

# AGIONT.wellbeing — Security Controls Overview

Sicherheitskontrollen-Übersicht | Deutsch & English

Stand: Mai 2026 — Version 2.1

Wir arbeiten mit:

 **AGIONT.wellbeing**

## Inhalt

<b>Executive Summary</b> .....	<b>4</b>
<b>1. Geltungsbereich</b> .....	<b>4</b>
<b>2. Sicherheitsarchitektur im Überblick</b> .....	<b>5</b>
<b>3. Identitäts- und Zugriffsmanagement</b> .....	<b>6</b>
3.1 Administrativer Zugriff über Tailscale.....	6
3.2 Endnutzer-Authentifizierung.....	6
3.3 Berechtigungskonzept .....	7
<b>4. Verschlüsselung und Schlüsselverwaltung</b> .....	<b>7</b>
<b>5. Netzwerksicherheit</b> .....	<b>7</b>
<b>6. Sicherer Betrieb</b> .....	<b>8</b>
<b>7. Backup und Wiederherstellung</b> .....	<b>8</b>
<b>8. Incident Response</b> .....	<b>9</b>
8.1 Reaktionsverfahren .....	9
8.2 Kommunikation mit Kunden .....	9
8.3 Forensische Bereitschaft .....	9
<b>9. Schwachstellen- und Patch-Management</b> .....	<b>9</b>
9.1 Identifikation .....	9
9.2 Behebung .....	9
9.3 Penetrationstests .....	10
<b>10. Sub-Auftragsverarbeiter</b> .....	<b>10</b>
<b>11. Compliance und Datenschutz</b> .....	<b>11</b>
11.1 DSGVO .....	11
11.2 Datenlöschung .....	11
11.3 Cyberversicherung und Mitarbeiter-Schulungen .....	11
11.4 ISO/IEC 27001:2022.....	12
<b>Anhang A — Kontroll-Mapping ISO/IEC 27001:2022 (Auswahl)</b> .....	<b>12</b>
<b>English Version</b> .....	<b>14</b>
<b>Executive Summary</b> .....	<b>14</b>
<b>1. Scope</b> .....	<b>14</b>
<b>2. Security Architecture Overview</b> .....	<b>15</b>
<b>3. Identity and Access Management</b> .....	<b>15</b>

- 3.1 Administrative Access via Tailscale ..... 15
- 3.2 End-User Authentication ..... 16
- 3.3 Authorisation Model..... 16
- 4. Encryption and Key Management ..... 16**
- 5. Network Security ..... 16**
- 6. Secure Operations ..... 17**
- 7. Backup and Recovery ..... 17**
- 8. Incident Response ..... 18**
  - 8.1 Response Procedure ..... 18
  - 8.2 Customer Communication ..... 18
  - 8.3 Forensic Readiness ..... 18
- 9. Vulnerability and Patch Management..... 18**
  - 9.1 Identification..... 18
  - 9.2 Remediation ..... 18
  - 9.3 Penetration Testing..... 19
- 10. Sub-Processors ..... 19**
- 11. Compliance and Data Protection ..... 20**
  - 11.1 GDPR ..... 20
  - 11.2 Data Deletion ..... 20
  - 11.3 Cyber Insurance and Staff Training ..... 20
  - 11.4 ISO/IEC 27001:2022..... 21
- Annex A — ISO/IEC 27001:2022 Control Mapping (Selection) ..... 21**

## Executive Summary

AGIONT.wellbeing wird als B2B-SaaS-Plattform für die Gefährdungsbeurteilung psychischer Belastungen betrieben. Diese Übersicht beschreibt die produktive Sicherheitsarchitektur und richtet sich an Compliance-Officer, Datenschutzbeauftragte und Beschaffungsverantwortliche.

Die zentralen Punkte im Überblick:

- Hosting in Hetzner-Rechenzentren in Frankfurt am Main. Drei dedizierte Server (Production, Monitoring, Survey) im privaten VLAN. Keine Datenausleitung in Drittländer.
- Administrativer Zugriff ausschließlich über Tailscale-Mesh-VPN. Kein öffentlicher SSH-Port, kein Root-Login. CI/CD-Deployments über Tailscale-OAuth-Tag — keine SSH-Keys im Repository.
- Endnutzer-Authentifizierung passwortlos über signierten Login-Link. Keine Passwort-Datenbank.
- TLS 1.3 mit HSTS für Web-Verkehr. Storage- und Backup-Verschlüsselung mit getrennter Schlüsselhaltung.
- Privacy-by-Design: technisch erzwungene Mindestgruppengrößen, Pseudonymisierung ab Werk.
- Backup über Restic mit AES-256: stündlich für Datenbanken, täglich vollständig, wöchentlich vollständige Snapshots — auf separater Storagebox; Object Storage als zweites Restic-Remote in Setup.
- Zentrale Log-Aggregation, SMS-Eskalation kritischer Sicherheitsereignisse innerhalb Minuten.
- Erstmeldung sicherheitsrelevanter Vorfälle an Kunden binnen 24 Stunden, DSGVO-Meldungen binnen 72 Stunden.
- Cyberversicherung mit Drittschadens- und Eigenschadens-Deckung. Jährliche Pflicht-Sicherheitsschulung aller Mitarbeitenden mit Zertifikat.

Das Dokument ist kein Zertifizierungsnachweis. Es orientiert sich an den Kontrollbereichen ISO/IEC 27001:2022 und ISO/IEC 27002:2022, ohne deren formale Zertifizierung zu beanspruchen.

## 1. Geltungsbereich

AGIONT.wellbeing ist eine B2B-SaaS-Plattform für Mitarbeitendenbefragungen, Berichterstellung und damit verbundene organisatorische Prozesse, einschließlich Maßnahmenmanagement und Workshop-Protokollierung. Dieses Dokument deckt die produktiven Komponenten und die zugehörigen Überwachungs- und Betriebssysteme ab.

Verantwortlich für den Inhalt: Thomas Artmann, Geschäftsführer der EUDEMOS Beratungsgesellschaft GmbH, Berlin-Schönefeld. Externer Datenschutzbeauftragter: Mag. jur. Djoko Lukic, Hamburg.

## 2. Sicherheitsarchitektur im Überblick

Die Plattform wird in den Hetzner-Rechenzentren in Frankfurt am Main betrieben und besteht aus drei logisch und netzwerktechnisch getrennten Servern in einem privaten VLAN:

- Production Server: Webanwendung, API, Datenbanken, Authentifizierung. Containerisiert über Coolify mit Traefik als TLS-Reverse-Proxy.
- Monitoring Server: Metrik-Erfassung, Log-Aggregation, Alerting. Nicht öffentlich erreichbar.
- Survey Server: Befragungs-Frontend, mehrmandantenfähig, vom App-Layer entkoppelt.

Auf dem öffentlichen Interface des Production-Servers sind ausschließlich die Web-Ports 80 (Redirect auf 443) und 443 (TLS) exponiert. Sämtliche administrativen Verbindungen — interaktiv durch Administratoren ebenso wie automatisiert durch die CI/CD-Pipeline — laufen über das Tailscale-Mesh-VPN.

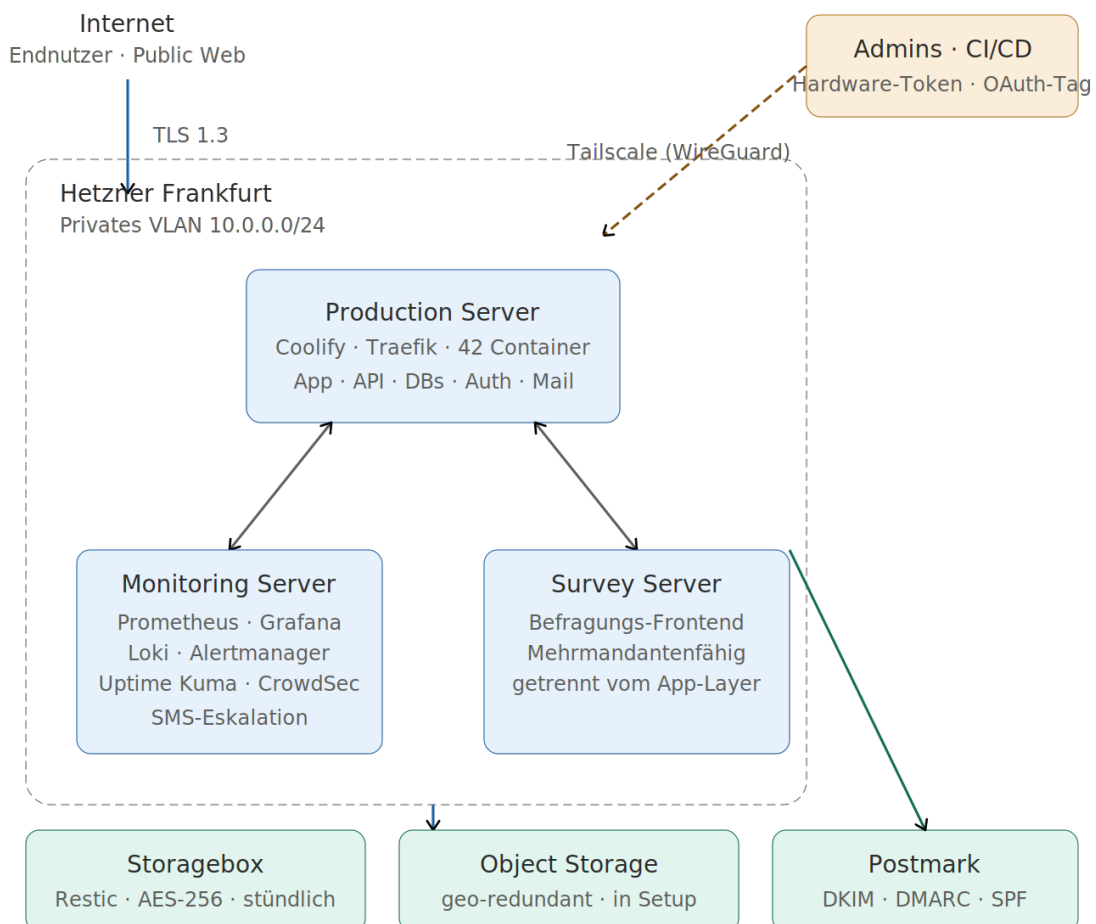


Abbildung 1: AGIONT.wellbeing Sicherheitsarchitektur — Hetzner Frankfurt mit drei Servern, Tailscale-Mesh für administrativen Zugriff, Restic-Backup auf separater Storagebox.

## 3. Identitäts- und Zugriffsmanagement

### 3.1 Administrativer Zugriff über Tailscale

Sämtliche administrativen Verbindungen zu Production und Monitoring laufen über ein Tailscale-Mesh-VPN auf Basis von WireGuard. Die Server haben keinen aus dem Internet erreichbaren SSH-Daemon; SSH ist exklusiv an das Tailscale-Interface gebunden.

Die Architektur im Detail:

- Kein öffentlicher SSH-Port. SSH lauscht ausschließlich auf der internen Tailscale-Schnittstelle.
- Kein Root-Login. Direkter Login als Root ist deaktiviert; administrative Aktionen erfolgen über sudo durch einen schlüsselbasiert authentifizierten Benutzer.
- Schlüsselbasierte Authentifizierung. Passwort-Login ist abgeschaltet. Schlüsseltypen sind auf moderne Algorithmen beschränkt.
- Hardware-Token. Wo unterstützt, kommen YubiKey/Passkey-basierte Verfahren zum Einsatz.
- Tailscale-ACLs. Zugriff ist auf benannte Identitäten und Tags eingeschränkt; alle Verbindungen werden zentral protokolliert.
- CI/CD über Tailscale-OAuth-Tag. Die Deployment-Pipeline (GitHub Actions) authentifiziert sich über einen dedizierten OAuth-Tag und erhält Zugriff ausschließlich auf die für das Deployment benötigten Knoten. Es liegen keine SSH-Keys oder Server-Credentials im Code-Repository.

Diese Architektur reduziert die externe Angriffsfläche der administrativen Schnittstelle auf null. Brute-Force-Versuche, gängige SSH-Exploits und Scans aus dem Internet erreichen den SSH-Dienst nicht. Tailscale-seitig ist nur authentifizierter Verkehr von berechtigten Knoten zulässig; Verbindungen werden Ende-zu-Ende über WireGuard verschlüsselt.

### 3.2 Endnutzer-Authentifizierung

Endnutzer melden sich passwortlos an. Beim Login wird ein zeitlich begrenzter, signierter Link an die hinterlegte E-Mail-Adresse gesendet. Daraus folgt:

- Es wird kein Passwort erfasst, gespeichert oder gehasht.
- Klassische Credential-Stuffing-Angriffe sind ausgeschlossen, da kein Passwort existiert.
- Bei Datenlecks externer Dienste sind keine Passwort-Hashes von AGIONT.wellbeing-Nutzenden betroffen.

### 3.3 Berechtigungskonzept

Berechtigungen folgen dem Need-to-know- und Least-Privilege-Prinzip. Das System unterstützt rollenbasierte Berechtigungen über mehrere Hierarchieebenen (Konzern, Bereich, Abteilung, Team) mit feingranularer Vererbung. Datenbankseitig sind Datensätze pro Mandant getrennt; ein kundenseitiger Zugriff auf Daten anderer Kunden ist technisch ausgeschlossen.

## 4. Verschlüsselung und Schlüsselverwaltung

- In transit: Sämtlicher öffentlicher Datenverkehr läuft über TLS 1.3 mit Fallback auf TLS 1.2. HTTP-Anfragen werden per 301 auf HTTPS umgeleitet. HSTS ist mit einem Jahr Geltungsdauer aktiv.
- At rest: Datenbanken und Datei-Storage liegen auf verschlüsselten Block-Devices der Hosting-Infrastruktur. Backups werden über Restic separat AES-256-verschlüsselt auf getrennter Infrastruktur abgelegt; der Restic-Repository-Schlüssel wird separat vom Repository selbst verwaltet.
- Secrets: Datenbank-Credentials und API-Keys werden über die Umgebungskonfiguration verwaltet. Geheimnisse werden nicht in Quellcode-Repositories gespeichert.
- Schlüssel-Rotation: TLS-Zertifikate werden über Let's Encrypt automatisiert erneuert. Datenbank- und Service-Account-Credentials werden anlassbezogen rotiert (Personalwechsel, Vorfälle) sowie nach festem Plan.

## 5. Netzwerksicherheit

Die externe Angriffsfläche ist auf das absolute Minimum reduziert.

- Public Exposure: Lediglich 80 (Redirect) und 443 (TLS) sind aus dem Internet erreichbar. Datenbanken, Caches und Monitoring-Endpunkte sind ausschließlich im privaten Tailscale-Mesh erreichbar.
- Container-Isolation: Anwendungs-Container kommunizieren über interne Docker-Netzwerke hinter Traefik als TLS-Reverse-Proxy. Eine explizite DOCKER-USER-iptables-Kette verhindert das versehentliche Exponieren von Container-Ports.
- Hetzner Cloud Firewall: Vorgelagerte Netzwerk-Firewall auf Hetzner-Ebene ergänzt die OS-seitige iptables-Konfiguration. Zwei unabhängige Firewall-Schichten.
- Intrusion Prevention: CrowdSec mit Community-Bedrohungsfeeds bannt automatisch IPs, die typische Angriffsmuster zeigen (Scraper, bekannte Exploit-Pfade, Web-Layer-Brute-Force gegen Login-Endpunkte).

## 6. Sicherer Betrieb

Die Beobachtbarkeitsschicht läuft auf einem dedizierten Monitoring-Server, getrennt vom Produktivsystem. Sie umfasst:

- Metrik-Erfassung in kurzen Intervallen für Host- und Container-Telemetrie (CPU, RAM, Disk-IO, Service-Health) mit Visualisierung in einem zentralen Dashboard.
- Zentrale Log-Aggregation für System- und Anwendungs-Logs. Sicherheitsrelevante Ereignisse (fehlgeschlagene Authentifizierung, Indikatoren für Injection-Versuche, ungewöhnliche Anfrage-Pattern) werden anhand definierter Regeln markiert und priorisiert.
- Aktive Endpunkt-Verfügbarkeitsprüfung der öffentlich erreichbaren Dienste, inkl. anwendungsspezifischer Deep-Checks (z. B. Login-Funktionalität).

Kritische Alerts werden vom Alertmanager nach Schweregrad geroutet und eskalieren binnen Minuten per SMS an den Geschäftsführer und das Operations-Team. Niederschwellige Ereignisse (z. B. CrowdSec-Bans gegen bekannte Scanner) werden gefiltert und fließen ohne SMS-Eskalation ins Dashboard, um Alarm-Müdigkeit zu vermeiden.

## 7. Backup und Wiederherstellung

Backups werden über Restic auf eine dedizierte Hetzner-Storagebox geschrieben. Restic verschlüsselt mit AES-256 und nutzt Content-Addressed Storage mit Deduplizierung — nur tatsächliche Änderungen werden übertragen und gespeichert.

Konkrete Backup-Strategie:

- Stündlich: SQL-Dumps aller Produktionsdatenbanken (App-Datenbank, Authentifizierung, Coolify, Chatwoot, LimeSurvey).
- Täglich (≈03:00 Uhr): inkrementeller Vollsnapshot inklusive Anwendungs-Code und Konfigurationen.
- Wöchentlich (sonntags): vollständiger Snapshot aller Datenbestände.
- Retention: 30 tägliche Snapshots, 8 wöchentliche Snapshots. Automatisches Pruning außerhalb der Retention-Policy.
- Täglicher Backup-Status-Report; Alerts bei ausgebliebenen Backups.

Die Wiederherstellungsfähigkeit wird durch periodische Restore-Tests verifiziert. Als zweites Restic-Remote für georedundante Sicherung wird derzeit Hetzner Object Storage eingerichtet. RTO und RPO werden durch eine Business Impact Analysis (BIA) bestimmt und richten sich nach der Kritikalität der Dienste (Authentifizierung, Befragungsteilnahme, Berichts-API).

## 8. Incident Response

### 8.1 Reaktionsverfahren

Dokumentierte Verfahren regeln Erkennung, Klassifizierung, Eindämmung, Beseitigung und Wiederherstellung. Jeder Vorfall wird im Anschluss in einem Lessons-Learned-Termin nachbesprochen; identifizierte Härungsmaßnahmen fließen in den Backlog.

### 8.2 Kommunikation mit Kunden

Bei sicherheitsrelevanten Vorfällen mit Auswirkung auf Kundendaten gelten folgende Zeiten:

- Erstmeldung an betroffene Kunden: binnen 24 Stunden nach Kenntnis.
- Statusaktualisierungen während der Behebung: mindestens werktäglich.
- Abschlussbericht inkl. Ursachenanalyse: binnen 30 Tagen nach Vorfallabschluss.
- DSGVO-relevante Datenpannen: Meldung an die Aufsichtsbehörde gemäß Art. 33 DSGVO binnen 72 Stunden.

### 8.3 Forensische Bereitschaft

Bei schwerwiegenden Vorfällen werden Beweismittel kontrolliert gesichert, Integritäts-Hashes der relevanten Artefakte berechnet und Bearbeitungsschritte dokumentiert. Die Hinzuziehung externer Forensik-Spezialisten ist vorgesehen, falls Umfang oder Kritikalität des Vorfalls dies erfordern.

## 9. Schwachstellen- und Patch-Management

### 9.1 Identifikation

Wir verfolgen kontinuierlich:

- Sicherheitshinweise zu Betriebssystem und Kernel der eingesetzten Distributionen.
- Sicherheitslücken in Anwendungs-Abhängigkeiten über Container-Image-Scanning und Dependency-Audit der Software-Bill-of-Materials.
- Aktive Sicherheitswarnungen für eingesetzte Komponenten und Frameworks.

### 9.2 Behebung

Schwachstellen werden anhand von CVSS-Score und Komponentenkritikalität priorisiert. Internetfacing Komponenten haben Vorrang. Richtwerte für die Behebung:

- Kritisch (CVSS  $\geq 9,0$ ): binnen 7 Kalendertagen.
- Hoch (CVSS 7,0–8,9): binnen 30 Kalendertagen.

- Mittel/niedrig: im Rahmen geplanter Wartungsfenster.

Die Wirksamkeit von Patches und Mitigationen wird über die Beobachtbarkeitsschicht (Service-Status, Fehlerraten, Sicherheitsindikatoren) verifiziert.

### 9.3 Penetrationstests

Wir setzen aktuell KI-gestützte Penetrationstests ein, die folgende Klassen abdecken:

- OWASP-Top-10-Pattern: Injection, Broken Authentication, Cross-Site-Scripting, unsichere Deserialisierung, Misconfiguration.
- API-Endpunkt-Fuzzing inkl. Authentifizierungs- und Autorisierungslogik.
- Tenant-Isolations-Tests zur Validierung der Mandanten-Trennung.

Wir benennen das offen: KI-gestützte Pentests ersetzen aktuell keine vollumfänglichen menschlichen Pentests. Sie liefern eine breite Erstprüfung mit hoher Wiederholungsfrequenz, haben aber Grenzen bei kreativen Angriffsketten und kontextspezifischen Logikfehlern. Externe Audits durch menschliche Pentester sind als Erweiterungsschritt vorgesehen, sobald Marktreife und Kundenbestand dies wirtschaftlich tragen. Wir verfolgen die Diskussion zur Wirksamkeit beider Ansätze aktiv und passen die Strategie entsprechend an.

## 10. Sub-Auftragsverarbeiter

Folgende Drittparteien werden für den Betrieb von AGIONT.wellbeing eingesetzt. Eine aktualisierte Liste wird unter [eudemos.dk/subprocessors](https://eudemos.dk/subprocessors) gepflegt.

Anbieter	Sitz	Funktion	Datenarten
Hetzner Online GmbH	Frankfurt (DE)	Hosting Production, Monitoring, Survey	sämtliche Produktionsdaten
Hetzner Storagebox	Deutschland (EU)	Backup-Storage (Restic, AES-256)	verschlüsselte Backup-Snapshots
Tailscale Inc.	USA / Kanada (Control Plane)	Mesh-VPN für Admin- und CI/CD-Zugriff	Verbindungs-Metadaten — keine Nutzlast
Microsoft Ireland Operations Ltd.	Irland (EU)	M365 für interne Kommunikation	E-Mails, projektbezogene Dokumente

Anbieter	Sitz	Funktion	Datenarten
Postmark (ActiveCampaign)	USA	Transaktionale E-Mail mit DKIM/DMARC/SPF	E-Mail-Adressen, Login-Link-Tokens
Let's Encrypt (ISRG)	USA	TLS-Zertifikate	öffentliche Domain-Daten

**Hinweis Tailscale:** Die Control Plane liegt außerhalb der EU. Übertragene Nutzdaten (Admin-Sessions, Datei-Übertragungen, CI/CD-Artefakte) sind durch WireGuard Ende-zu-Ende verschlüsselt; Tailscale sieht ausschließlich Verbindungs-Metadaten (welche Knoten verbinden sich wann, wie lange), nicht den Inhalt. Eine Datenverarbeitungsvereinbarung ist abgeschlossen.

## 11. Compliance und Datenschutz

### 11.1 DSGVO

- Datenverarbeitungsvereinbarungen nach Art. 28 DSGVO sind Standardbestandteil jedes Kundenvertrages.
- Externer Datenschutzbeauftragter: Mag. jur. Djoko Lukic, Hamburg.
- Privacy-by-Design: Pseudonymisierung ab Werk; Mindestgruppengrößen sind im System fest verdrahtet und können auch von Administratoren nicht unterlaufen werden.
- Identifizierbare Verarbeitung wird nur ermöglicht, wenn der Anwendungsfall dies ausdrücklich erfordert (z. B. 360-Grad-Feedback).

### 11.2 Datenlöschung

Kundendaten werden auf Anfrage oder zum Vertragsende gelöscht. Automatisierte Aufbewahrungsregeln für Befragungsdaten sind kundenseitig konfigurierbar. Betriebsprotokolle und Sicherheits-Logs werden zur Unterstützung von Untersuchungen und gemäß gesetzlicher Aufbewahrungspflichten vorgehalten und nach Ablauf automatisch gelöscht.

### 11.3 Cyberversicherung und Mitarbeiter-Schulungen

EUEMOS unterhält eine Cyberversicherung mit Drittschadens- und Eigenschadensdeckung. Die Police umfasst Haftpflichtansprüche durch Datenverlust oder Cyber-Vorfälle, Wiederherstellungskosten, Betriebsunterbrechung und forensische Aufklärungskosten.

Sämtliche Mitarbeitende durchlaufen jährlich eine verpflichtende Sicherheitsschulung mit Abschlusszertifikat. Inhalte umfassen unter anderem den Umgang mit personenbezogenen Daten, Phishing-Erkennung, sichere Authentifizierung, Endgeräte-Hygiene und das Verhalten im Vorfallsfall. Die Teilnahme wird personenbezogen dokumentiert.

### 11.4 ISO/IEC 27001:2022

Dieses Dokument orientiert sich an den Kontrollbereichen der ISO/IEC 27001:2022 und ISO/IEC 27002:2022. Eine indikative Zuordnung wesentlicher Kontrollen findet sich in Anhang A. AGIONT.wellbeing ist nicht zertifiziert; das Dokument ersetzt keine Erklärung zur Anwendbarkeit (Statement of Applicability).

## Anhang A — Kontroll-Mapping ISO/IEC 27001:2022 (Auswahl)

Auswahl der für die Plattform-Architektur wesentlichen Kontrollen mit Zuordnung zur Implementierung. Die Tabelle ist nicht vollständig und keine Konformitätserklärung.

Kontrolle	Titel (kurz)	Implementierung bei AGIONT
A.5.1	Richtlinien zur Informationssicherheit	Dokumentierte Policies (Access Control, Data Security, Acceptable Use, Asset Management)
A.5.7	Bedrohungsinformationen	CrowdSec-Community-Feeds, regelmäßige Sicherheitshinweis-Auswertung
A.5.15	Zugriffskontrolle	RBAC, Need-to-know, Tailscale-ACLs, keine gemeinsam genutzten Konten
A.5.23	Sicherheit bei Cloud-Diensten	Hetzner Frankfurt; vorgelagerte Hetzner Cloud Firewall; private Netzwerke
A.5.30	IKT-Bereitschaft für Geschäftskontinuität	BIA-basierte RTO/RPO; Backup- und Restore-Verfahren
A.5.34	Datenschutz und Schutz personenbezogener Daten	DSGVO-konforme Verarbeitung; Datenminimierung; AVV als Standard
A.6.3	Sensibilisierung und Schulung	Jährliche Pflicht-Sicherheitsschulung mit Zertifikat für alle Mitarbeitenden

<b>Kontrolle</b>	<b>Titel (kurz)</b>	<b>Implementierung bei AGIONT</b>
A.8.2	Privilegierte Zugriffsrechte	Tailscale-only Admin-Zugriff; kein Root-Login; SSH per Schlüssel
A.8.5	Sichere Authentifizierung	Schlüssel-SSH, MFA/Hardware-Token, passwortlose Endnutzer-Anmeldung
A.8.8	Schwachstellen-Management	Kontinuierliche Auswertung; CVSS-basierte Priorisierung; KI-gestützte Pentests
A.8.13	Datensicherung	Restic AES-256: stündlich DB, täglich voll, wöchentlich Snapshot
A.8.15	Protokollierung	Zentrale Log-Aggregation für System- und Anwendungs-Logs
A.8.16	Überwachungsaktivitäten	Metrik-Erfassung, Alarmierung mit SMS-Eskalation, Endpunkt-Checks
A.8.24	Verwendung von Kryptografie	TLS 1.3, HSTS; Storage- und Backup-Verschlüsselung; Schlüssel-Trennung

## English Version

### Executive Summary

AGIONT.wellbeing operates as a B2B SaaS platform for psychological workplace risk assessments. This overview describes the production security architecture and is addressed to compliance officers, data protection officers and procurement teams.

Key points at a glance:

- Hosting in Hetzner data centres in Frankfurt am Main, Germany. Three dedicated servers (Production, Monitoring, Survey) on a private VLAN. No data transfer to third countries.
- Administrative access exclusively via Tailscale mesh VPN. No public SSH port, no root login. CI/CD deployments via Tailscale OAuth tag — no SSH keys in the repository.
- Passwordless end-user authentication via signed login link. No password database.
- TLS 1.3 with HSTS for web traffic. Storage and backup encryption with separated key management.
- Privacy by design: technically enforced minimum group sizes, pseudonymisation by default.
- Backups via Restic with AES-256: hourly for databases, daily full, weekly full snapshots — on a separate Storagebox; Object Storage as a second Restic remote being set up.
- Centralised log aggregation, SMS-based escalation of critical security events within minutes.
- Customer notification of security incidents within 24 hours, GDPR notifications within 72 hours.
- Cyber insurance covering third-party and own-damage claims. Mandatory annual security training for all staff with certificate.

This document is not a certification record. It is aligned with the control areas of ISO/IEC 27001:2022 and ISO/IEC 27002:2022 without claiming formal certification.

## 1. Scope

AGIONT.wellbeing is a B2B SaaS platform for employee surveys, reporting, and related organisational processes including action management and workshop documentation. This document covers the production components and the corresponding monitoring and operational systems.

Document owner: Thomas Artmann, Managing Director, EUEDEMOS Beratungsgesellschaft GmbH, Berlin-Schönefeld. External Data Protection Officer: Mag. jur. Djoko Lukic, Hamburg, Germany.

## 2. Security Architecture Overview

The platform is operated in Hetzner data centres in Frankfurt am Main and consists of three logically and network-separated servers on a private VLAN:

- Production server: web application, API, databases, authentication. Containerised via Coolify with Traefik as TLS reverse proxy.
- Monitoring server: metric collection, log aggregation, alerting. Not publicly accessible.
- Survey server: survey frontend, multi-tenant, decoupled from the application layer.

On the public interface of the production server, only web ports 80 (redirect to 443) and 443 (TLS) are exposed. All administrative connections — interactive admin sessions as well as automated CI/CD deployments — traverse the Tailscale mesh VPN.

See Figure 1 in the German section above for the architecture diagram.

## 3. Identity and Access Management

### 3.1 Administrative Access via Tailscale

All administrative connections to production and monitoring traverse a Tailscale mesh VPN based on WireGuard. Servers do not run an internet-reachable SSH daemon; SSH is bound exclusively to the Tailscale interface.

Architecture in detail:

- No public SSH port. SSH listens only on the internal Tailscale interface.
- No root login. Direct root access is disabled; administrative actions go through sudo from a key-authenticated user.
- Key-based authentication. Password login is disabled. Allowed key types are restricted to modern algorithms.
- Hardware tokens. Where supported, YubiKey/Passkey methods are used.
- Tailscale ACLs. Access is restricted to named identities and tags; all connections are centrally logged.
- CI/CD via Tailscale OAuth tag. The deployment pipeline (GitHub Actions) authenticates via a dedicated OAuth tag and obtains access only to the nodes required for deployment. No SSH keys or server credentials reside in the code repository.

This architecture reduces the external attack surface of the administrative interface to zero. Brute-force attempts, common SSH exploits, and internet scans cannot reach the SSH service. On the Tailscale side, only authenticated traffic from authorised nodes is permitted; connections are end-to-end encrypted via WireGuard.

### 3.2 End-User Authentication

End users sign in passwordless. On login, a time-limited, signed link is sent to the registered email address. As a consequence:

- No password is collected, stored, or hashed.
- Classic credential stuffing attacks are eliminated since no password exists.
- Data breaches at unrelated services do not expose any AGIONT.wellbeing user passwords.

### 3.3 Authorisation Model

Permissions follow the need-to-know and least-privilege principles. The system supports role-based authorisation across multiple hierarchy levels (group, division, department, team) with fine-grained inheritance. Records are tenant-isolated at the database layer; cross-tenant data access is technically prevented.

## 4. Encryption and Key Management

- In transit: All public traffic is served over TLS 1.3 with TLS 1.2 fallback. HTTP is redirected to HTTPS via 301. HSTS is active with a one-year max-age.
- At rest: Databases and file storage reside on encrypted block devices of the hosting infrastructure. Backups are separately AES-256-encrypted via Restic on separate infrastructure; the Restic repository key is managed independently of the repository itself.
- Secrets: Database credentials and API keys are managed via environment configuration. Secrets are never stored in source-code repositories.
- Key rotation: TLS certificates are renewed automatically via Let's Encrypt. Database and service-account credentials are rotated on event (personnel changes, incidents) and on a fixed schedule.

## 5. Network Security

The external attack surface is reduced to a strict minimum.

- Public exposure: Only ports 80 (redirect) and 443 (TLS) are reachable from the internet. Databases, caches and monitoring endpoints are reachable only within the private Tailscale mesh.

- Container isolation: Application containers communicate over internal Docker networks behind Traefik as TLS reverse proxy. An explicit DOCKER-USER iptables chain prevents accidental container port exposure.
- Hetzner Cloud Firewall: An upstream network-level firewall on the Hetzner side complements the OS-level iptables configuration. Two independent firewall layers.
- Intrusion prevention: CrowdSec, fed by community threat intelligence, automatically bans IPs exhibiting common attack patterns.

## 6. Secure Operations

Observability runs on a dedicated monitoring server, separated from production. It covers:

- Short-interval metric collection for host and container telemetry (CPU, memory, disk I/O, service health) with visualisation in a centralised dashboard.
- Centralised log aggregation for system and application logs. Security-relevant events (failed authentication, indicators of injection attempts, anomalous request patterns) are flagged based on defined rules.
- Active endpoint availability checks of all publicly reachable services, including application-specific deep checks (e.g. login functionality).

Critical alerts are routed by Alertmanager based on severity and escalate within minutes via SMS to the Managing Director and the operations team. Lower-severity events (e.g. CrowdSec bans against known scanners) are filtered and surfaced via the dashboard without SMS escalation, to avoid alert fatigue.

## 7. Backup and Recovery

Backups are written via Restic to a dedicated Hetzner Storagebox. Restic encrypts with AES-256 and uses content-addressed storage with deduplication — only actual changes are transferred and stored.

Concrete backup strategy:

- Hourly: SQL dumps of all production databases (application database, authentication, Coolify, Chatwoot, LimeSurvey).
- Daily (≈03:00): incremental full snapshot including application code and configurations.
- Weekly (Sundays): full snapshot of all data.
- Retention: 30 daily snapshots, 8 weekly snapshots. Automated pruning outside the retention policy.
- Daily backup status report; alerts on missed backups.

Recoverability is verified through periodic restore tests. As a second Restic remote for geo-redundant backup, Hetzner Object Storage is currently being set up. RTO and RPO are derived from a Business Impact Analysis (BIA) and reflect service criticality (authentication, survey participation, reporting API).

## 8. Incident Response

### 8.1 Response Procedure

Documented procedures cover detection, classification, containment, eradication and recovery. Each incident is reviewed in a lessons-learned session; identified hardening measures enter the backlog.

### 8.2 Customer Communication

For security incidents affecting customer data the following timelines apply:

- Initial notification of affected customers: within 24 hours of detection.
- Status updates during remediation: at least once per business day.
- Final report including root-cause analysis: within 30 days of incident closure.
- GDPR-relevant data breaches: notification to the supervisory authority pursuant to Art. 33 GDPR within 72 hours.

### 8.3 Forensic Readiness

For severe incidents, evidence is preserved in a controlled manner, integrity hashes are computed for relevant artefacts, and processing steps are documented. External forensic specialists are engaged where the scope or criticality of the incident warrants it.

## 9. Vulnerability and Patch Management

### 9.1 Identification

We continuously track:

- Security advisories for the operating system and kernel of the distributions in use.
- Vulnerabilities in application dependencies via container image scanning and dependency auditing of the software bill of materials.
- Active security advisories for the components and frameworks deployed.

### 9.2 Remediation

Vulnerabilities are prioritised by CVSS score and component criticality. Internet-facing components take precedence. Target remediation timelines:

- Critical (CVSS  $\geq$  9.0): within 7 calendar days.

- High (CVSS 7.0–8.9): within 30 calendar days.
- Medium/low: within scheduled maintenance windows.

The effectiveness of patches and mitigations is verified via the observability layer (service status, error rates, security indicators).

### 9.3 Penetration Testing

We currently use AI-driven penetration testing covering:

- OWASP Top 10 patterns: injection, broken authentication, cross-site scripting, insecure deserialisation, misconfiguration.
- API endpoint fuzzing including authentication and authorisation logic.
- Tenant isolation tests to validate multi-tenant separation.

We state this openly: AI-driven pentests do not currently replace full human-led penetration tests. They provide broad first-pass coverage at high frequency, but have limitations on creative attack chains and context-specific business-logic vulnerabilities. External audits by human pentesters are foreseen as an extension step once platform maturity and customer base economically justify it. We follow the discussion on the effectiveness of both approaches actively and adapt the strategy accordingly.

## 10. Sub-Processors

The following third parties are used for the operation of AGIONT.wellbeing. An up-to-date list is maintained at [eudemOS.dk/subprocessors](https://eudemOS.dk/subprocessors).

Provider	Location	Function	Data Categories
Hetzner Online GmbH	Frankfurt (DE)	Hosting Production, Monitoring, Survey	all production data
Hetzner Storagebox	Germany (EU)	Backup storage (Restic, AES-256)	encrypted backup snapshots
Tailscale Inc.	USA / Canada (control plane)	Mesh VPN for admin and CI/CD access	connection metadata only — no payload
Microsoft Ireland Operations Ltd.	Ireland (EU)	M365 for internal communication	emails, project documents

Provider	Location	Function	Data Categories
Postmark (ActiveCampaign)	USA	Transactional email with DKIM/DMARC/SPF	email addresses, login-link tokens
Let's Encrypt (ISRG)	USA	TLS certificates	public domain data

**Note on Tailscale:** The control plane resides outside the EU. Transferred payloads (admin sessions, file transfers, CI/CD artefacts) are end-to-end encrypted via WireGuard; Tailscale only sees connection metadata (which nodes connect, when, and for how long), not the content. A data processing agreement is in place.

## 11. Compliance and Data Protection

### 11.1 GDPR

- Data Processing Agreements pursuant to Art. 28 GDPR are a standard part of every customer contract.
- External Data Protection Officer: Mag. jur. Djoko Lukic, Hamburg.
- Privacy by design: pseudonymisation by default; minimum group sizes are hard-coded and cannot be circumvented even by administrators.
- Identifiable processing is enabled only when the use case explicitly requires it (e.g. 360-degree feedback).

### 11.2 Data Deletion

Customer data is deleted on request or at contract termination. Automated retention rules for survey data are configurable on the customer side. Operational logs and security logs are kept to support investigations and statutory retention obligations and are deleted automatically once their retention period expires.

### 11.3 Cyber Insurance and Staff Training

EUDEMOS maintains a cyber insurance policy covering third-party and own-damage claims. The policy includes liability claims arising from data loss or cyber incidents, recovery costs, business interruption, and forensic investigation costs.

All staff complete a mandatory annual security training with a final certificate. Topics include handling of personal data, phishing recognition, secure authentication, endpoint hygiene, and incident response behaviour. Participation is documented per individual.

## 11.4 ISO/IEC 27001:2022

This document is aligned with the control areas of ISO/IEC 27001:2022 and ISO/IEC 27002:2022. An indicative mapping of key controls is provided in Annex A. AGIONT.wellbeing is not certified; this document does not replace a Statement of Applicability.

## Annex A — ISO/IEC 27001:2022 Control Mapping (Selection)

Selection of controls relevant to the platform architecture, mapped to the corresponding implementation. The table is not exhaustive and is not a declaration of conformity.

Control	Title (short)	AGIONT Implementation
A.5.1	Information security policies	Documented policies (Access Control, Data Security, Acceptable Use, Asset Management)
A.5.7	Threat intelligence	CrowdSec community feeds, periodic security advisory review
A.5.15	Access control	RBAC, need-to-know, Tailscale ACLs, no shared accounts
A.5.23	Information security for cloud services	Hetzner Frankfurt; upstream Hetzner Cloud Firewall; private networks
A.5.30	ICT readiness for business continuity	BIA-based RTO/RPO; backup and restore procedures
A.5.34	Privacy and protection of personal data	GDPR-compliant processing; data minimisation; standard DPA
A.6.3	Awareness, education, and training	Mandatory annual security training with certificate for all staff
A.8.2	Privileged access rights	Tailscale-only admin access; no root login; key-based SSH

<b>Control</b>	<b>Title (short)</b>	<b>AGIONT Implementation</b>
A.8.5	Secure authentication	Key-based SSH, MFA/hardware token, passwordless end-user login
A.8.8	Vulnerability management	Continuous monitoring; CVSS-based prioritisation; AI-driven pentests
A.8.13	Information backup	Restic AES-256: hourly DB, daily full, weekly snapshot
A.8.15	Logging	Centralised log aggregation for system and application logs
A.8.16	Monitoring activities	Metric collection, alerting with SMS escalation, endpoint checks
A.8.24	Use of cryptography	TLS 1.3, HSTS; storage and backup encryption; key separation