Data Protection Impact Assessment (DPIA) — Deltawall Deployment

> Template for the deploying organization (the controller). Deltawall GmbH acts as processor. Complete before rollout; review annually and on any material change.

1. Description of the processing

- **Purpose:** Preventing leakage of personal and confidential data into AI tools; producing an

auditable record of AI usage for compliance (GDPR Art. 5(2) accountability, DORA/NIS2 where applicable).

- **Means:** Browser extension performing on-device detection and redaction; opt-in AI gateway for

sanctioned tools; DNS-metadata discovery. **No TLS interception, no raw content storage.**

- **Data processed on-device (transient):** prompt text, attached files — analysed locally, never transmitted.
- **Data transmitted/stored server-side:** data-class labels, salted snippet hashes, timestamps,

pseudonymous subject token, destination service, rule fired, outcome, endpoint id.

- **Special categories:** health-related *labels* may occur (detection class HEALTH); content itself is never stored.

2. Necessity and proportionality

- Legal basis: legitimate interest (Art. 6(1)(f)) — protecting personal data entrusted to the

organization; balancing test documented in Annex A.

- Minimization: pseudonymization by default; department-level aggregation; configurable retention

with aggregate-then-discard; works-council mode removes individual-level processing entirely.

- No automated decision-making with legal effect on employees; **no productivity scoring or ranking.**

3. Risks to data subjects

RISK	LIKELIHOOD	SEVERITY	MITIGATION
Function creep into employee monitoring	Medium	High	Works-council mode; four-eyes unmask; audit of every unmask; contractually bounded purpose
Re-identification from metadata	Low	Medium	Salted hashes; salt deletion on erasure; access control on identity map
Unauthorized access to evidence log	Low	Medium	RBAC, tenant isolation, EU-region hosting, encryption at rest/in transit
Over-blocking impacting work	Medium	Low	WARN/coach actions; justification flow; rule simulator before publish

4. Data subject rights

- **Access/portability:** metadata export per subject via DPO (requires four-eyes unmask).
- **Erasure:** deletion of the subject-identity mapping and snippet salt renders all records

anonymous while preserving evidence-log integrity (EDPB Guidelines 02/2025 alignment).

- **Information:** employee privacy notice template in Annex B; works-council pack provided.

5. Consultation

- □ DPO consulted (date, outcome)
- □ Works council / CSE consulted (date, agreement reference)
- □ Supervisory authority consultation needed? (only if residual risk high)

6. Sign-off

ROLE	NAME	DATE	SIGNATURE
Controller representative			
DPO			
CISO			