*Version: 1.0, effective from **1 August 2026** (client decision 2026-08-05) — this document is versioned **separately** from the Data Processing Agreement (DPA); it constitutes the content of its Annex III.*

**The Slovak version is the governing text.**

This document specifically describes the technical and organisational measures adopted by **WebHeroes s.r.o.** (processor, "Klubos") pursuant to Art. 32 GDPR to ensure the security of personal data processed in the Klubos service, as well as the measures by which it assists the controller (club) in fulfilling its obligations (Clause 8(d) and Clause 9 of the DPA).

**Shared-responsibility model.** Every measure has a designated responsible party: **Klubos** (application layer and platform operations), **Club** (controller — use of the Service) or **Hetzner** (infrastructure sub-processor). Hetzner Online GmbH is responsible **exclusively for the physical and infrastructure layer up to the hypervisor** (Falkenstein and Nuremberg data centres, DE); its own TOM document designates the management, maintenance and security of cloud servers — including updates, authorisation procedures and the protection of transferred data and software — as the **client's responsibility**. Everything above the hypervisor is therefore secured by Klubos.

## 1. Physical access control

| Measure | Responsible |
|---|---|
| Physical security of the data centres (fencing, CCTV, entry control, security service) — Falkenstein DC (application and live data) and Nuremberg DC (backups) | Hetzner |
| Evidence of the physical-security level via the annual TÜV audit report | Hetzner |
| No personal data on local devices outside the data centres; administration exclusively remote over secured channels | Klubos |

## 2. Electronic access control

| Measure | Responsible |
|---|---|
| User authentication via a central identity system (Keycloak) with session management | Klubos |
| Server-side authorisation: every access bound to a role and capabilities within the organisation and club | Klubos |
| Encryption of data in transit (TLS) on all public interfaces | Klubos |
| Encryption of internal traffic between cluster nodes (WireGuard encryption of the pod-to-pod network) | Klubos |
| Confidentiality of the Club's user credentials; prompt removal of access from persons who should no longer have it | Club |

## 3. Internal access control

| Measure | Responsible |
|---|---|
| Least-privilege principle for internal and administrator access; access to production data only to the extent necessary for operations and support | Klubos |
| Confidentiality undertaking of persons authorised to process data (Clause 7.4(b) of the DPA) | Klubos |
| Management of the Organisation's own users, roles and permissions | Club |

## 4. Transfer control

| Measure | Responsible |
|---|---|
| Data transfer exclusively over encrypted channels (TLS); no unencrypted exports | Klubos |
| E-mail dispatch via a contracted sub-processor (Scaleway S.A.S., EU) | Klubos |
| Lawfulness and minimisation of the data the Club enters into or exports from the Service | Club |

## 5. Separation control (tenant isolation)

| Measure | Responsible |
|---|---|
| Multi-tenant isolation at the application level: every query bound to the organisation and club (scoped queries); server-authoritative verification that the caller holds rights to the resource | Klubos |
| Client-supplied identifiers are always loaded through organisation- and club-scoped queries; out-of-scope access behaves as a non-existent resource | Klubos |
| Environment separation (production vs. development/test); test environments do not use production personal data | Klubos |

## 6. Input control

| Measure | Responsible |
|---|---|
| Append-only audit log of consequential actions (actor, action, target, organisation/club scope, UTC time) — immutable at the database level | Klubos |
| Structured operational logs without personal-data values | Klubos |
| Responsibility for the substantive accuracy of data entered by the Club's users | Club |

## 7. Availability control

| Measure | Responsible |
|---|---|
| Redundant data-centre infrastructure (power, connectivity) | Hetzner |

| Measure | Responsible |
|---|---|
| Database backups: daily backup with continuous transaction-log archiving (point-in-time recovery, PITR); **backup data are encrypted**; backup retention **30 days**; backup storage in the Nuremberg DC (nbg1), in a separate project isolated from the live data (Falkenstein); restores are tested regularly — *a go-live prerequisite* | Klubos |
| Health probes, operational monitoring and alerting (self-hosted tooling only); graceful shutdown | Klubos |
| Containers run as non-root, with declared health checks | Klubos |

## 8. Job and instruction control

| Measure | Responsible |
|---|---|
| Processing exclusively on the controller's documented instructions (Clause 7.1 of the DPA); configuration and use of the Service's functions constitute instructions | Klubos |
| Prohibition on using data processed for clubs for Klubos's own purposes (Art. 28(10) GDPR); the marketing audience is built exclusively from the registration opt-in flag | Klubos |
| Written Art. 28 GDPR contracts with all sub-processors (Annex IV of the DPA) | Klubos |
| Supply-chain integrity in CI: dependency scanning (SCA/CVE), secret scanning, SBOM, static security analysis (SAST), container image signing | Klubos |

## 9. Measures assisting the controller with data-subject rights

| Measure | Responsible |
|---|---|
| Service tooling for exporting a member's data in a machine-readable format (Arts. 15, 20 GDPR) | Klubos |
| Service tooling for erasing/anonymising a member's data while honouring statutory retention obligations (legal hold) | Klubos |
| Handling data-subject requests addressed to members; identification of the requester | Club |

## 10. Measures for detecting and notifying personal-data breaches

| Measure | Responsible |
|---|---|
| Continuous monitoring and alerting of operational and security signals | Klubos |
| Append-only audit log as the basis for forensic analysis and breach documentation (Clause 9.2 of the DPA) | Klubos |
| Internal incident-response procedure including notification deadlines and the internal breach register (internal document, version of 2026-08-05) | Klubos |
| Prompt notification of a breach detected on the Club's side (e.g. a compromised account) | Club |

## Evolution of the measures (evolution clause)

1. The measures in this document are subject to technical progress and further development. Klubos may introduce **alternative adequate measures**; however, the security level established by this document **must not be reduced** (non-degradation undertaking).
2. Material changes are documented; every previous version remains **archived** with its validity date and is available to the controller on request.
3. An update of this document constitutes an update of information in a DPA annex pursuant to Clause 2(a) — it **does not require a new acceptance of the DPA** and does not change the DPA's version.