsahu nevyhnutnom na prevádzku a podporu	Klubos

Opatrenie	Zodpovedný
Závazok dôvernosti osôb oprávnených spracúvať údaje (doložka 7.4 písm. b) DPA)	Klubos
Správa vlastných používateľov, rolí a oprávnení v rámci Organizácie	Klub

4. Kontrola prenosu

Opatrenie	Zodpovedný
Prenos údajov výlučne šifrovanými kanálmi (TLS); žiadne nešifrované exporty	Klubos
Odosielanie e-mailov cez zmluvného sub-sprostredkovateľa (Scaleway S.A.S., EÚ)	Klubos
Zákonnosť a minimalizácia údajov, ktoré Klub do Služby vkladá alebo z nej exportuje	Klub

5. Kontrola oddelenia (izolácia nájomcov)

Opatrenie	Zodpovedný
Viacnájomná izolácia na aplikačnej úrovni: každý dopyt viazaný na organizáciu a klub (scoped queries); serverovo autoritatívne overenie, že volajúci má práva na daný zdroj	Klubos
Identifikátory dodané klientom sa vždy načítavajú cez dopyty viazané na rozsah organizácie a klubu; prístup mimo rozsahu sa správa ako neexistujúci zdroj	Klubos
Oddelenie prostredí (produkcia vs. vývoj/test); testovacie prostredia nepoužívajú produkčné osobné údaje	Klubos

6. Kontrola vstupu

Opatrenie	Zodpovedný
Append-only auditný záznam konsekvencných akcií (aktér, akcia, cieľ, rozsah organizácie/klubu, čas UTC) — nemenný na úrovni databázy	Klubos
Štruktúrované prevádzkové logy bez hodnôt osobných údajov	Klubos
Zodpovednosť za obsahovú správnosť údajov vkladaných používateľmi Klubu	Klub

7. Kontrola dostupnosti

Opatrenie	Zodpovedný
Redundantná infraštruktúra dátových centier (napájanie, konektivita)	Hetzner
Zálohovanie databázy: denná záloha s priebežnou archiváciou transakčného denníka (obnova k bodu v čase, PITR); záložné dáta sú šifrované ; retencia záloh 30 dní ; úložisko záloh v DC Norimberg (nbg1), v samostatnom projekte oddelenom od živých dát (Falkenstein); obnova záloh sa pravidelne testuje — <i>podmienka spustenia ostrej prevádzky</i>	Klubos

Opatrenie	Zodpovedný
Health-proby, prevádzkový monitoring a alerting (výlučne self-hosted nástroje); riadené odstavovanie (graceful shutdown)	Klubos
Kontajnery bežia bez oprávnení root, s deklarovanými health-checkmi	Klubos

8. Kontrola zákaziek a pokynov

Opatrenie	Zodpovedný
Spracúvanie výlučne na základe zdokumentovaných pokynov prevádzkovateľa (doložka 7.1 DPA); pokynom je konfigurácia a používanie funkcií Služby	Klubos
Zákaz použitia údajov spracúvaných pre kluby na vlastné účely Klubosu (čl. 28 ods. 10 GDPR); marketingové publikum sa tvorí výlučne z registračného opt-in príznaku	Klubos
Písomné zmluvy podľa čl. 28 GDPR so všetkými sub-sprostredkovateľmi (príloha IV DPA)	Klubos
Integrita dodávateľského reťazca v CI: skenovanie závislostí (SCA/CVE), skenovanie tajomstiev, SBOM, statická bezpečnostná analýza (SAST), podpisovanie kontajnerových obrazov	Klubos

9. Opatrenia na pomoc prevádzkovateľovi s právami dotknutých osôb

Opatrenie	Zodpovedný
Nástroje Služby na export údajov člena v strojovo čitateľnom formáte (čl. 15, 20 GDPR)	Klubos
Nástroje Služby na vymazanie/anonymizáciu údajov člena so zachovaním zákonných uchovávacích povinností (legal hold)	Klubos
Vybavovanie žiadostí dotknutých osôb voči členom; identifikácia žiadateľa	Klub

10. Opatrenia na detekciu a oznamovanie porušení ochrany údajov

Opatrenie	Zodpovedný
Priebežný monitoring a alerting prevádzkových a bezpečnostných signálov	Klubos
Append-only auditný záznam ako podklad pre forenznú analýzu a dokumentáciu porušenia (doložka 9.2 DPA)	Klubos
Interný postup reakcie na incidenty vrátane lehôt oznámení a interného registra porušení (interný dokument, verzia z 2026-08-05)	Klubos
Bezodkladné oznámenie porušenia zisteného na strane Klubu (napr. kompromitovaný účet)	Klub

Vývoj opatrení (doložka o vývoji)

1. Opatrenia v tomto dokumente podliehajú technickému pokroku a ďalšiemu vývoju. Klubos smie zaviesť **alternatívne primerané opatrenia**, úroveň zabezpečenia stanovená týmto dokumentom sa však **nesmie znížiť** (záväzok neznižovania).
2. Podstatné zmeny sa dokumentujú; každá predchádzajúca verzia zostáva **archivovaná** s dátumom platnosti a je na požiadanie prístupná prevádzkovateľovi.
3. Aktualizácia tohto dokumentu je aktualizáciou informácií v prílohe DPA podľa doložky 2 písm. a) — **nevyžaduje novú akceptáciu DPA** a nemení jej verziu.