TEMPLATE · KASHI LABOR-CONSULTATION PACKET · V1

Labor-Consultation Packet

Pilot-launch document for Kashi 可視 deployments. Prepared for executive sponsor, legal counsel, and worker representative review.

Company: _____ · Pilot start date: _____ · Packet version: v1 · 2026-04-21

> **Purpose of this packet.** Kashi is not deployable as a silent pilot layered underneath ordinary meeting software. Deployment requires the documented alignment of three roles — **executive sponsor**, **legal / compliance reviewer**, and **worker representative**. This packet is the artifact that alignment produces. It serves as the amendment record for 就業規則 (shuugyou kisoku / work-rules revision) filing, the written-opinion anchor for the employee-representative process (per MHLW sample filing 000683138), and the internal governance charter for Kashi usage.

§1 · Purpose statement

Kashi is a privacy-bounded meeting governance system that surfaces repeated interaction asymmetries — under explicit uncertainty — as contestable structural signals for human review. Its purpose in this organization is to:

- Surface repeated meeting-level patterns that would otherwise remain institutionally invisible
- Support early self-correction by managers before patterns harden into late-stage people incidents
- Provide affected individuals with private, observational visibility into patterns that concern them
- Reduce the time that hidden operating loss (presenteeism, regrettable attrition, formal-escalation premium) remains unmanaged

Kashi is **not** a harassment detection system. Kashi does not determine intent, illegality, or individual culpability. Outputs are starting points for human conversations, never substitutes for them.

§2 · Approved uses

1. **Employee self-awareness.** Affected individuals may view their own pattern page privately. No notification to employer.
2. **Manager self-correction.** Managers receive weekly Manager Mirror reports on their own behavior, paired with future-oriented feedforward commitments. Private to the manager.
3. **Aggregated hotspot visibility.** Executives receive per-manager pattern-intensity reports under k≥5 anonymization. No named-subordinate data.
4. **Structured escalation support.** If an affected individual chooses to escalate, Kashi's structural output may support that individual's own case preparation.
5. **Governed remediation (Lane B).** If a pattern persists after the protected self-correction window, it transitions to documented remediation under the organization's agreed process.

§3 · Prohibited uses

The following uses are contractually prohibited AND technically non-exportable from Kashi. No API path, no export format, no workflow allows Kashi output to feed these decisions:

- Performance review or performance-improvement plans
- Promotion, demotion, or internal-transfer decisions
- Discipline, warning, or termination decisions
- Compensation setting, bonus allocation, or ranking
- Redundancy planning or workforce reduction
- Productivity surveillance or time-tracking
- Any employer-visible inference about an individual's mental or emotional state
- Any form of public or semi-public team / manager / employee ranking

Violation of any prohibition constitutes material breach of the service agreement.

§4 · Role access matrix

ROLE	CAN SEE	CANNOT SEE
Individual employee	Full access to their own weekly pattern page, their own trends, their own evidence vault (if enabled), their own audit log showing who drilled into data about them	Any other individual's data. No aggregates.

ROLE	CAN SEE	CANNOT SEE
Manager	Their own Manager Mirror: their own behavioral pattern vs their own baseline. k≥5 anonymized team aggregates if the team size supports it.	**Never:** individual subordinate reports. Never: named-individual pattern data for their own team members.
HR / Compliance	Org-wide aggregates (k≥5). Team-level threshold alerts that trigger human inquiry. Approved case summaries after Lane-B transition.	Raw content. Individual pattern data without documented case justification + employee notice.
Executive (CEO / COO / CFO)	Per-manager pattern intensity (calm / watch / concern). Aggregate modeled impact ranges. No named-subordinate data.	Named subordinate data. Individual meeting content. Any headline company-wide "health score."
Restricted Investigator	Individual data unlocked *only* via a documented case with employee notice per 労働施策総合推進法 duty of care.	Unrelated employee data. Fishing expeditions.
System Admin (customer-side)	Technical settings, tenant flags, role assignments, retention config, audit log access.	Substantive content unless separately authorized under a documented case.
Kashi staff	Technical telemetry, incident investigation data (ciphertext for evidence vault).	**No transcript content. No pattern data. Even with root credentials.** Break-glass procedures require dual approval + audit log entry + customer notification.

§5 · Retention map

DATA CLASS	DEFAULT RETENTION	NECESSITY JUSTIFICATION
Raw transcripts	14 days, isolated storage	Minimum needed for QA on diarization quality + for contestability window. Purged automatically.
Analytics metrics	24 months	Enables detection of year-over-year trends and trajectory-improvement after remediation. Less would undermine longitudinal evidence; more would be disproportionate.
Review-worthy events	12 months	Matches most labor-law statute-of-limitations windows for harassment-related claims in Japan and the EU.

DATA CLASS	DEFAULT RETENTION	NECESSITY JUSTIFICATION
Case / legal hold	Extended, justified	Only when a case is formally open. Case closure triggers review for deletion.
Evidence vault (E2E encrypted)	Controlled by the affected individual	Only the affected individual holds the decryption key. Employer stores ciphertext they cannot read.
Audit telemetry	12–24 months	Sufficient to support challenge workflows and regulatory audit. The affected individual can read their own log.

§6 · Drill-down conditions & audit logging

1. Every non-self-view drill-down writes an audit log entry with *role*, *actor ID*, *timestamp*, *reason code*, *target scope*, and *case ID (if applicable)*.
2. Reason codes are enumerated (not free-form). Examples: `aggregate_review`, `documented_case_investigation`, `audit_verification`.
3. The affected individual may view their own audit log at any time via their self-dashboard.
4. Drill-down into named individual data (reserved for Restricted Investigator role) requires: (a) documented case, (b) prior notice to the affected employee, (c) dual approval from HR lead + legal counsel.
5. Break-glass access (emergency only) requires dual approval + post-hoc case documentation within 48 hours + affected-employee notification.

§7 · Transcript-error & event-review challenge process

1. **Challenge initiation.** Any individual may challenge: (a) transcript accuracy, (b) speaker attribution, (c) context window, (d) the summary, (e) the threshold choice, (f) the review-worthy-event disposition.
2. **Provisional suppression.** Once a challenge is filed, the challenged object is marked *Contested*. Employer-facing surfaces stop showing it until resolved.
3. **Human review.** Challenges are reviewed by a trained reviewer independent of the affected manager. Reviewer must log rationale for decision.
4. **Resolution states.** *Upheld* (reopened) · *Downgraded* (lower evidence grade) · *Withdrawn* (removed) · *Escalated* (to governance process).
5. **Downstream recompute.** If a transcript correction changes an event, all derived aggregates recompute. Old derived outputs are retracted.
6. **Retention under challenge.** The challenged object and its source context are preserved through the challenge resolution, even if routine retention would otherwise delete them.

§8 · Anti-retaliation & no-silent-repurposing

Company commits:

- No employee shall suffer adverse treatment for viewing their own pattern page, enabling the evidence vault, marking a confound, drafting an escalation, or filing a challenge.
- Employer receives no notification of any of those actions. They are architecturally private.
- Kashi will not be repurposed — even silently — for performance, promotion, discipline, compensation, ranking, redundancy planning, or productivity surveillance. Violation voids the service agreement.
- Material change to Kashi's scope, visibility, or retention requires re-consultation with the employee representative **before** the change takes effect.

§9 · Pilot sunset / deletion rules

- This pilot runs for **90 days** from the pilot start date.
- At 90 days, either: (a) the pilot converts to annual contract, (b) the pilot extends by mutual agreement, or (c) the pilot ends.
- If the pilot ends, all tenant data (transcripts, analytics, review-worthy events) is deleted within **30 days**. The affected individual's evidence vault (E2E encrypted) is exported to them in their chosen format before deletion.
- Audit logs are retained for 12 months post-deletion for compliance purposes.
- A public-facing summary of the pilot outcome (aggregate metrics only, no named individuals) may be shared, subject to worker-representative review.

§10 · Signatures

This packet takes effect upon signature by all three parties below.

Executive sponsor

_____

Name · Title · Date

Legal / compliance reviewer

_____

Name · Firm / Internal Counsel · Date

Worker representative (employee-rep per 労働基準法 §90, union delegate, or works-council member)

_____

Name · Role · Date

Kashi (vendor)

_____

Name · Title · Date

This is a template. Adapt sections to reflect your organization's specific roles, policies, and work-rules context. For Japanese deployments, attach this packet to the 就業規則 amendment filing per MHLW sample 000683138. This template is provided under the Kashi service agreement and is not legal advice; have your own counsel review before executing.
