GRUND INSTITUTE
COGNITION BY DESIGN

PUBLIC

Trust & Compliance Overview

GRUNDMIND
A Grund Institute company · Switzerland
GM-TRUST-001 · Version 0.7 · 9 August 2026

Document ID	GM-TRUST-001
Version	0.7 - Branded working draft
Owner	GrundMind / Grund Institute
Review status	Prepared from current product implementation and public trust materials; external legal/security assurance not yet completed.

1. Purpose

This document provides a concise enterprise overview of how GrundMind protects participant data, preserves evidence integrity, controls reporting, and constrains the intended use of its AI adoption diagnostic. It is designed as a first-line due-diligence document for prospective customers, security teams, privacy teams and procurement.

2. What GrundMind is

GrundMind is an organisational AI adoption, workflow-improvement, enablement, governance, capability-development and developmental-support platform and advisory service. It collects structured assessment evidence, applies predefined scoring and evidence rules, separates reporting layers, and supports human-reviewed interpretation and client reporting.

CURRENT POSITION	**Human-reviewed advisory system** Core scores and evidence states are determined through predefined rules. AI may assist with draft interpretation, but client-facing narratives require explicit human review and publication.

NOT INTENDED FOR	**Employment decision-making** GrundMind is intended for organisational AI adoption, workflow improvement, enablement, governance, capability development and developmental support. It is not designed or permitted for individual employment decision-making. GrundMind outputs must not be used to make, recommend, rank, score or materially influence decisions concerning an individual's recruitment or hiring, promotion, compensation, performance evaluation, disciplinary action, termination, selection for redundancy or headcount reduction, or allocation of work, tasks, shifts or responsibilities. GrundMind may identify organisational, workflow, capability or structural changes for consideration, but its outputs must not be used to determine which individuals should be selected for employment-related actions. All findings require human interpretation and may be used only within GrundMind's stated organisational and developmental purposes.

3. Trust architecture

Stage	Control objective	Current approach
1. Invitation	Give only the intended participant access	Individual survey links; participant access restricted to the assigned assessment.
2. Assessment	Preserve confidentiality and response durability	Progressive saving, resume support, visible save-failure handling, duplicate-submission protection.
3. Evidence	Preserve integrity and provenance	Exact survey version retained; result layers generated from protected evidence; immutable snapshots used for reporting.
4. Analysis	Avoid invented certainty	Defined evidence thresholds; insufficient evidence is suppressed; missing responses are not treated as zero.

Stage	Control objective	Current approach
5. Interpretation	Keep automation under human control	AI-assisted drafting may be used, but reviewed narrative remains separate until explicitly published.
6. Delivery	Limit exposure of client findings	Controlled report delivery; standard Team and Corporate reporting is aggregated; named Manager Support is tightly restricted.

4. Reporting and privacy boundaries

- Standard Team Results and Corporate Results are aggregated organizational reporting layers.
- Manager and employee evidence remain separate evidence sources and are not averaged together to hide disagreement.
- Named individual Fit scores, named Cognitive Archetypes, raw answers, free-text evidence and employee ranking are not part of standard manager reporting.
- A restricted Manager Support view may identify a person only where operationally necessary to provide support, and is limited to the support need and recommended manager actions.
- Participant, Individual, Team, Manager, Manager–Team Alignment and Corporate reporting layers remain distinct.

5. Current assurance status

Area	Status	Meaning
Swiss FADP / GDPR	Controls implemented; documentation in progress	Privacy and access safeguards are designed with these regimes in mind; deployment-specific legal bases and roles still require engagement-level assessment.
EU AI Act	Internal intended-use position; external review planned	Product is designed around human-reviewed adoption support rather than employment decision-making. No external classification opinion has yet been obtained.
ISO/IEC 27001	Control mapping in progress	Internal security controls are being documented against the standard; GrundMind is not ISO 27001 certified.
ISO/IEC 42001	Framework development	Responsible-AI governance is being formalized; no certification claim.
DPIA support	Prepared - v0.6	Product-level data-flow, risk and safeguard material is available to support customer/controller DPIAs where applicable; customer-specific assessment remains separate.

Area	Status	Meaning
DPA / controller-processor role	Prepared - DPA v0.3 / role paper v0.4	A working DPA template and role analysis are available; engagement-specific schedules and external legal review remain required.
SOC 2	Not claimed	No SOC 2 assurance report is currently claimed.

6. Security controls currently evidenced in the product

- Restricted participant access to assigned assessments.
- Role-based administrative access and restricted raw-answer inspection.
- Organization-scoped application views and database access controls.
- Progressive response saving and secure resume behavior.
- Visible save-failure handling and duplicate final-submission protection.
- Immutable Individual, Team, Manager, Alignment and Corporate result snapshots.
- Defined evidence thresholds and suppression of insufficient-evidence results.
- Human-controlled publication of narrative interpretations.
- Archive/restore lifecycle controls preserving historical evidence while hiding archived entities from normal operations.
- Controlled client report generation and delivery rather than unrestricted customer platform access.

7. Due-diligence material

Document	Status
Trust & Compliance Overview	Prepared - v0.7
Controller / Processor Position Paper	Prepared - v0.4
Technical & Organisational Measures (TOMs)	Prepared - v0.6
DPA template	Prepared - v0.3
DPIA Support Pack	Prepared - v0.6
Data-flow & Architecture Overview	Prepared - v0.5
Subprocessor & Hosting Register	Prepared - v0.1; account-level verification open
Retention & Deletion Standard	Approval draft - v0.1
Responsible AI & Acceptable Use Standard	Prepared - v0.2; public
Incident Response Overview	Prepared - v0.1; first exercise pending
Enterprise Security Questionnaire Answer Bank	Prepared - v0.2; internal

8. Contact

Security and due diligence: security@grundmind.com
General enquiries: info@grundmind.com
Avenue de la Moesette, 1110 Morges, Switzerland

IMPORTANT BOUNDARY

References to GDPR, the Swiss FADP, the EU AI Act, ISO/IEC 27001, ISO/IEC 42001, OWASP or other standards describe intended safeguards, design references or current readiness work. They are not claims of formal certification, legal compliance, regulatory classification or external assurance unless explicitly stated.