Data Protection
Social Dialogue on Artificial Intelligence in the
METAL INDUSTRIES: DATA PROTECTION

1

PURPOSE AND SCOPE

- Guidance for managers, employers and employers' organisations, trade unions and workers' representatives involved in Artificial Intelligence (AI) deployment and data protection in the metal industries.
- Objective: strengthen social dialogue on AI and data protection and translate legal principles into practicable workplace safeguards.
- Focus: lawful, fair and transparent data practices, including worker privacy, monitoring limits, contestability and negotiated governance.

WHY AI INTENSIFIES DATA PROTECTION RISKS?

- **Expands what can be collected, inferred, linked and operationalised in real time.**
- **Normalises data processing as a routine management practice unless constrained by necessity, proportionality and clear legal bases.**
- **Creates power asymmetries through opaque metrics, vendor-controlled systems and continuous updating.**

2

3

CORE SAFEGUARD

- **Worker data should be collected and processed transparently, with workers' knowledge and, where required by law, appropriate authorisation or other lawful bases, in line with data protection law.**
- **Governance implication: information, consultation and negotiation should address, as relevant, data categories, purposes, access rules, retention periods, minimisation requirements and explanation duties.**

CHALLENGES TO DATA PROTECTION: WHAT CHANGES?

- **Generative AI and Large Language Models (deep learning models trained on large volumes of text data to generate and interpret language) process large volumes of worker data (for example email and calendar content) to produce recommendations and evaluations, such as performance evaluation and meeting or training recommendations.**
- **These systems can enable illegitimate surveillance and privacy harms and data protection breaches, including risks to confidentiality and unlawful access.**
- **They may also produce unreliable outputs ("hallucinations"); therefore, reliability, efficacy and safety should be carefully monitored**

4

5

AI MANAGEMENT SYSTEMS: THE CENTRAL WORKPLACE RISK CLUSTER

- **Systems used to hire, train, manage, evaluate, reward or discipline workers, with varying degrees of automation.**
- **Key risks: illegitimate surveillance, work intensification, knowledge imbalances, poor decisions without sufficient oversight and unchallengeable decisions.**
- **High-stakes consequence: operational decisions (including performance management, worker remuneration and hiring and firing) may be influenced without meaningful human oversight, accountability and accessible review mechanisms.**

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only, and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

6

6.1 EXAMPLE 1: ENTERPRISE SOFTWARE INTEGRATED WITH A MONITORING TOOL (SALESFORCE WITH ACTIVTRAK)

- AI-enabled access to employee emails, calendars, performance indicators and workflow data expands surveillance capacity.
- Monitoring tools can generate granular metrics, activity logs, rankings and alerts, enabling continuous behavioural tracking, depending on configuration and governance constraints.
- Governance problem: excessive, unlawful or disproportionate surveillance and increased risk of unauthorised access to personal data.

6.2 EXAMPLE 2: WAREHOUSE MANAGEMENT SYSTEMS (BLUE YONDER AND INFOR)

- Handheld and wearable device metrics decompose work into tasks and quantify performance in detail.
- Scheduling, forecasting and performance scoring can intensify control, pressure and disciplinary capacity.
- Governance problem: autonomy erosion, privacy risk and escalation of managerial control through opaque scoring systems.

GOVERNANCE RESPONSE: SOCIAL DIALOGUE AND COLLECTIVE BARGAINING

- **Collective bargaining is expected to become increasingly central for defining enforceable safeguards against algorithmic monitoring and data misuse.**
- **Workers' representatives prioritise bargaining for rights to challenge technology-assisted decisions and to receive advice from independent external data expertise.**
- **European-level social partners highlight that monitoring and surveillance tools should only be used where necessary and proportionate and privacy must be ensured.**

7

8

INFORMATION AND CONSULTATION AS OPERATIONAL LEVERS

- **Use information and consultation rights to obtain meaningful detail: what data is processed, for what purposes, with which legal basis, who accesses it, for how long, and with what explanation.**
- **Emerging national pathways include strengthening of works council and worker-representative rights to obtain algorithm-related information and to be consulted on deployment, legal rights to algorithm information and strengthened consultation mechanisms.**

NEGOTIATION CHECKLIST BEFORE DEPLOYMENT

- **Before implementing AI tools, employers should clarify and document:**
- **Categories of worker data collected.**
- **Purposes and legal basis for processing.**
- **Retention periods and deletion rules.**
- **Access rights, including third parties (sellers and processors), any cross-border transfers and the purposes of access.**
- **Auditability, explanation duties and escalation pathways.**

9

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only, and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

10

MAIN PRINCIPLE: DATA MINIMISATION

- Apply a minimum data processing rule: collect and process only data that is strictly necessary for a legitimate purpose and proportionate to that purpose.
- Translate into bargaining terms: monitoring limits, purpose limitation, “function-creep” controls (purpose limitation) and, where appropriate, periodic review.

COLLECTIVE AGREEMENTS AS A LEGAL AND PRACTICAL INSTRUMENT

- **Collective agreements can specify safeguards for data processing in employment contexts, including recruitment and management purposes.**
- **Agreements can require transparency on how worker data is used and how systems process data.**
- **Agreements can forbid the most intrusive applications and define enforceable red lines.**

11

12

EUROPEAN METAL INDUSTRIES: JOINT GUIDANCE LOGIC

- **European sectoral partners emphasise that AI is data-intensive and therefore data treatment and protection are central.**
- **Shared principle: data usage must be lawful, fair and transparent, consistent with General Data Protection Regulation principles.**
- **Company-level cooperation in the design and introduction of new systems is presented as critical for successful technological change.**

NATIONAL AND COMPANY EXAMPLES

- **Spain: legal duty to inform workers’ representatives about algorithmic systems affecting decisions and working conditions, including profiling. Illustrative agreements include banning profiling and creating non-monitored communication channels for workers–trade union.**
- **Italy: negotiated provisions reinforcing information rights and maintaining human oversight by limiting automated decision-making.**
- **United States: company agreement commits to notification and negotiation with a trade union when AI deployments may affect workers and provides a channel to contest automated decisions.**

13

14

KEY TAKE-AWAY FOR SOCIAL PARTNERS

- **AI can support productivity and job quality, but only where data processing is constrained by lawful purpose, minimisation, transparency, human oversight and negotiated safeguards enforced through social dialogue.**

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only, and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.