June 2024

Bargaining over Workers' Data Rights

How Unions and Works Councils Can Use Collective Bargaining to Specify Workplace Data Protection Norms

Halefom Abraha

Workers' Rights in the Digital Age

FRIEDRICH EBERT STIFTUNG

WORKERS' RIGHTS IN THE DIGITAL AGE

BARGAINING OVER WORKERS' DATA RIGHTS

How Unions and Works Councils Can Use Collective Bargaining to Specify Workplace Data Protection Norms

Content

EXECUTIVE SUMMARY

Workplace compliance with existing data protection law appears poor. A variety of reasons explain poor compliance, including a lack of legal clarity. Therefore, in order to boost workplace data protection compliance, the norms of the General Data Protection Regulation (GDPR) will need to be specified for the workplace context.

This paper focuses on Art. 88 GDPR, which allows Member States to 'provide for more specific rules' on the processing of employees' personal data in the employment context, in the form of national laws or collective agreements, including 'works agreements' (i. e. firm-level agreements). It identifies where the GDPR requires specification for the workplace and indicates how unions and works councils might go about that. Although the paper can serve as inspiration for the content of national workplace data protection laws, it is written for unions and works councils that negotiate agreements on data protection issues.

The paper provides guidance on several data protection aspects, such as the need for unions and works councils to

- **clarify substantive and procedural requirements**, including the conditions around consent as a legal base for the processing of workers personal data, the restrictions on uses of technology like emotion-detection, and how workers should be involved in data protection impact assessments.

- **specify the scope of individual and collective data rights**, by creating a framework to make sure workers can effectively exercise the right to be informed and to access their personal data, as well as by negotiating additional collective data access, information, and litigation rights that go beyond the GDPR.

- **establish clear norms for algorithmic management**, for instance around the design, deployment and use of algorithmic systems, the degree of transparency (high!), and the importance for unions and works councils to demand the right to audit algorithms and to be involved in decisions throughout the technology-lifecycle.

The accompanying paper ´Improving workplace data protection´ discusses several other underexplored options under the GDPR that can help to specify norms for workplace data protection, like the creation of codes of conduct and certification schemes under Arts. 40 and 42 GDPR.

INTRODUCTION

Workers have specific data protection needs that general data protection rules may not fully address. Recognising this, Article 88 of the GDPR allows Member States and social partners to establish more detailed norms for the workplace. Currently, there is an environment of legal uncertainty due to the lack of action by Member States in utilising Article 88. Nonetheless, social partners should not wait for Member States to act. Article 88 GDPR allows social partners to ensure the protection of worker´s data rights by establishing more specific norms through collective agreements.

As the workplace becomes increasingly digitised, the need for robust collective agreements has never been more pressing. Social partners are ideally positioned to identify the data protection risks faced by workers, evaluate the origin, nature, likelihood and severity of these risks, define specific safeguards, and oversee the proper implementation of existing norms. Therefore, this short paper sets out specific areas of data protection that trade unions and works councils should focus on clarifying in their agreements with employers.

The detailed norms provided by social partners for the workplace do not undermine any more favourable protections offered by Member State laws and the general requirements and principles of the GDPR.

1

SUBSTANTIVE AND PROCEDURAL REQUIREMENTS

1.1 CLARIFYING THE REQUIREMENTS FOR CONSENT

'Consent' within the meaning of the GDPR constitutes an effective legal basis only if it is freely given, specific, informed, and unambiguous. However, regulatory authorities, policymakers, and worker representatives have long deemed it as an inappropriate legal basis for processing employee personal data due to the inherent power and information imbalance between employers and employees.

That means that in employment settings, consent cannot typically be considered 'freely given' within the meaning of the GDPR. The imbalance of power also means that workers may not genuinely have an option to withhold consent without fear of repercussions. Furthermore, the deployment of opaque and sophisticated monitoring and algorithmic management systems further undermines the validity of consent as workers are not in a position to fully comprehend these technologies, the extent and consequences of the data collected, and what they are consenting to, thereby undermining the principle of informed consent.

The GDPR recognises this problem and allows collective agreements, including works agreements, to provide for specific rules on conditions under which personal data in the employment context may be processed on the basis of the consent (Recital 155). This presents an opportunity for trade unions and works councils to negotiate with employers. At the very least, trade unions and works councils should:

i. Encourage the employer to use legal bases other than consent for processing worker data. Appropriate legal bases include necessity for the performance of the employment contract (Art. 6(1(b); compliance with an external legal obligation (Art. 6(1(c); or protection of the vital interests of the worker or another natural person (Art. 6(1(d). The other legal bases (necessity for the public interest, Art. 6(1)(e), and legitimate interest of the employer, Art. 6(1)(f)) may be more legally ambiguous and should therefore ideally be avoided.

ii. Specify the conditions under which consent may be used as a legal basis. For instance, when it offers clear legal or economic advantage to the worker. But trade unions and works councils should also work to identify contexts, purposes, practices, and processing activities where consent is inadmissible, for instance when it is used for the deployment of algorithmic management systems.

iii. When consent is used, trade unions and works councils should ensure the negotiation includes easily accessible opt-out mechanisms, allowing workers to withdraw consent without facing negative consequences.

1.2 RESTRICTING CERTAIN TECHNOLOGIES, PRACTICES, AND PURPOSES

Certain data processing in employment settings poses severe risks to human dignity as well as the legitimate interests and fundamental rights of workers. This is particularly the case when the processing operation goes far beyond what is necessary and proportionate for a clearly defined legitimate interest, or when the processing extends beyond what is necessary for the performance of an employment contract, or when the processing affects existing levels of control, autonomy and trust.

Trade unions and works councils should establish clear prohibitions on potentially harmful monitoring technologies, such as emotion-detection, as well as harmful practices and purposes such as psychological or emotional manipulation.[1] Unions and works councils have a crucial role in identifying the specific conditions under which employee monitoring is acceptable. This negotiation should focus on establishing clear boundaries for monitoring, particularly outside working hours, such as during breaks or off-duty periods. This is crucial due to the increasingly blurred lines between professional and private life. An essential aspect of these negotia-

1 Note that the EU 'Platform Work Directive', adopted by the European Parliament on 24 April 2024, and pending approval of the Council of the EU and publication in the Official Journal of the EU, will prohibit processing by digital labour platforms of any personal data on the emotional or psychological state of platform workers; any personal data in relation to private conversations, including especially in relation to communications with worker representatives; and any collection of worker personal data outside of working time (Art. 7(1)(a–c)). See further Adams-Prassl et al. 2023 ('Regulating algorithmic management: a blueprint,' European Labour Law Journal, 2023), pp. 128–131.

tions should prohibit monitoring practices that infringe on the private life of workers. This includes the surveillance of personal communications unrelated to the worker's essential tasks and conversations with union representatives. Continuous monitoring should be prohibited unless it is strictly necessary for health, safety, security or the protection of property.

Furthermore, it is vital to ensure that monitoring does not extend to observing workers' behaviours with the intent to predict, identify, profile, interfere, restrain, or coerce them in exercising their legal rights. These rights encompass, but are not limited to, the freedom to organise and engage in collective bargaining through representatives chosen by the employees themselves. Establishing prohibitions on these types of monitoring practices is necessary to safeguard the dignity and rights of workers, maintaining a fair and respectful workplace.

1.3 ESTABLISHING A FAIR BALANCE BETWEEN WORKER'S AND EMPLOYER'S INTERESTS

The most challenging aspect of data processing in the employment context is striking a fair balance between employers' legitimate interests and workers' specific rights to dignity, privacy, and other fundamental rights. The question of proportionality arises specifically when employee data processing goes beyond what is strictly required within the contractual employment relationship. Any processing of employee data that is not intrinsically connected and strictly necessary for the performance of the contract must be carried out after a balancing of interests. This includes interpreting the limits of an employer's 'legitimate interest', which is often used as a primary legal basis to deploy automated monitoring and decision-making technologies in the workplace.

Unfortunately, existing laws do not offer clear frameworks for conducting such a balancing exercise. What constitutes legitimate interest remains uncertain, context-dependent, and prone to abuse. It changes over time, in different contexts, and across business models. Employers can easily argue that any form of monitoring and surveillance in the workplace is proportionate and necessary for the business interests and purposes they define themselves, including improving productivity, efficiency, and innovation.

In 2023, for example, an administrative court in Germany ruled that constant electronic surveillance of individual workers' activities was lawful — despite the regional data protection authority's assessment that it was not — because the employer had a legitimate business interest in the collection and processing of these data, both for the real-time organisation of work and for personnel management decisions such as training, feedback, and performance evaluation (see further Abraha 2023; Verwaltungsgericht Hannover 2023). The data protection authority remains of the view that their original assessment was correct (Landesdatenschutzbeauftragte Niedersachsen 2023), and has appealed the decision. While most data protection experts would likely agree with the data protection authority in this case, it must at the same time be admitted that the GDPR itself does not clearly define important terms such as 'legitimate interests,' or how such interests, even if 'legitimate,' are to be balanced against data subjects' rights and interests in the protection of their personal data, including fundamental data protection principles such as data minimisation.

Trade unions and works councils should therefore engage with employers through proactive dialogue and negotiation to establish a clear framework for fairly balancing interests of workers and employers, including creating a transparent and mutual understanding of what constitutes 'legitimate interest' and how it aligns with the protection of workers' data rights.

Trade unions and works councils are well positioned to provide tailored solutions that reflect the unique needs of different workplaces or sectors. These norms can go beyond the minimum standards set by the GDPR, offering enhanced protections where necessary. They can delineate the contexts, purposes, practices, and processing activities that should be off-limits, including the continuous or permanent monitoring of workers' behaviour. They can also identify the circumstances and processing operations in which 'legitimate interest' cannot be invoked as a valid legal ground.

1.4 CLARIFYING HOW THE EMPLOYER AND THE WORKS COUNCIL WILL SUPPORT EACH OTHER'S COMPLIANCE WITH DATA PROTECTION OBLIGATIONS

Worker representative bodies, including trade unions and works councils, process the personal data of workers, potentially including sensitive personal data as defined in Article 9 GDPR. Trade unions are independent legal entities and therefore their processing of workers' personal data can be regulated normally under the GDPR. That is, trade unions are 'normal' data controllers and must fulfil the same obligations as all other controllers.

Works councils, however, may be in a more complex legal situation, as they are typically not independent legal entities, but rather part of the employer organisation. However, the works council may have access to workers' personal data that 'the employer' does not (and should not) have access to, and the works council may have interests and aims that differ from those of the employer. Nonetheless it appears that the works council is still considered 'part of' the employer for the purposes of compliance with data protection law.

This may create an unclear legal situation that raises a variety of questions. For example, if the works council requests information from the employer in exercising its information and consultation rights, to what extent can the employer rely on its obligations under data protection law to refuse such requests? More broadly, how does the employer go

about handling such requests? If the works council, for example, requests from the employer personal data about workers, but those workers refuse to give their consent for the works council to receive or process that data, can the works council rely on other legal bases such as legitimate interests? On a different topic, to what extent is the employer obligated to finance technical infrastructure and operational expertise to ensure that personal data processed by the works council is processed securely, and that the works council can promptly and satisfactorily fulfil its obligations to individual workers regarding their data protection rights (e. g., rights of access, right to rectification, etc.) – even when the employer is not entitled to access that data?

Preliminary examination of 'grey literature' in selected Member States indicates that the legal framework surrounding these issues is only just beginning to be developed, and many questions remain without clear or satisfactory answers. In the meantime, works councils and trade unions may wish to consider at least attempting to clarify in plant-, firm- or sector-level collective agreements some issues relating to the works council's processing of workers' personal data, such as:

i. A joint understanding of the works council's data protection obligations under nationally applicable labour law.

ii. A common understanding that even if the works council is part of the employer (i. e., not an independent 'controller') for purposes of data protection law, the works council may collect, store, and process personal data to which the employer does not, and should not, have access.

iii. A joint understanding that despite (ii), it is in the interest of the employer to support the works council, especially through access to technical infrastructure and expertise, in ensuring that it has the capacity to process the personal data that it processes in compliance with data protection law; e. g., to ensure that the data are stored securely and deleted when no longer needed, and that workers can exercise their data protection rights with respect to the works council's processing of their personal data

iv. Specify concrete resources to be provided relating to (iii); e. g., specific technical resources and personnel that will be made available to ensure the works council is able to comply with its data protection obligations.

1.5 GETTING INVOLVED IN DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

The GDPR requires employers to conduct an ex-ante DPIA where data processing activities are likely to pose a high risk to workers' rights and freedoms (Art. 35). The introduction of new technology in the workplace, in particular, is identified as likely to entail such a risk. The GDPR outlines the components of a typical DPIA, including a systematic description of the envisaged processing, assessments of the necessity and proportionality, risks to the rights and freedoms of workers, and measures to address the risks. While the GDPR does not precisely define the 'high-risk' threshold, Article 35(3) provides a non-exhaustive list of relevant processing activities, such as automated decision-making. European guidelines on DPIA also classify 'employee monitoring' as high-risk, citing vulnerable data subjects (Recital 75), and systematic monitoring (Article 53). Consequently, many supervisory authorities have listed 'employment monitoring' as an operation always requiring a DPIA.

However, the effectiveness of a DPIA depends significantly on workers' or their representatives' involvement in the process and proper consideration of their views. In countries like Germany, labour laws make works council involvement mandatory, but this is not the case in other Member States. Notably, the GDPR requires employers to seek workers' or their representatives' views 'where appropriate' (Article 35(9) GDPR), a term that employers themselves interpret, potentially limiting worker participation.

Therefore, trade unions and works councils should advocate for consistent involvement in the DPIA process, in line with Article 35(9) of GDPR. This provision should be interpreted strictly, making worker or representative involvement mandatory. Trade unions and works councils must assert this right, placing the onus on the employer to justify any lack of consultation during DPIA. Moreover, they should identify potential 'high-risk' data processing scenarios and ensure adequate technical and organisational measures are in place to mitigate these risks. This responsibility is crucial as Art 35(1) indicates that the 'context and purposes' of processing are relevant factors in risk assessment. Finally, trade unions and works councils must ensure that DPIAs are regularly reviewed, particularly when changes in the processing operations alter the risk landscape.

2

THE SCOPE OF INDIVIDUAL AND COLLECTIVE DATA RIGHTS

2.1 SPELLING OUT THE RIGHT TO BE INFORMED IN CONCRETE TERMS

The principle of transparency is a fundamental prerequisite for ensuring accountability and the exercise of workers' data rights. Article 88(2) of the GDPR explicitly stipulates that specific rules set forth through collective agreements should pay particular attention to the transparency of data processing. The GDPR also prescribes what information should be provided to workers, how it should be communicated, and the timing of such communication in relation to their personal data processing. Trade unions and works councils could play a crucial role in how 'the right to be informed' is implemented and enforced through collective agreements without prejudice to more favourable rules provided by domestic law. In this context, the right to be informed should cover at least the following aspects:

i. **Timeframe:** Workers should be informed about data processing practices at three stages of the employment relationship: at the job application stage, once the employment contract is offered, and during the employment relationship. The GDPR sets specific timelines for these notifications depending on the data's origin and processing purpose. If personal data is gathered directly from the worker, they must be informed at the beginning of the processing cycle. Alternatively, if the data is acquired from other sources, information must be provided 'within a reasonable period after obtaining the personal data, but at the latest within one month'. For any 'further processing' for different purposes other than originally collected, workers must be informed before the new processing begins.

   Trade unions and works councils should provide guidance on how these requirements are to be implemented. Additionally, they should ensure workers are fully informed about any new monitoring and decision-making technologies before their introduction in the workplace.

ii. **Categories of personal data and a description of the processing purposes:** The GDPR lists extensive categories of information that should be provided to workers (Articles 13 and 14 GDPR). This requirement applies whether the personal data is collected directly from the worker or from other sources. According to Art 13 (2(f) and Art 14 (2(g) of the GDPR, the categories of personal data that should be provided to the worker include: (1) the existence of automated decision-making; (2) meaningful information about the logic involved; and (3) the significance and the envisaged consequences of the processing for the worker. Although the mere provision of information about the existence of solely automated decision-making is straightforward, the other aspects remain controversial and lead to uncertainties in practice (see Custers and Heijne, 2022). The GDPR does not define what constitutes 'meaningful information about the logic involved', although the existing literature suggests that it should be interpreted in line with the underlying aim of the right to be informed, and the principle of transparency. In this regard, information that is too generic or too detailed may not contribute to achieving these objectives and thus fail to meet the criterion of meaningfulness. For instance, a technical and complex description of the algorithmic management system or merely mentioning that an automated decision-making system is being used cannot be considered meaningful. Therefore, unions and works councils could play a role in clarifying and expanding these requirements in the employment context.[2]

iii. **Modality of providing information to individual workers:** The GDPR stipulates that information must be presented to workers in a manner that is concise, transparent, intelligible and in an easily accessible form, using clear and plain language - but employers, and controllers generally, do not always comply with data subject access requests in ways that meet these requirements. Researchers working with Uber drivers, for example, reported that the company responded to drivers' requests for their personal data by providing each driver with 26 separate 'raw data' files (Stein et al. 2023) - an unusable, overwhelming 'mountain' of data most workers probably cannot make sense of. Additionally, information should be made readily available through the information systems normally used by the employ-

2 For details on how these requirements can be expanded, see Adams-Prassl et al. 2023 ('Regulating algorithmic management: a blueprint,' European Labour Law Journal, 2023), Policy Option 3.

ees. The specific implementation of these requirements will vary depending on the data processing circumstances. While the GDPR does not require a specific modality, it does require employers to 'take appropriate measures' that suit their data processing practices. Trade unions and works councils should take a leading role in defining how these requirements can be practically applied.

iv. **Means for workers to exercise their data rights:** Simply providing information about data processing does not fully comply with the GDPR's fairness and transparency standards, nor does it effectively enable workers to exercise their rights. In addition to providing specific information in the specified modalities and time, the employer has a positive obligation to facilitate the exercise of workers' data rights. For this reason, the employer must provide workers with the summary of the data rights they have, and the steps workers can take to exercise each right. This summary of rights should be presented separated from the categories of information highlighted above. For instance, the employer should explicitly bring to the attention of each worker that they have the right to object at any time to processing of their personal data. However, this information is not sufficient in itself. The employer should also inform each worker about the mechanisms for them to exercise this right. Trade unions and works councils should play a crucial role in identifying specific workers' data rights stipulated in the GDPR and in collective agreements and ensure that these rights and they ways of exercising them are explicitly communicated to each worker.

2.2 SPECIFYING THE RIGHT OF ACCESS TO PERSONAL DATA

Right of access (Art. 15 GDPR) enables workers to request and receive a copy of the personal data about them that the employer keeps. The purpose of this right is to increase transparency and allow employees to understand how and why their data is being used, thereby enabling them to verify the lawfulness of the processing. However, this right comes with certain limitations and could be used by employers as pretext to withhold information from workers. For instance, the right of access may be restricted to protect the rights and freedoms of others. The employer may also use intellectual property or trade secret exceptions to limit or refuse the right of access by workers. This is particularly challenging as data produced by workers as part of their work could be embedded with business-related information, triggering corporate interest and trade secret claims. To improve legal certainty and ensure that these exemptions are not - intentionally or even accidentally - misused by employers, unions and works councils can set out in collective agreements specific categories of information that are and are not to be considered 'protected.' Collective agreements can also set out procedures, such as redaction of sensitive individual words, that the employer can use to protect sensitive information while still fulfilling workers' rights to access their personal data. Additionally, the employer may reject or limit the right of access under the 'excessive request' exception.

Recital 63 GDPR indicates that employers can ask workers to specify the data they wish to receive or the processing activities about which they wish to be informed. This requirement could significantly affect the right of access because the requirement assumes that workers know all the categories of personal data collected by their employers and processing activities, which is not usually the case in practice. Trade unions and works councils could play a crucial role in ensuring the effective implementation of the right of access. Trade unions and works councils can and should negotiate collective agreements that provide more favourable conditions for access to personal data. They should also work towards establishing clear procedures and policies in the workplace regarding data access requests, thus ensuring that these requests are handled efficiently and in compliance with the GDPR.

2.3 BARGAINING FOR COLLECTIVE DATA ACCESS AND INFORMATION RIGHTS

One of the core tasks of worker representative bodies is to counterbalance employers' prerogatives and address collective risks and harms through social dialogue. However, the focus of data protection laws like the GDPR on individual rights limits the role these bodies could play in addressing these issues at a collective level. While the protections under the GDPR and Member State laws are crucial, they are not sufficient against the collective risks posed by new technologies and processing activities. Therefore, trade unions and works councils must negotiate for new collective data rights and expand protections provided by national laws and practices, including co-determination rights. At the very least, they should address the following:

i. **Establish a collective right to be informed:** Extending the GDPR's right to be informed about data processing to worker representative bodies acknowledges the collective nature of the workplace and the shared impact of data processing practices. This ensures that workers are collectively informed about how their data is collected and used, which is particularly relevant in the context of using new technologies where individual understanding is often limited. Trade unions and works councils could use the GDPR language (Art. 12–15) to further specify what information should be provided to worker representatives, how it should be communicated, and the timing of such communication.

ii. **Establish collective data access rights:** Direct access to workplace data is crucial for worker representatives to perform their 'protective' functions effectively. By leveraging collective access rights, they can counterbalance information and power asymmetry in the

workplace, exercise other collective rights, and voice their collective concerns. This right could also serve as organising and power-building tools for worker representative bodies. While the GDPR covers the content, timing and modalities of notifying workers, trade unions and works councils should further clarify and specify how these requirements are to be implemented collectively, especially in the context of algorithmic management. The corresponding rights of access and notification in the context of algorithmic management are explained below.

iii. **Establish a right to collective litigation and complaints:** Negotiate the rights for worker representatives to initiate collective litigation or file with data protection authorities on behalf of workers groups (Art 80) GDPR). This approach addresses systemic problems at the system level, rather than leaving it to individual workers to handle them.

iv. **Balance collective and individual rights:** While collective access and information rights are essential for monitoring compliance with labour law, data protection laws and agreements, it is crucial to ensure these collective rights do not infringe upon individual workers' data rights. Therefore, personal data of workers should be shared with trade unions and works councils only as much as is required for the fulfilment and supervision of obligations laid down in national or collective agreements.

3

NORMS FOR ALGORITHMIC MANAGEMENT

While algorithmic management warrants its own separate regulation, trade unions and works councils must prioritise the data protection aspects using of such technology in the employment context. Trade unions and works councils should negotiate clear terms addressing at least the following key aspects of algorithmic management:

i. **Involvement of workers:** Workers or their representatives should be actively involved in all stages of algorithmic management systems, from procurement, configuration, deployment to evolution and impact assessment.

ii. **Transparency in design and implementation:** Trade unions and works councils should negotiate to gain a comprehensive understanding of the architecture and operational mechanisms of these systems. This encompasses knowing the algorithms' scientific basis or 'logic,' data inputs, decision-making processes, and how they are applied in various workplace scenarios. As indicated in (i), they should ensure that the design process is transparent, involving worker representation wherever possible. Understanding how these systems function, change, and affect workers is key to safeguarding employee rights and interests. This includes insight into data collection, analysis methods, and the criteria for making employment-related decisions. By doing this, trade unions and works councils can effectively monitor and influence the ethical use of technology in the workplace, ensuring it aligns with worker welfare and regulatory standards.

iii. **Ethical use of AI systems:** There should be transparent and fair norms for using algorithmic management systems in various HR processes like hiring, matching, assigning tasks, performance evaluation (such as promotion and discipline), monitoring and other personnel decisions. Prohibitions should be set against using these systems for punitive or manipulative purposes, including for making predictions about a worker's behaviour that are unrelated to the worker's essential job functions; monitoring workers' emotions, personality, or other types of sentiments; and identifying, profiling, or predicting the likelihood of workers exercising their legal rights. Additionally, prohibitions should be set against using fully automated decision-making for dismissal.

iv. **Algorithm Audit:** Trade unions and works councils must advocate for the right to audit algorithms used in the workplace to ensure they comply with legal and ethical standards.

v. **Mitigating Occupational Health and Safety Risks:** Clear terms should be negotiated to address OSH risks, including psychosocial risks, such as discrimination, deskilling, work intensification or acceleration, privacy harms, and inappropriately competitive or even toxic workplace culture, arising from algorithmic management (for more on this, see Cefaliello et al. 2023; Faragher 2019; Staab and Geschke 2019).

vi. **Expanding Platform Work Directive Protections:** The Platform Work Directive can guide trade unions and works councils in applying Art. 22 GDPR protections to the employment context. This Directive enhances legal clarity on automated decision-making systems, addressing both fully automated and semi-automated processes. It elaborates on the GDPR's transparency requirements (Articles 13(2)(f), 14(2)(g) and 15(1)(h), requiring employers to make algorithms understandable to workers, their representatives, and labour authorities. Additionally, it forbids processing personal data unrelated to job performance and any data on workers' emotional or psychological states. The Directive requires impact assessment of these systems and guarantees the right to explanations and reviews of significant decisions. Trade union and works councils should advocate to expand these protections across all employment settings, ensuring uniformity in protecting workers' dignity, interests and rights, irrespective of the employment relationship's legal nature.

vii. **Clarifying protections against automated decision-making:** Guidelines should be established to define what constitutes significant automated decision-making within the meaning of the GDPR. Trade unions and works councils should provide clear guidance on how Art. 22 GPDR protections, including the right to obtain human intervention, the right to express one's point of view, the right to contest the decision, and the right to obtain an explanation of the decision reached should be interpreted in the employ-

ment context. For instance, the required degree of explicability is dependent on the context, severity and consequences and trade unions and works councils are well positioned to provide tailored understanding of these situations.

4

ENFORCEMENT CONSIDERATIONS

The GDPR faces an enforcement challenge, especially in the employment context, where data protection authorities often lack sufficient resources and expertise to effectively enforce workplace data protection rules. This issue is more pronounced in cases involving automated monitoring and decision-making which intersect with data protection, labour and social protection laws.

To enhance enforcement effectiveness in this area, trade unions and works councils should advocate for the establishment of collaborative enforcement mechanisms among various regulatory bodies. The Platform Work Directive supports this approach, envisioning a collaborative regulatory framework. It allocates responsibilities between DPAs and labour authorities, stipulating the exchange of relevant information related to their respective regulatory roles. In this process, the inclusion of trade unions and works councils is crucial.

Additionally, it is important that trade unions and works councils actively participate in enforcing workplace data protection rules. Such involvement would strengthen the legal position of trade unions and works councils in enforcement matters.

REFERENCES

Abraha, Halefom (October 8, 2023).Automated Monitoring in the Workplace and the Search for a New Legal Framework: Lessons from Germany and Beyond Available at SSRN: https://ssrn.com/abstract=4595760.

Adams-Prassl, Jeremias and others (2023). 'Regulating Algorithmic Management: A Blueprint' 14 European Labour Law Journal 124.

Custers, Bart and Heijne, Anne-Sophie (2022). 'The Right of Access in Automated Decision-Making: The Scope of Article 15(1)(h) GDPR in Theory and Practice' 46 Computer Law & Security Review 105727.

Hießl, Christina (2023). 'Jurisprudence of National Courts in Europe on Algorithmic Management at the Workplace' (European Centre of Expertise in the field of labour law, employment and labour market policies (ECE).

Bagdi, Katalin (2019). The works council as an independent data controller (in Hungarian). Proceedings of the XVI Debrecen Legal Workshop, 2019. https://doi.org/10.24169/DJM/2019/1-2/1.

Cefaliello et al. (2023). 'Making algorithmic management safe and healthy for workers: addressing psychosocial risks in new legal provisions,' European Labour Law Journal, 2023, esp. pp. 197–200.

Faragher, Jo (2019). 'Zalando accused of misusing software to rank workers' (Personnel Today 2019). https://www.personneltoday.com/hr/zalando-accused-of-misusing-software-to-rank-workers/.

Groß, Torsten (2019). Germany: Works Council's Right To Information In Relation To Sensitive Personal Employee Data. Mondaq, 10 Sep 2019. https://www.mondaq.com/germany/data-protection/843698/works-councils-right-to-information-in-relation-to-sensitive-personal-employee-data.

Lamken, Tessa (2022). Works council as data protection law controller? Externer Datenschutzbeauftragter Dresden, 19 Jun 2022. https://externer-datenschutzbeauftragter-dresden.de/en/data-protection/works-council-as-responsible-in-data-protection-law.

Landesdatenschutzbeauftragte Niedersachsen (2023). Thiel: Das "allgemeine Persönlichkeitsrecht der Mitarbeiterinnen und Mitarbeiter überwiegt unternehmerische Interessen". https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/thiel-das-allgemeine-persoenlichkeitsrecht-der-mitarbeiterinnen-und-mitarbeiter-uberwiegt-unternehmerische-interessen-219596.html.

Staab and Geschke (2019). 'Ratings als arbeitspolitisches Konfliktfeld: das Beispiel ZONAR' (Hans-Böckler-Stiftung 2019). https://www.boeckler.de/de/boeckler-impuls-zalando-beschaeftigte-im-bewertungsstress-18789.htm.

Stein et al. (2023). ''You are you and the app. There's nobody else.': Building Worker-Designed Data Institutions within Platform Hegemony' (CHI '23: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems April 2023). https://doi.org/10.1145/3544548.3581114.

Stepanova, Olga (2022). Works councils and data protection: a complex relationship in Germany. LinkedIn Pulse, 6 Nov 2022. https://www.linkedin.com/pulse/works-councils-data-protection-complex-relationship-olga-stepanova.

Stogov, Christina (2022). The new Section § 79a of the Works Council Constitution Act (BetrVG): Support obligations of the works council in complying with data protection regulations. Vangard News & Analysis (blog), Apr 2022. https://vangard.de/en/news-analysis/blog/the-new-79a-betrvg-support-obligations-of-the-works-council.

Verwaltungsgericht Hannover (2023). Datenerhebung bei Amazon in Winsen ist rechtmäßig. https://www.verwaltungsgericht-hannover.niedersachsen.de/aktuelles/pressemitteilungen/datenerhebung-bei-amazon-in-winsen-ist-rechtmassig-219664.html.

ABOUT THE AUTHOR

Halefom H. Abraha is an Assistant Professor at the International and European Law (IER) Department of the Utrecht School of Law. His research and teaching interests lie in AI Regulation, algorithmic management in the labour market, and data protection. He also researches cross-border data access in the law enforcement context and digital sovereignty. Dr. Abraha completed his postdoctoral research at the Bonavero Institute of Human Rights, University of Oxford. He has advised governments and international organisations such as the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) on multiple areas of digital technology and public policy.

Acknowledgement
Thanks to Dr Michael 'Six' Silberman for helping me write this paper. Additional support for the preparation of this paper was provided by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement no. 947806).

IMPRINT

Published by: Friedrich-Ebert-Stiftung |
Competence Centre on the Future of Work |
Cours Saint Michel 30e | 1040 Brussels | Belgium

Dr. Tobias Mörschel, Head of Friedrich-Ebert-Stiftung
Competence Centre on the Future of Work

Responsible/Contact: Justin Nogarede
justin.nogarede@fes.de

For more information about the Competence Centre on the Future of Work, see:
https://futureofwork.fes.de/

Design/Typesetting: pertext, Berlin | www.pertext.de

ISBN 978-3-98628-495-4