

Human Risk Management(HRM)

PURCHASING TOOLKIT

GDPR & Works Council (Betriebsrat) Consultation Template
For EU HRM Procurement & Deployment Approval



How to Use This Document

This briefing document is designed to support EU-based organizations evaluating or procuring a Human Risk Management (HRM) platform.

It serves as:

- A sample Works Council (Betriebsrat) consultation overview
- A GDPR-aligned privacy briefing template
- A starting point for DPIA preparation
- An internal enablement document for Security, Legal, HR, and Procurement

Organizations may adapt this document to reflect their specific implementation scope, governance model, and regulatory requirements.

Its purpose is to accelerate internal alignment and reduce friction during procurement and approval.

Early alignment with the Works Council and privacy stakeholders significantly reduces procurement delays and accelerates HRM deployment timelines.

Executive Summary

This document outlines how an AI-native Human Risk Management (HRM) platform under consideration can be structured to comply with GDPR requirements and support Works Council (Betriebsrat) consultation. The examples provided reflect a mature AI-native HRM architecture and governance approach, with Living Security used as a practical reference model during procurement and consultation.

An HRM platform under consideration should:

- Process only security-relevant employee data necessary for cybersecurity risk reduction
- Apply Privacy-by-Design principles, including strict data minimization
- Support configurable obfuscation to mask employee identities in reports and dashboards
- Enforce role-based access controls aligned with the principle of least privilege
- Support EU data residency, including hosting in AWS EU-West (Dublin)
- Enable transparent governance and documented approval prior to activation

The objective is to balance measurable cybersecurity risk reduction with strong employee data protection safeguards and Works Council oversight.

INTRODUCTION:

HRM Platforms in the Context of GDPR and Works Council Review

HRM Platforms in the Context of GDPR and Works Council Review

In Germany and other EU jurisdictions, the deployment of systems that process employee-related data may require consultation and formal approval by the Works Council (Betriebsrat).

Human Risk Management (HRM) platforms operate strictly within the domain of cybersecurity risk reduction. While limited employee-related data is processed, the purpose of processing is confined to protecting company systems, data, and business continuity from cyber threats.

This document provides an overview of:

- The purpose and legal basis for processing
- Categories of data processed
- What data is not processed
- How obfuscation protects employee identity
- How role-based access controls limit visibility
- How proportionality and necessity are ensured
- How EU data residency is supported

An HRM platform evaluated for EU deployment should be designed in alignment with:

- Art. 5 GDPR (Purpose Limitation, Data Minimization, Transparency)
- Art. 6(1)(f) GDPR (Legitimate Interest)
- § 26 BDSG (Employee Data Processing)
- Art. 25 GDPR (Privacy by Design and by Default)
- Art. 32 GDPR (Security of Processing)

Purpose of Processing (Zweckbindung)

The sole purpose of an HRM platform evaluated for EU deployment should be to reduce human-driven cybersecurity risk and strengthen organizational information security.

Processing activities are carefully limited to:

- Identifying security-relevant risk patterns
- Delivering targeted security education or interventions
- Providing aggregated reporting on cybersecurity risk trends

An HRM platform evaluated for EU deployment should not be designed or intended for:

- Employee performance monitoring
- Productivity tracking
- Behavioral surveillance outside of cybersecurity context
- Monitoring private communications

Processing must be limited to what is necessary and proportionate to achieve the defined cybersecurity objective in accordance with:

- Art. 5(1)(b) GDPR – Purpose Limitation
- Art. 5(1)(c) GDPR – Data Minimization

Legal Basis

Processing for cybersecurity purposes is typically based on:

- Art. 6(1)(f) GDPR – Legitimate interest in protecting company systems and data against cyber threats
- § 26 BDSG – Processing of employee data for employment-related purposes
- A formal Works Council agreement (Betriebsvereinbarung), where applicable

Processing is proportionate, necessary, and strictly limited to cybersecurity protection purposes.

Categories of Data Processed

Only data necessary for cybersecurity purposes should be processed.

1. Identity Data (Association Layer)

Used exclusively to associate security-related signals with the correct employee profile.

Examples:

- Business email address or username
- Department, role, and location
- Reporting line (manager relationship)
- Employment status

Identity data is sourced from authoritative internal systems (e.g., HRIS or IAM platforms such as Workday, SAP SuccessFactors, Microsoft Entra ID, Okta, SailPoint).

An HRM platform evaluated for deployment should not replicate HR files or function as an HR system.

2. Security-Related Behavioral Data

Examples:

- Phishing simulation participation
- Security training completion
- Security interaction signals (e.g., reporting suspicious emails)

These data points relate exclusively to cybersecurity engagement.

3. Security Event Signals (If Integrated)

Examples:

- Email security alerts
- Endpoint security alerts
- Access anomalies relevant to cybersecurity

An HRM platform deployed for cybersecurity purposes should not process:

- Personal email content
- Private communications
- Productivity metrics
- Non-security behavioral activity

This ensures processing remains strictly within the cybersecurity context.

What “Obfuscation” Means

Obfuscation is a privacy safeguard that masks employee identities in reports and dashboards while preserving cybersecurity risk insights.

A simple way to understand obfuscation:

It functions like a privacy filter, personal details are hidden, but underlying risk trends remain visible and actionable.

For example:

- The system may identify that a department has elevated phishing risk
- It can measure exposure duration and risk movement
- But employee names and identifiable details can be hidden from administrators who do not require access

Obfuscation can be configured based on:

- Geography (e.g., country-specific rules)
- Organizational unit
- Role category
- Defined HR/IAM attributes

When enabled:

- Identifiable employee details are not visible in dashboards
- Administrators cannot access protected personal data within the defined scope
- Risk analytics continue to function using protected data structures

This supports:

- Art. 5(1)(c) GDPR – Data Minimization
- Art. 32 GDPR – Security of Processing
- The principle of least privilege

An HRM platform should be designed to reduce cybersecurity risk without unnecessarily exposing employee identity information.

EU Data Residency

An HRM platform evaluated for EU deployment should support regional data residency.

Data should be capable of being hosted within the European Union.

For example:

- Living Security supports EU hosting in AWS EU-West (Dublin).

This supports alignment with:

- GDPR territorial requirements
- Local governance expectations
- Works Council data localization considerations

Data residency options are defined and documented prior to deployment.

Governance & Approval Process

Implementation follows a structured governance approach:

1. Definition of processing scope and purpose
2. Review of data categories and integrations
3. Configuration of obfuscation and visibility controls
4. Validation with privacy and legal stakeholders
5. Formal approval prior to activation

No integrations proceed without documented agreement on scope and privacy safeguards.

What This Means for Employees

An HRM platform deployed for cybersecurity purposes:

- Does not monitor productivity or general behavior
- Does not access private communications or email content
- Is used strictly for cybersecurity protection purposes
- Applies identity obfuscation and role-based access controls
- Operates under documented governance and Works Council oversight

The system is intended to reduce the likelihood of cybersecurity incidents that could impact employees, customers, and the organization.

It is not intended to evaluate job performance or conduct general behavioral monitoring.

By combining targeted risk reduction with privacy safeguards, the platform supports both security resilience and employee data protection.

Employee Communication & Transparency

Clear communication with employees is an important component of responsible HRM deployment.

Organizations are encouraged to:

- Inform employees of the cybersecurity purpose of the platform.
- Clearly state what data is processed and what is not processed.
- Reinforce that the system is not used for performance monitoring or productivity tracking.
- Explain how obfuscation and role-based access controls protect employee identities.
- Provide contact information for Data Protection or HR representatives for questions.

Transparent communication strengthens trust, reduces resistance, and reinforces that the objective is collective cybersecurity resilience — not employee surveillance.

Next Steps in the Works Council Consultation Process

To support a structured and efficient consultation process, organizations may consider the following steps:

1. Internal Alignment

Review scope of data processing with Security, Legal, HR, and Data Protection stakeholders.

- Confirm legal basis (Art. 6(1)(f) GDPR and § 26 BDSG, where applicable).
- Identify whether a DPIA under Art. 35 GDPR is required.

2. Define Privacy Safeguards

- Document data categories and integration scope.
- Define obfuscation rules and visibility restrictions, if necessary for your organization.
- Confirm EU data residency requirements.

3. Prepare Works Council Briefing

- Share this document (adapted to your environment).
- Clarify that processing is strictly limited to cybersecurity purposes.
- Provide clear examples of what is not monitored.

4. Formalize Governance

- Incorporate requirements into a Works Council agreement (Betriebsvereinbarung), where required.
- Document role-based access controls and approval workflows prior to activation.

Early, transparent engagement significantly reduces approval delays and strengthens trust in the deployment process.

This framework is intended to support transparent consultation, informed Works Council dialogue, and privacy-aligned HRM deployment within the European regulatory environment.

APPENDIX A

Data Protection Impact Assessment (DPIA) Overview

Where required under Art. 35 GDPR, a DPIA may be conducted. Typical DPIA components include:

A1. Description of Processing

- Purpose: Cybersecurity risk reduction
- Data categories: Identity data + security-relevant signals
- Data subjects: Employees

A2. Necessity & Proportionality

- Limited to security context
- No productivity monitoring
- No performance evaluation
- No personal communication content processing
- Obfuscation and RBAC reduce exposure

A3. Risk Assessment

Potential risks considered:

- Unauthorized access to identity data
- Excessive internal visibility
- Misinterpretation as performance monitoring

Mitigation measures:

- Role-based access controls
- Configurable obfuscation
- EU data residency
- Governance approvals
- Principle of least privilege

Residual risk is assessed as proportionate to the legitimate interest in protecting company systems and data.

APPENDIX B

Works Council (Betriebsrat) FAQ

Is this a surveillance system?

No. An HRM platform deployed for cybersecurity purposes should process only security-relevant data and should not monitor productivity or general behavior.

Does it read or store email content?

No. Only security-related metadata or alert signals are processed.

Can managers use it for performance evaluation?

An HRM platform deployed for cybersecurity purposes is designed for cybersecurity risk reduction. Access controls and obfuscation restrict unnecessary visibility.

Can employee identities be protected?

Yes. Obfuscation can be configured based on geography, role, or organizational attributes.

Is EU data stored in the EU?

Yes. Leading HRM platforms support EU data residency, including AWS EU-West (Dublin).

Can access be limited?

Yes. Role-based access controls enforce least privilege and limit exposure of identifiable information.

