Technische und organisatorische Maßnahmen (TOMs)

Anlage 2 zum Auftragsverarbeitungsvertrag (AVV) zwischen atvari GmbH und dem Verantwortlichen

Die Maßnahmen beruhen auf dem betrieblichen Stack der atvari GmbH (Nix-basierte reproduzierbare Builds, git-geführte Änderungen, EU-Anbieter, statisch-orientierte Architektur) und werden jährlich im Rahmen der Selbstauskunft gemäß AVV § 6 Abs. 2 / Anlage 1 § 5 bewertet. Fassung **v1.1, 2026-10-30**.

I. Vertraulichkeit

- Zugriff auf Verarbeitungsumgebungen nur über persönliche Konten nach dem Need-to-know-Grundsatz; Mehrfaktor-Authentifizierung auf allen Firmenkontos, die sie unterstützen (Proton, Codeberg, Hetzner, sevDesk, Clockodo, fynk, sipgate, Munito/OpenCode Console)
- Passwörter, Schlüssel und Zugangsdaten der Kunden ausschließlich im zweckgebundenen Vault (Proton Pass) gemäß Anlage 1 § 4
- Vollständige Datenträgerverschlüsselung auf allen Arbeitsgeräten
- Verschlüsselte Übertragung (TLS) für alle Dienste; die Website sendet X-Content-Type-Options: nosniff, während HSTS und weitere Härtungsheader auf der Hosting-Plattform (eigene git-pages-Instanz auf Hetzner-Servern) noch ausstehen
- Datenminimalismus dokumentiert auf der Trust-Seite: **keine Cookies**, nur aggregierte, personenunbezogene Webanalyse aus unserer selbst betriebenen Plausible-Instanz, ausschließliche LocalStorage-Nutzung im Browser (atvari.eu/trust)
- Vertraulichkeitsverpflichtung von Beschäftigten ab Beschäftigungsbeginn (AVV § 4)

II. Integrität

- Jede Änderung an Systemen und Website läuft über **git-geführte, versionierte Änderungen** (Forgejo/Codeberg); Geschichte und Urheber sind nachvollziehbar
- **Reproduzierbare Builds** aus gesperrten Lock-Files (Nix-Flakes); Deployment automatisiert über CI-Pipeline
- Produktions- und Testumgebungen getrennt: Kundenumgebungen strikt je SoW, keine gemeinsamen Konten oder Mandanten zwischen Kunden
- Abhängigkeiten werden über gepinnte Locks aktualisiert; Freigaben atvari-seitig gesteuert: Sicherheitsmeldungen werden laufend geprüft, kritische innerhalb von 7 Tagen behandelt, das Übrige im monatlichen Update-Zyklus
- Zugriffsprotokolle liegen auf den von uns betriebenen Servern (gehostet bei Hetzner) sowie beim Mailanbieter; Einsicht an den Verantwortlichen nach Anlage 1 § 5

III. Verfügbarkeit und Belastbarkeit

- Architektur **„statisch zuerst“**: keine dynamischen Serveranteile ohne Notwendigkeit; kleinstmögliche Angriffsfläche
- Hosting beim EU-Anbieter Hetzner mit dessen Verfügbarkeits- und Lastabsicherung; die Dienste selbst (Website, Analyse) betreiben wir; die aktuelle Anbieterliste ist auf atvari.eu/trust veröffentlicht
- Backups/Wiederherstellung: der Betriebszustand liegt bei den SaaS-Anbietern (Proton, sevDesk, Clockodo, fynk); die Website ist zustandslos und aus der Codeberg-Git-Historie neu baubar; Arbeitsgerätedaten spiegeln nach Proton Drive; keine atvari-seitigen Backups für projektspezifische Kundeninfrastruktur (je SoW)
- Störungs- und Meldeweg: öffentlicher Sicherheitskontakt (/.well-known/security.txt, PGP-pinned) sowie Meldung an den Verantwortlichen gemäß AVV § 7

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- **Jährliche TOM-Überprüfung** mit dokumentierter Selbstauskunft (Anlage 1 § 5)
- außerplanmäßige Prüfung nach signifikanten Architektur-, Anbieter- oder Rechtsänderungen
- die Trust-Seite (atvari.eu/trust) sowie security.txt (mit festem „Expires“-Datum) dokumentieren den aktuellen Stand maschinenlesbar und menschenlesbar

als Anlage 2 zum AVV vom

atvari GmbH	Verantwortlicher
Datum	Datum