Technical and organisational measures (TOMs)

Annex 2 to the Data Processing Agreement (DPA) between atvari GmbH and the Controller

The measures are based on the operational stack of atvari GmbH (Nix-based reproducible builds, git-tracked changes, EU vendors, static-first architecture) and are reviewed annually as part of the self-attestation under DPA § 6 para. 2 / Annex 1 § 5. Version **v1.1, 2026-10-30**.

I. Confidentiality

- Access to processing environments only via personal accounts on a need-to-know basis; multi-factor authentication enforced on every company account that supports it (Proton, Codeberg, Hetzner, sevDesk, Clockodo, fynk, sipgate, Munito/OpenCode Console)
- Client passwords, keys and access data exclusively in the purpose-bound vault (Proton Pass) per Annex 1 § 4
- Full-disk encryption on all work machines
- Encrypted transport (TLS) for all services; the website sends X-Content-Type-Options: nosniff, while HSTS and further hardening headers remain pending with the hosting platform (our own git-pages instance on Hetzner servers)
- Data minimisation documented on the trust page: **no cookies**, only aggregated, non-personal web analytics from our self-hosted Plausible instance, localStorage used in the browser only (atvari.eu/trust)
- Confidentiality undertakings of employees from the first day of engagement (DPA § 4)

II. Integrity

- Every change to systems and the website runs through **git-tracked, versioned changes** (Forgejo/Codeberg); history and authorship are traceable
- **Reproducible builds** from locked files (Nix flakes); deployment automated via CI pipeline
- Production and test environments separated: client environments are strictly per the SoW, with no shared accounts or tenants between clients
- Dependencies updated via pinned locks; releases controlled by atvari: security advisories are reviewed continuously, critical items are mitigated within 7 days, everything else follows the monthly update cycle
- Access and activity logs are kept on the servers we operate (hosted at Hetzner) and by our email provider; disclosure to the Controller per Annex 1 § 5

III. Availability and resilience

- Architecture **“static first”**: no dynamic server components without need; minimal attack surface
- Hosting at the EU provider Hetzner including its availability and load protection; the services themselves (website, analytics) are operated by us; the current provider list is published at atvari.eu/trust
- Backups/restore: operational state rests with the SaaS vendors (Proton, sevDesk, Clockodo, fynk); the website is stateless and rebuildable from the Codeberg git history; work machine data syncs to Proton Drive; no atvari-side backups for project-specific client infrastructure (per SoW)
- Incident and notification route: public security contact (/.well-known/security.txt, PGP-pinned) and notification to the Controller per DPA § 7

IV. Procedures for regular review, assessment and evaluation

- **Annual TOM review** with documented self-attestation (Annex 1 § 5)
- unscheduled review after significant architecture, vendor or legal changes
- the trust page (atvari.eu/trust) as well as security.txt (with a fixed “Expires” date) document the current state in a machine- and human-readable way

as Annex 2 to the DPA of

atvari GmbH	Controller
Date	Date