

Works-Council / CSE Documentation Pack — Deltawall

For consultation under BetrVG §87(1)(6) (DE), WOR Art. 27 (NL), CSE information-consultation (FR). Deltawall is designed so that co-determination bodies can approve it without individual-monitoring concerns.

1. What Deltawall is — and is not

Is: a data-loss-prevention control for AI tools. It detects sensitive data (IBANs, citizen IDs, credentials, personal data) in the browser *before* it is sent to an AI service, and redacts or blocks it according to company policy. It records *that* a policy decision happened.

Is not: an employee-monitoring or performance tool. It does not read screens, does not log keystrokes, does not intercept encrypted traffic, does not store what employees write, and produces **no individual productivity metrics, rankings, or scores** — the dashboard aggregates to department level only.

2. Technical safeguards relevant to co-determination

1. **On-device analysis:** prompt/file content is inspected inside the employee's browser and never leaves the device in raw form. The server receives only: data-class label (e.g. "IBAN"), a salted cryptographic hash, timestamp, destination, and the policy outcome.
2. **Pseudonymization by default:** events reference a random subject token. The mapping to a person is stored separately and can only be opened through a **four-eyes procedure** (one authorized requester + one independent approver, typically the DPO), each access itself being logged.
3. **Works-council mode:** at the works council's request, the org-wide switch removes every individual-level view and disables unmasking entirely. This can be made a condition of the works agreement (Betriebsvereinbarung / accord d'entreprise).
4. **Tamper-evident audit:** the record is hash-chained and signed, so neither employer nor vendor can silently alter it — protecting employees as much as the company.

3. Data flows (summary for the agreement annex)

DATA	WHERE PROCESSED	WHERE STORED	RETENTION
Prompt/file content	Employee device only	Never stored	n/a
Data-class labels + hashes	Employee device → EU backend	EU region, encrypted	configurable (default 90 days granular)
Subject identity mapping	EU backend, restricted table	EU region	until employment ends / erasure
Department aggregates	EU backend	EU region	configurable (default 24 months)

4. Suggested works-agreement clauses

- Purpose limitation: use solely for data-leak prevention & compliance evidence; disciplinary use excluded

except where legally mandated and only via the four-eyes procedure with works-council notification.

- Works-council mode: enabled by default / toggle changes require works-council consent.
- Review: joint review of policies and detection classes every 12 months.
- Transparency: employees receive the privacy notice (DPIA Annex B) before rollout.

5. Questions the works council typically asks — with answers

- *Can a manager see what an employee typed?* No. Content is never stored or transmitted.
- *Can a manager see who triggered a block?* Only via the four-eyes unmask with documented reason,

and never in works-council mode.

- *Does it slow employees down?* Redaction happens inline; typical overhead is imperceptible.
- *Can it be used to measure productivity?* No such metric exists in the product, by design.