

Works Council Agreement - Hide Email Protection Template

Draft Betriebsvereinbarung structure for German customers. It requires review by German employment and data-protection counsel and negotiation with the responsible works council.

DRAFT FOR REVIEW

1. Purpose

Hide supports the detection and verification of suspected phishing, invoice fraud, changed bank details and impersonation. It may not be used to measure employee performance or conduct.

2. Scope

Covered organizational units and function mailboxes: [list]. Personal mailboxes are excluded unless expressly listed after necessity review. Covered surfaces and start date: [list/date].

3. Permitted processing

- Automated checks may evaluate sender routing, domains, links, payment fields and scam-language patterns.
- OK results do not create employee alerts. Caution and Stop results show reasons and one verification action.
- Raw content is not retained by default. Workspace records contain verdict and process evidence.
- Automatic quarantine is off by default and requires a separate documented decision.

4. Prohibited uses

- No ranking, scoring or comparison of employees.
- No statistics on messages read, response speed, mistakes or individual check volume.
- No use for disciplinary measures, attendance monitoring or productivity management.
- No access beyond selected mailboxes and authorized incident records.

5. Access and roles

Mailbox owners see their alerts. Approvers see Stop events and required verification steps. Administrators configure protected mailboxes and suppliers. Access is role-based and logged. [Works council/auditor access arrangement].

6. Alerts and human review

A result is a verification aid, not proof of misconduct or fraud. Payment decisions remain with authorized people. Employees can mark a result legitimate, report an error and request review. No adverse personnel action may rely solely on a Hide result.

7. Transparency and rights

Employees receive the plain-language data flow, selected mailbox list, retention table, contact points and complaint route before activation. GDPR access, correction, restriction, objection and deletion requests follow the customer's established process.

8. Retention

Raw content is discarded after processing. Extracted dedupe fields default to 90 days. Workspace check and audit records default to three years unless the customer selects a shorter lawful period. Logs are content-free and target 14 days.

9. Security and incidents

The customer and Hide maintain least-privilege access, encryption, MFA for administrators, revocable mailbox authorization and documented incident handling. Material incidents affecting employees are communicated under applicable law and this agreement.

10. Oversight and changes

The parties review aggregate false-warning and miss rates without employee-level metrics at least [quarterly]. Material changes to data categories, purposes, recipients, mailbox scope or automated actions require prior works-council involvement.

11. Term and signatures

Effective date: [date]. Termination and after-effects: [terms]. Employer: [name/date/signature]. Works council: [name/date/signature]. Data protection officer consulted: [name/date].