June 2024

Improving Workplace Data Protection

Achieving Workplace GDPR Compliance, Clarifying National Workplace Data Protection Rules, and Enhancing Worker Data Protection through Social Dialogue

Justin Nogarede, Michael 'Six' Silberman, and Joanna Bronowicka

Workers' Rights in the Digital Age

FRIEDRICH EBERT STIFTUNG

WORKERS' RIGHTS IN THE DIGITAL AGE

IMPROVING WORKPLACE DATA PROTECTION

Achieving Workplace GDPR Compliance, Clarifying National Workplace Data Protection Rules, and Enhancing Worker Data Protection through Social Dialogue

Content

EXECUTIVE SUMMARY

Workplace compliance with existing data protection law appears poor. A variety of reasons explain poor compliance, including lack of legal clarity and under-resourcing of worker organisations (e. g., unions), data protection officers, and data protection authorities.

This paper explores what social partners, governments and civil society organisations can do to improve data protection compliance at work, across the following major themes:

1. Existing data protection law provides a range of options for social partners and national governments that have thus far not been fully explored. These options, such as codes of conduct and certification schemes under Arts. 40 and 42 GDPR, could clarify matters that are as yet not fully clear in data protection law, and could improve compliance and reduce the enforcement burden on data protection authorities.

2. Member States should make use of Article 88 GDPR to enact national workplace data protection rules – and social partners and civil society organisations should encourage them to do so. Recent legal developments at EU level have clarified the requirements on national Article 88 laws. This creates an opportunity for Member States to improve legal clarity around application of existing data protection rules to the work context, provide additional substantive protections, and improve compliance and enforcement.

3. Technical experts can assist unions and data protection authorities in auditing algorithmic systems. The complexity and opacity of work-related data processing systems and practices has created a need for technical insight and expertise in assessing whether those systems and practices comply with applicable law.

4. Strategic litigation can help address legal uncertainties and provide financial deterrents against non-compliance. Such litigation has proved fruitful in the area of consumer data processing; its potential should be assessed in the area of work-related data processing as well.

This paper elaborates on these themes, providing specific examples and references to relevant literature where appropriate.

INTRODUCTION

On 19 October 2023, the Friedrich-Ebert-Stiftung (FES) Competence Centre on the Future of Work convened an expert workshop in Brussels to discuss the state of data protection compliance and enforcement at the workplace. Policymakers including regional and national data protection officials and European Commission officials attended, as did practitioners including trade union officials and technical experts from civil society organisations as well as academics actively involved in policy research in this area.

The discussion was oriented toward FES Future of Work's overall assignment to consider how to bring about a European economy with decent work, equal opportunity and social protection for all in the context of rapid proliferation of digital technologies in the world of work. While sophisticated digital technologies can enhance productivity and European competitiveness, they must be molded by social dialogue and guided by regulatory frameworks to ensure that the digital transformation supports and reinforces, rather than corrodes, the European commitment to social partnership and fundamental human rights.

Data protection law in particular has a significant role to play in guiding the digital transformation, including at the workplace. The sheer quantity of complaints lodged with data protection authorities (DPAs) has created significant enforcement challenges, however. These are acknowledged by DPAs, by the European Data Protection Board, and by the European legislator; indeed, on 7 April 2023 the Commission proposed a new Regulation to address enforcement challenges specifically arising in transnational cases (the proposed 'Regulation laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679').

The technical and organisational complexity of workplace data processing, however, has posed particular challenges not just for DPAs, but also for social partners, such as trade unions attempting to encourage and ensure employer compliance with data protection rules. Indeed, this complexity, combined with legal uncertainty regarding certain key terms and concepts in existing data protection law – such as the boundaries of data controllers' 'legitimate interests' and the exact conditions for data subjects' consent to be 'truly' 'given freely' – create challenges even for employers who *want* to comply.

Researchers, data protection authorities, and social partners have been calling for years for national workplace data protection laws to address some of these issues, but thus far no Member State legislation has addressed them fully. This workshop was convened with a view to discussing the state of progress on these difficult challenges and clarifying steps that could be taken to address them by social partners, civil society actors, Member States, and EU institutions.

In early 2024 the EU approved the Platform Work Directive and the AI Act, both of which are relevant for data processing in the workplace. At the time of the workshop, however, these laws were still the subject of intense negotiations, and their benefits and shortcomings will only become fully visible in the coming years. Therefore, this paper focuses on the (lack of) compliance with the General Data Protection Regulation: a horizontal law that governs the processing of personal data of all EU workers regardless of their contractual status, that has been implemented by the Member States, and which has now been in force for almost six years.

Five main themes emerged from the discussion:

1. **Workplace compliance with existing data protection law appears poor**, and workshop participants were not aware of any signs or indications that it is likely to improve any time soon.

2. **Existing data protection law provides a range of options for social partners and national governments that have thus far not been fully explored.** Beyond Article 88, which offers Member States the option to lay down nationally-specific workplace data protection rules, the GDPR also empowers controllers and other parties to establish voluntary codes of conduct (Article 40) and certification schemes (Article 42). While voluntary systems cannot substitute for mandatory laws that are adequately enforced, possibilities to use these to address legal uncertainties and improve compliance among 'well-meaning' controllers should be explored. Beyond voluntary schemes, Article 80(2) GDPR allows Member States to empower civil society organisations to lodge data protection complaints without an individual mandate ('own-initiative' complaints), but few Member States have done so.

3. **Member States should make use of Article 88 GDPR to enact national workplace data protection rules – and social partners and civil society organisations should encourage them to do so.** Recent legal developments at European level have clarified the requirements for such 'Article 88' laws. These requirements are stringent, and Member States must pay careful attention to them, or risk seeing their laws becoming invalidated later. Additionally, recent scholarly research and civil society proposals have clarified desirable content for such laws.

   In theory, an EU Directive could provide a transnational 'framework' for workplace data protection. This could be desirable, as it could reduce the risk of fragmentation arising from significantly diverging national rules. The political prospects for such a Directive are uncertain, however. As a result, most workshop participants placed more priority on establishing national rules.

4. **Technical experts can assist unions and data protection authorities in auditing algorithmic systems.** Such audits are possible even when platforms are not willing or able to provide transparency about the way workers' data is collected or processed and can potentially reveal a lack of compliance with GDPR rules. Technical experts are exploring different methods that can reveal GDPR violations, including analysing data received from companies through individual requests, deploying data-scraping methods, or 'black-box' analysis.

5. **Strategic litigation can help address legal uncertainties and provide financial deterrents against non-compliance.** The model for this is the work undertaken with respect to consumer data protection by Max Schrems and his 'NOYB' organisation. A similar organisation could be set up to support legal initiatives focusing on *workplace* data protection.

The remainder of this paper elaborates on these themes. The paper concludes with a collection of next steps for social partners, researchers, and civil society actors.

1

COMPLIANCE AND ENFORCEMENT CHALLENGES

According to several workshop participants, companies are often not willing and able to comply with workers' requests for information or access, as they do not keep accurate and complete records of personal data processing, do not carry out data protection impact assessments, and often rely on – and have significantly invested in – software that does not provide the requisite levels of transparency and user control (i. e. deletion of data) to be compliant with the GDPR.

In addition, participants noted that enterprises often do not comply with the GDPR because they have no incentives to do so: immediate investment of time and resources is needed to make software and business practices GDPR-compliant, whilst the risks associated with non-compliance are uncertain and generally low. In practice, data protection authorities (DPAs) only have the resources to act on complaints, which individual workers are reluctant to lodge, given the power imbalance at the workplace. In the words of one participant, "workers using their data rights under the GDPR are seen as taking hostile action against the firm." Moreover, even when complaints do reach DPAs, they only take enforcement action and impose dissuasive fines in a very small minority of cases.

On top of all this, works councils and unions lack the expertise and resources to translate sometimes abstract legal principles into concrete collective and company-level agreements that govern data processing at work, and hence do not force employers and platforms to take the GDPR seriously. Lack of expertise is also an issue for companies, especially small and medium-sized enterprises.

Finally, it appears that both collective labour and individual workers do not prioritise data protection and data governance to the extent they possibly should, as they mostly consider these issues through the lens of individual privacy, instead of adopting the view that data flows increasingly affect workplace relations across the board (autonomy, sanctions, rewards, competitive dynamics). That is, data processing shapes both workers' working conditions and the power relationships between workers and employers (see e. g. Adams and Wenckebach 2023; Calacci and Stein 2023).

2

UNDEREXPLORED OPTIONS IN DATA PROTECTION LAW

This section reviews five thus far little-used possibilities established by the GDPR that could improve workplace data protection. Section 2.1 briefly introduces Art. 88 GDPR, which empowers Member States to set out additional data protection rules specific to the work context. Recent legal developments relating to such 'Article 88 rules,' as well as suggested content for such rules, are discussed further in the companion paper, 'Bargaining over workers' data rights,' by Halefom Abraha.

Section 2.2 discusses opportunities created by Art. 80(2) GDPR, which empowers Member States to allow not-for-profit organisations such as trade unions and consumer associations to lodge complaints with DPAs without an explicit mandate from the directly affected data subjects.

Section 2.3 introduces Art. 25 GDPR ('data protection by design and default'), which requires controllers to 'implement appropriate technical and organisational measures' to effectively implement data-protection principles, and discusses its potential relevance at the workplace.

Section 2.4 reviews Arts. 40–41 GDPR. These provisions empower bodies representing groups of data controllers to establish voluntary codes of conduct to further specify the meaning of GDPR principles in specific contexts. 'Employer processing of workers' personal data' could be one such context.

Finally, Section 2.5 reviews Art. 42–43 GDPR, which provide for the establishment of data protection certification systems.

2.1 ARTICLE 88 GDPR: NATIONALLY SPECIFIC WORKPLACE DATA PROTECTION RULES

Art. 88 GDPR establishes that Member States may 'provide for more specific rules' regarding processing of employees' personal data in the employment context. These rules may take the form of national laws or collective agreements, including 'works agreements' (i. e. agreements concluded at the level of the undertaking, e. g. *Betriebsvereinbarungen*). Recital 155 clarifies that these rules may set out, e. g., appropriate legal bases and purposes for processing of employees' personal data. For examples of collective bargaining agreements on data, see the Digital Bargaining Hub created by Public Services International (PSI).

Art. 88(3) GDPR requires Member States to notify the Commission regarding their use of these provisions. Legal scholarship published in 2022 assessed the extent to which Member States' documented use of the provisions up to that time addressed previously documented challenges in the area of workplace data protection (Abraha 2022). At that time, 17 Member States had established workplace-specific data protection rules of one sort or another. Abraha (2022) found, however, that while this use had enabled 'diverse and at times innovative regulatory approaches' by Member States to address needs arising from their specific labour law and industrial relations traditions, Member States' employment-specific rules did not all seem to meet the requirements set out in Art. 88(2).

Art. 88(2) requires that nationally-specific workplace data protection rules 'include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard' to specific data processing practices. At the time, Abraha wrote that Member States' diverse usages of Art. 88 GDPR appeared to risk increasing fragmentation with regard to workplace implementation and enforcement of GDPR.

And, indeed, in 2023, in *Hauptpersonalrat der Lehrerinnen*, a German administrative court asked the CJEU to assess whether the German laws implementing Art. 88 GDPR met Art. 88(2) requirements. The CJEU found that, as they did not add substantive new workplace-specific rules with 'suitable and specific' safeguards, they did not. The ruling appears to have effectively invalidated the German Art. 88 law and may have significant implications for other Member State laws as well (see further Abraha 2023).

This rather dramatic ruling creates an opportunity for civil society actors to encourage national legislators to ensure that the content of new national workplace data protection laws provides substantive, usable, and relevant protections for workers in the face of increasingly high-stakes workplace data processing.

The companion paper by Halefom Abraha ('Bargaining over workers' data rights') discusses the specific content

that unions and, especially in countries where union power and capacity is limited, other civil society actors may wish to advocate for.

2.2 ARTICLE 80(2) GDPR: EMPOWERING 'OWN-INITIATIVE' COMPLAINTS FROM CIVIL SOCIETY ORGANISATIONS

According to Art. 80(1) of the GDPR, Member States are to ensure that data subjects can mandate an organisation to represent them and lodge complaints with Data Protection Authorities (DPAs) (Art. 77), go to court to challenge decisions of DPAs (Art. 78), and sue data controllers and processors if their rights have been infringed (Art. 79). However, anecdotal evidence suggests that workers may be reluctant to mandate organisations to complain or litigate on their behalf, because it puts them at risk of retaliatory actions by their employers.

Fortunately, Article 80(2) of the GDPR provides that Member States can allow any not-for-profit organisation that acts in the public interest and protects data subjects' rights to lodge complaints with DPAs and to initiate legal proceedings against controllers and processors. They can do so without being mandated by individuals. In other words, they can bring "own-initiative complaints". This could allow unions or other organisations to start administrative procedures or demand legal remedies for workers (excluding compensation), without the latter being individually singled out and vulnerable to employer reprisals.

What is more, the Court of Justice of the EU (CJEU) in the case C-319/20, *Meta Platforms Ireland*, has confirmed that organisations that fulfill the requirements of Article 80 GDPR and/or relevant national laws can bring claims that are in the collective interest of individuals, without having to prove that individual data subjects' rights have been infringed (i. e. that actual harm has occurred).

Unfortunately, save for possibly Denmark (BEUC 2023), it seems no Member State has implemented Art. 80(2), which is optional (see e. g. Pato 2019). However, beyond Denmark, several Member States allow for the possibility of class actions in the consumer sphere, and sometimes more broadly. This is for instance the case in France, Belgium, Germany, the Netherlands and Spain.

It would be worthwhile to conduct further legal analysis to clarify if and where organisations representing collective labour, such as unions, could bring GDPR claims without a prior mandate from individual workers.

2.3 ARTICLE 25 GDPR: DATA PROTECTION BY DESIGN AND DEFAULT

Article 25 GDPR, entitled 'Data protection by design and by default,' requires data controllers to 'implement appropriate technical and organisational measures [...] designed to implement data-protection principles,' to meet GDPR's requirements and protect data subjects' rights.

This article enshrines in law a primarily technical or design 'paradigm' for data protection compliance, developed largely within the field of software engineering (see e. g. Dewitte 2023). While the potential limitations of a technical or 'by design' approach to worker protection in the context of machine-learning, artificial intelligence, or other 'self-learning' decision-making systems have been documented (see e. g. Cefaliello et al. 2023), it should be noted that this does not mean that this approach cannot make some contributions to improving compliance.

Indeed, the European Data Protection Board's Guidance 4/2019 on Article 25 indicates that Article 25 imposes fairly strong obligations on controllers with respect to the systems they may use to process personal data. The Guidance specifies, for example, that while 'processors and producers are [...] key enablers of [data protection by design and default], [...] **controllers are required to only process personal data with systems and technologies that have built-in data protection**' (para. 94, p. 29; emphasis added). On its face, this is a fairly stringent requirement, and the EDPB's Guidance comprehensively elaborates the nature of 'built-in data protection,' including an example in the context of workplace data processing (pp. 22–23).

However, as with the GDPR as a whole, the major issue is one of compliance and enforcement. We can estimate that, at the present juncture, a significant percentage of workplace data processing simply does not comply with Art. 25 GDPR (see e. g. Christl 2023, especially p. 63; more generally see e. g. Christl 2021), and DPAs and worker representatives lack the capability to enforce compliance. Art. 25 nonetheless raises the possibility that compliance can be improved by 'one-time' technical changes to the design of 'standard' software systems used in many workplaces. Future research could assess commonly used workplace software systems for their compliance with the requirements established by Art. 25 as elaborated by the EDPB Guidelines, and highlight opportunities for technical changes that could improve compliance.

Art. 25(3) establishes that Art. 42 GDPR certification mechanisms can be used to demonstrate compliance with the requirements set out by Art. 25(1–2). EDPB Guidance 4/2019 further 'encourages all controllers to make use of certifications and [Art. 40 GDPR] codes of conduct' (p. 4). Future research could therefore examine the possibility of enshrining 'data protection best practices' for workplace software in certifications and codes of conduct.

2.4 ARTICLES 40–41 GDPR: CODES OF CONDUCT

Article 40 GDPR, 'Codes of conduct,' and Article 41 GDPR, 'Monitoring of approved codes of conduct,' establish the legal framework for data protection codes of conduct. While these

codes of conduct are voluntary, the provisions of Arts. 40–41 set out a clear oversight framework for the content of these codes and the manner in which compliance is to be monitored once a controller has signed a code. That is, they are not arbitrary, but rather a form of 'regulated self-regulation.'

Art. 40 sets out that codes of conduct may be developed by 'associations and other bodies representing categories of [data] controllers or processors [...] for the purpose of specifying the application of [GDPR]' in their specific processing practices. Codes of conduct can specify the meaning of key concepts in the GDPR for the specific processing practices of the involved controllers/processors, such as 'fair and transparent' and 'legitimate interests,' as well as standard or 'best' practices to be followed in order to meet data protection obligations, such as information to be provided to data subjects regarding processing and practices to be undertaken to ensure compliance with Art. 25 GDPR (see above, Section 2.3).

It could be possible to consider 'employers' as a 'category' of data controllers, and/or to consider 'providers of software used to process workers' personal data' as controllers and/or processors, and to establish GDPR codes of conduct for these categories of controllers/processors. In this context, such codes could also clarify currently ambiguous and contested terms and questions in the GDPR, such as the specific meaning of the phrase 'strictly necessary' and the proportionality of worker personal data processing (e. g., when an employer's 'legitimate interests' in processing worker data may outweigh, or be outweighed by, workers' data protection rights).

Silberman and Johnston (2020) introduce the content of Arts. 40–41 GDPR in the context of worker data processing (pp. 13–14) and consider the framework established by these provisions in light of past shortcomings of 'self-developed' codes of conduct developed by employers in global commodity value chains (pp. 14–16).

A possible next step for civil society actors could be to conduct qualitative research with relevant stakeholders, especially worker and employer representatives (e. g. through interviews and workshops) and software providers regarding the possible content of GDPR codes of conduct for employers and/or providers of software used to process workers' personal data. This research could also explore possible processes for ensuring that workers and worker representatives are substantively involved in developing, enforcing, and evolving these codes of conduct.

2.5 ARTICLE 42–43 GDPR: CERTIFICATION SCHEMES

Art. 42 GDPR supports the creation of voluntary certification mechanisms, as they can facilitate compliance with the law and improve transparency for data subjects. Especially in the absence of sufficient enforcement, certification can be an important way to improve compliance, by specifying the implications of general data protection provisions contained in the GDPR for specific contexts and data processing operations.

What is unique about the GDPR is that it leaves open who is to draw up the certification criteria – the crucial ingredient in any certification scheme. This means that any organisation, including a union or any other entity that takes workers' interests seriously, can develop a scheme. Once the criteria have been developed, Art. 42 and 43 stipulate that they have to be approved by a data protection authority (DPA) – or, for EU-wide schemes, the European Data Protection Board – and subsequently used by a certification body or DPA to certify data controllers and processors (see e. g. Kamara & De Hert 2018).

The GDPR does not prohibit certification schemes outside the framework of Art. 42 and 43 – and they do exist. These schemes do not benefit from the soft presumptions of compliance that exist for operators that have been certified in accordance with e. g. Art. 42 and 43 (see Art. 24(3), Art. 25(3), Art. 28(5), and Art. 32(3). Nor do they benefit from Art. 83 (2 sub j), which allows adherence to a certification scheme in line with the GDPR to be taken into account when determining fines (i. e. a lower fine).

The potential offered by certification has not been adequately explored to date. According to the European Data Protection Board's own register, there are at present – as of May 2024 – only 4 officially approved certification schemes in operation. These include 1 pan-European scheme, called Europrivacy, as well as 3 national schemes – 1 in Germany, 1 in Luxembourg and 1 in the Netherlands. All are general schemes, meaning that they do not restrict themselves to specific sectors or processing operations. This is far from ideal, as these schemes have yet to make clear how the GDPR applies in a given context such as employee data processing, or for specific operations, like automated processing of CVs (Von Grafenstein 2021).

Therefore, civil society could consider investigating the possibility of drawing up certification schemes that are particularly focused on workers' data processing and pressing issues in a workplace context. Relevant stakeholders, including workers and their representatives, would need to be involved in drawing up such schemes.

3

AUDITING ALGORITHMS VIA INDEPENDENT INVESTIGATIONS

In recent years, a number of methods have been tested to audit algorithmic systems deployed by companies which are unwilling or unable to reveal their impact on working conditions. These methods of investigation can help to detect data protection and labour law violations. The evidence obtained through these methods can be used to trigger or support strategic litigation, as leverage in collective bargaining efforts or to raise awareness of workers and the general public.

These methods have been developed and tested by novel organisations such as Worker Info Exchange, PersonalData.io, Reversing.Works and the Workers' Algorithm Observatory. All methods developed so far require consent and participation of the workers in collecting data necessary for further analysis. The most prominent data collection methods are:

- **Data Subject Access Requests (DSARs):** Workers can demand a copy of their own data using their data rights granted in the GDPR. They can do so by sending an email to the company or authorising a third party to do so on their behalf. The disadvantage of this method is that companies might send incomplete or illegible data, or fail to respond in the first place. While failure to respond is itself nominally a violation of GDPR and is therefore not an insurmountable barrier – as data protection authorities (DPAs) can intervene to direct companies to provide the requested data – it can increase the complexity and cost of this approach.

- **Data Scraping:** Alternative methods of collecting data of individual workers involve them taking regular screenshots of their working app or authorising a piece of software to do so on their behalf. However, just like in the case of DSARs, this method typically requires participation of a relatively large number of workers.

- **Black Box Analysis:** This method requires that a worker share their login and password with a technical expert who can then log in to the app and analyse the data it collects and shares with the platform or other companies. This data collection method can produce useful results even with one participating worker.

The efficiency of these methods depends on the ability to replicate results with a large number of participants and over long periods of time. The data collected through these methods can reveal evidence of elements of the logic embedded in the algorithmic system, but might be insufficient to establish a complete picture. Researchers and practitioners who combine technical, legal, and social expertise have been collaborating across organisations and countries to develop, test and combine methods that allow for further independent audits of algorithmic systems.

The major difficulty identified by this nascent community of practice is closer collaboration with worker organisations, which can help identify further cases of privacy and labor violations. Trade unions and other workers' organisations can help by linking technical investigations to workers' grievances. They can also make use of the findings of technical investigations in their collective efforts to improve working conditions.

Independent technical audits have thus far focused mainly on platform work, especially in the delivery and transportation sectors. Future audits could also investigate data processing systems and practices in 'traditional' workplaces.

4

IMPROVING LEGAL CLARITY AND COMPLIANCE THROUGH STRATEGIC LITIGATION

In the face of significant non-compliance with data protection norms at work, as well as a lack of tailored data protection norms for the workplace, the workshop participants explored the potential of 'strategic litigation' to clarify and enforce GDPR rules. Although strategic litigation typically refers to initiating a legal proceeding in courts, it was stressed that in the case of the data protection laws, data protection authorities (DPAs) can also play an important role.

Importantly, workers and their representatives face lower barriers when filing a DPA complaint than a lawsuit, because a DPA complaint does not have to be accompanied by detailed legal arguments as long as it contains convincing evidence of potential GDPR violations. This evidence could take the form of a forwarded email exchange with the company showing that it did not comply fully with a Data Subject Access Request (DSAR). It could also take the form of pictures or screenshots of features of the software that is considered problematic.

More detailed documentation of the technical audit involving analysis of data obtained through multiple DSARs, data scraping or black-box analysis can also be submitted as evidence to the DPA, but it is not necessary. In the best-case scenario, a well-documented complaint serves to trigger a DPA to conduct its own investigation into company practices. Such investigations can result in sanctions that include compelling the company to remedy the problems – as well as significant fines, which can serve as a deterrent for other companies.

Civil society could play a role by supporting actors who collect evidence of violations and submit it as part of complaints to national DPAs or labour courts, thereby helping to produce case law and DPA rulings that improve legal certainty; raise awareness of the rules for workers, trade unions, employers, software providers and authorities; and, when these cases lead to fines, incentivise businesses to comply. Such a strategy of supporting the actors 'from below' might be particularly useful when it comes to clarifying regulations at the national level, because workers and trade unions might be concerned that private enforcement via litigation is time-consuming and involves significant expenses in the form of legal experts. It would be particularly worthwhile to support the creation of a platform for exchanging practices of evidence-collection and analysis, as well as experience and expertise regarding the various national laws and procedures.

However, there might also be potential for a more top-down approach similar to the one pioneered by organisations such as "None of Your Business" (NOYB) and Foxglove, active in the field of data protection. Although these organisations do not focus on employees as a specific category of data subjects, it would be advisable to explore their interest in expanding their scope of action to workers, or founding a new organisation dedicated exclusively to workers as data subjects. As already stated in Section 2.2, further research should address in which national jurisdictions such organisations could represent workers in line with Art. 80(2), as national rules for collective claims vary across EU Member States. Such an organisation would be best equipped to explore legal strategies on an EU scale by preparing lawsuits that have the potential to reach the Court of Justice (CJEU).

5

NEXT STEPS FOR SOCIAL PARTNERS, RESEARCH, AND CIVIL SOCIETY ACTORS

With a view to the issue of non-compliance with the GDPR at the workplace, the preceding sections looked at several underexplored options to remedy the situation. It is evident, however, that the effectiveness of those options would greatly benefit from improved enforcement by data protection authorities (DPAs) as well. Therefore, an expansion of DPA capacity and activities, especially in the area of workers' data processing, would be very welcome. This would also involve DPAs securing sufficient funding and investing in technical expertise, as well as improving effective enforcement and mutual cooperation, points which have been made by researchers (Nogarede 2021, ICCL 2021, 2023; NOYB 2022, 2023).

With this general context having been established, the remainder of this section proceeds to suggest next steps for the specific areas that were addressed in sections 2, 3 and 4 with the aim of redressing the compliance gap of data protection at the workplace.

5.1 CLARIFYING, SPECIFYING, AND OPERATIONALISING DATA PROTECTION LAW

As has been explained, a barrier to compliance with data protection at work is that none of the mechanisms to tailor the GDPR to the work context, ranging from Art. 88 laws and collective agreements to certification schemes and codes of conduct, have been sufficiently leveraged.

LAWS AND COLLECTIVE BARGAINING

In an accompanying paper, 'Bargaining over workers' data rights', Halefom Abraha has provided guidance to unions on how to specify data protection law for the workplace. This can serve as a template for Art. 88 laws and collective agreements that can be used across Europe.

Civil society and organised labour can use the paper and principles underlying it to initiate discussions with relevant governments and between the social partners. Momentum can be generated if the German government follows through on the announcement it made in connection with the 2023 Data Strategy (*Fortschritt durch Datennutzung*) by publishing its draft Employee Data Protection Act.

CODES OF CONDUCT AND CERTIFICATION

It is difficult to get workers' data protection rights recognised in practice. At the same time, for employers small and large, there is a lot of uncertainty about how to comply with the GDPR in workplace contexts. Many of the requirements established by the GDPR could be further clarified in codes of conduct and certification schemes. Art. 25 GDPR, which stipulates that data controllers take 'appropriate technical and organisational measures' to ensure 'data protection by design and by default,' is one example of a provision that could benefit from such clarification.

As a start, it would be valuable for future research to assess to what extent commonly used workplace software systems comply with the requirements of Art. 25, and if they do not, what technical and organisational changes could be made to improve compliance. Given that even the European Commission itself has been found to breach data protection rules relating to its use of Microsoft's 365 software package (EDPS 2024), this would be an especially topical case to consider. Such an assessment could also help clarify the kind of elements that would be suitable for codes of conduct and certification schemes – and help build the case for their necessity.

Beyond assessing compliance of individual software packages with the GDPR, civil society actors could look into the specification of law through codes of conduct and certification schemes. A possible first step would be to conduct interviews and organise workshops with relevant stakeholders, in particular worker and employer representatives, as well as software providers, regarding such codes and schemes for employers of software used to process personal data of workers. This research could explore both the possible content of such codes as well as possible processes to ensure workers' ongoing involvement in developing, enforcing, and evolving them.

Further investigations will have to be carried out about the drawbacks and advantages of each option in a given work context. For instance, while both codes of conduct and certification schemes are voluntary, the difference is that for certification schemes under the GDPR, there is no restriction as to who drafts the criteria, whereas for a code of conduct this is limited to "associations and other bodies representing

controllers or processors". That said, certification schemes would most likely need to be used by national certification bodies to become effective.

Therefore, civil society research could engage representatives from potentially relevant organisations (such as regional and national data protection authorities), technical inspection associations (i. e. TÜVs), technical standardisation organisations (such as DIN, CEN, and ISO), and accreditation bodies (e. g. DakkS, ILNAS) in exploratory discussions to consider their possible roles in developing these mechanisms and promoting their adoption.

5.2 STRENGTHENING PRIVATE ENFORCEMENT OF DATA PROTECTION LAW

As mentioned at the outset, compliance with data protection law at work appears to be poor. Even though new procedural rules are being negotiated to improve cooperation between DPAs, the latter are unlikely to be able to turn the situation around on their own. Moreover, with the recently agreed Platform Work Directive and AI Act, responsibilities and coordination challenges for DPAs will only increase. With this in mind, this section explores the next steps that organised labour and other civil society organisations can take themselves to boost data protection compliance and enforcement at the workplace.

EVIDENCE COLLECTION

There is anecdotal evidence of widespread non-compliance with the GDPR at the workplace. But this is not widely known beyond practitioners and experts. Therefore, a useful step would be for organised labour and other civil society actors to collect a list of obvious and widespread GDPR infringements at work – either in a short report or, better yet, an online database. This could be complemented by surveys, focus groups, or other methods helping to understand workers' attitudes toward GDPR rights, as well as to get a better picture of non-compliance – for instance with regard to information rights set out in Art. 13 and 14 of the GDPR. These actions would make visible to a wider audience what experts already know and it would help make non-compliance a political issue. It would help social partners, academics and civil society to focus their efforts.

ENCOURAGING COLLECTIVE LABOUR TO WORK WITH TECHNICAL EXPERTS

Some evidence is difficult to obtain without technical expertise. Thus, section 3 highlighted the potential offered by technical methods to expose data protection and labor law violations. The challenge, however, is to bring this technical community closer to the workers' organisations which can voice workers' grievances and help identify legal infringements.

One very positive step would be for workers' organisations to allocate more resources to data protection and data governance issues by increasing training on these topics and highlighting their relevance for collective bargaining. Efforts in this direction are underway (Colclough 2023), and it would complement existing activities from Public Services International as well as FES Future of Work and UNI Europa, which have built online tools that gather information on existing collective bargaining agreements that also cover data-gathering at the workplace.

In addition, workers' organisations could redouble efforts to build connections with – and facilitate access to – technical experts like data analysts. An opportunity is to be found here, as there is a mounting body of law allowing workers representatives to rely on outside experts at the cost of the employer (German Works Constitution Act Section 80(3); Platform Work Directive Art. 13(3)).

STRATEGIC LITIGATION

Beyond matters of technical expertise and evidence-gathering, civil society organisations could help pinpoint where opportunities exist to advance strategic litigation involving workers' data, with litigation also including the lodging of complaints with DPAs. A first step would be conducting a legal analysis to find out where 'own-initiative' complaints by unions are possible in the EU, under Art. 80(2) GDPR or other legislation like collective claims laws, as well as analysing the different costs, risks and bottlenecks associated with litigation involving workers' data rights.

In addition, it would be useful to map the field of existing stakeholders that are working to advance workers' data protection rights with a view to assessing whether they can help increase workplace data protection compliance through administrative and legal procedures, or whether it would be worthwhile to establish a new organisation dedicated exclusively to the rights of workers as data subjects. Such an organisation might be better equipped to explore legal strategies on the EU scale by preparing lawsuits that have the potential to reach the Court of Justice (CJEU).

REFERENCES

Abraha, H. (2022). A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace. *International Data Privacy Law* 12(4) 276–296. https://doi.org/10.1093/idpl/ipac015.

Abraha, H (2023). Hauptpersonalrat der Lehrerinnen: Article 88 GDPR and the Interplace between EU and Member State Employee Data Protection Rules. *The Modern Law Review* 87(2) 484–496. https://doi.org/10.1111/1468-2230.12849.

Abraha, H (2024). *Bargaining over workers´ data rights*. Friedrich-Ebert-Stiftung, June.

Adams, Z., and Wenckebach, J. (2023). Collective regulation of algorithmic management. *European Labour Law Journal* 14(2): 211–229. https://doi.org/10.1177/20319525231167477.

BEUC (2023). Recommendations on harmonising procedural matters in the GDPR, March. Accessed at https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-034_recommendations_on_harmonising_cross-border_procedural_matters_in_the_GDPR.pdf.

Bundesregierung (2023). Fortschritt durch Datennutzung. Strategie für mehr und bessere Daten für neue, effektive und zukunftsweisende Datennutzung, August. Accessed at https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2023/datenstrategie.html.

Calacci, D. and Stein, J. (2023). From access to understanding: Collective data governance for workers. *European Labour Law Journal* 14(2): 253–282. https://doi.org/10.1177/20319525231167981.

Cefaliello, A., Moore, P. V., and Donoghue, R. (2023). Making algorithmic management safe and healthy for workers: Addressing psychosocial risks in new legal provisions. *European Labour Law Journal* 14(2) 192–210.

Christl, W. (2021). Digitale Überwachung und Kontrolle am Arbeitsplatz: Von der Ausweitung betrieblicher Datenerfassung zum algorithmischen Management? Vienna: Cracked Labs/Arbeiterkammer Wien. https://crackedlabs.org/dl/CrackedLabs_Christl_UeberwachungKontrolleArbeitsplatz.pdf.

Christl., W. (2023). Monitoring, Streamlining and Reorganizing Work with Digital Technology: A case study on software for process mining, workflow automation, algorithmic management and AI based on rich behavioral data about workers. Vienna: Cracked Labs/Arbeiterkammer Wien. https://crackedlabs.org/dl/CrackedLabs_Christl_Celonis.pdf.

Colclough, C. (2023). Protecting workers´ rights in digitised workplaces. *Equal Times*, 4 May. Accessed at https://www.thewhynotlab.com/publications/protecting-workers-rights-in-digitised-workplaces.

Dewitte, P. (2023). A Brief History of Data Protection by Design. From multilateral security to Article 25(1) GDPR. *Technology and Regulation* 80–94. https://doi.org/10.26116/techreg.2023.008.

European Data Protection Board (EDPB) (2020). Guidelines 4/2019 on Article 25. Data Protection by Design and by Default. Version 2.0. Accessed at https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

European Data Protection Supervisor (EDPS) (2024). European Commission´s use of Microsoft 365 infringes data protection law for EU institutions and bodies, March. Press Release. Accessed at https://www.edps.europa.eu/system/files/2024-03/EDPS-2024-05-European-Commission_s-use-of-M365-infringes-data-protection-rules-for-EU-institutions-and-bodies_EN.pdf.

Irish Council for Civil Liberties (ICCL) (2021). Europe´s enforcement paralysis. Accessed at https://www.iccl.ie/wp-content/uploads/2021/09/Europes-enforcement-paralysis-2021-ICCL-report-on-GDPR-enforcement.pdf.

Irish Council for Civil Liberties (ICCL) (2023). 5 years: GDPR´s crisis point. Accessed at https://www.iccl.ie/digital-data/iccl-2023-gdpr-report/.

Kamara, I. and De Hert, P. (2018). Data Protection Certification in the EU: Possibilities, Actors and Building Blocks in a reformed landscape, 7–33. In Rodrigues, R. and Papakonstantinou, V. (eds). *Privacy and Data Protection Seals*. T.M.C. Asser Press.

Nogarede, J. (2021). No digitalisation without representation. An analysis of policies to empower labour in the digital workplace. FEPS Policy Study, November. Accessed at https://feps-europe.eu/publication/826-no-digitalisation-without-representation/.

NOYB (2022). Annual Report 2022. Accessed at https://noyb.eu/en/annual-report-2022-out-now

NOYB (2023). 5 Years of the GDPR: National Authorities let down European Legislator, May. Accessed at https://noyb.eu/en/5-years-gdpr-national-authorities-let-down-european-legislator.

Pato, A (2019). The national adaptation of article 80 GDPR: Towards the effective private enforcement of collective data protection rights, 98–106. In: McCullagh, K., Tambou, O. and Bourton, S. (eds.). National Adaptations of the GDPR, Collection Open Access Book, Blogdroiteuropeen, Luxembourg, February 2019.

Silberman, M. and Johnston, H. (2020). Using GDPR to improve legal clarity and working conditions on digital labour platforms. Working paper 2020.05. ETUI. Accessed at https://www.etui.org/sites/default/files/2020-06/WP%202020.05%20GDPR%20Working%20conditions%20digital%20labour%20platforms%20Silberman%20Johnston%20web.pdf.

Von Grafenstein, M. (2021). Specific GDPR certification schemes as rule, general schemes (and criteria) as exception. HIIG Discussion Paper 2021-04. DOI 10.5281/zenodo.4905484.

ABOUT THE AUTHORS

Justin Nogarede is Senior Policy Officer at FES Future of Work. He focuses on data protection issues at work and the political economy of digitalisation. Before joining the team, he covered the digital policy portfolio at the Foundation for European Progressive Studies (FEPS). In the past, he also worked as policy officer in the Secretariat-General of the European Commission, on better regulation, the application of EU law, and various digital and single market policy files.

Michael Six Silberman works as a postdoctoral researcher in the 'iManage' Project on 'Rethinking Employment Law for a World of Algorithmic Management,' based at the Bonavero Institute of Human Rights at the University of Oxford, and as the Lecturer in Sociotechnical Systems at the London College of Political Technology (Newspeak House). In the past, Silberman worked for IG Metall, the trade union in the German manufacturing sector, on rights for workers on digital labour platforms.

Joanna Bronowicka is a sociologist at the Center for Interdisciplinary Labour Law Studies at the European University Viadrina in Frankfurt (Oder) where she researches algorithmic management, resistance practices, and mobilisations of platform workers in Berlin. Previously, she worked as the director of the Centre for Internet and Human Rights and as an analyst at the Ministry of Digitisation in Poland.

Acknowledgements

Special thanks to Christina Colclough for facilitating the October 2023 workshop and for her contributions to this report, and to the workshop participants for sharing their time and expertise with us. We thank James Turner for editing the report and Ha-Thu Mai from FES Future of Work for co-organising the workshop. Participation and writing time for co-author Silberman was funded partially by the European Research Council 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 978-3-98628-494-7