

Data Protection Impact Assessment (DPIA) - Template

Customer worksheet for evaluating email and payment-fraud processing. The customer remains responsible for deciding whether Article 35 GDPR requires a DPIA.

DRAFT FOR REVIEW

1. Processing description

Describe selected mailboxes, user groups, surfaces, categories checked, alert recipients, retention, vendor-master use and whether messages can be moved. Hide recommends function mailboxes first and label plus alert as the default response.

2. Purpose and lawful basis

Purpose: reduce payment fraud and support documented verification. Record the customer's Article 6 basis, Section 26 BDSG analysis where employee data is involved, and any works-council agreement. Hide does not decide the customer's legal basis.

3. Necessity and proportionality

- Why current-message checking or selected function-mailbox scanning is necessary.
- Why less intrusive alternatives do not meet the same risk.
- How mailbox scope, alert rules and retention are minimized.
- How employees receive transparent information and can exercise rights.

4. Data flow

Stage	Document
Collection	Selected email fields, body text, links and attachment metadata; invoice fields when present.
Analysis	Deterministic rules and bounded external intelligence; optional model wording under a zero-retention arrangement.
Storage	Verdict and signal record; no raw content by default; 90-day extracted dedupe fields.
Recipients	Authorized workspace members and approved sub-processors only.

5. Risk assessment

Risk	Controls and residual-risk decision
Employee monitoring	Function mailboxes first; no employee productivity metrics; aggregate summaries; works-council review.
Unauthorized workspace access	Exact membership checks, MFA for admins, audit events, domain verification.
Sensitive message exposure	Memory-only processing, content-free logs, least-privilege scopes, short processing window.
False Stop verdict	Conservative rules, concrete reasons, independent verification action, feedback and evaluation gate.
Missed scam	No safe guarantee, evidence limitations, independent verification guidance, incident feedback.
Processor or transfer risk	EU hosting target, sub-processor register, Article 28 terms and Chapter V review.

6. Consultation record

Data protection officer: [name/date/opinion]. Information security: [name/date/opinion]. Works council: [status/date/reference]. Affected-user consultation: [method/outcome]. Legal review: [counsel/date].

7. Decision

Residual risk: [low/medium/high]. Approved scope: [describe]. Required measures before launch: [list]. Review date: [date]. Owner: [name/role]. If high residual risk remains, document prior-consultation analysis under Article 36 GDPR.