


# A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace

Halefom H. Abraha  \*

## Key Points

- The distinct challenges of data processing at work have led to long-standing calls for sector-specific regulation. This leaves the European legislature with a dilemma.
- While the distinct features of employee data processing give rise to novel issues that cannot adequately be addressed by an omnibus data protection regime, a combination of legal, political, and constitutional factors have hindered efforts towards adopting harmonized employment-specific legislation at the EU level.
- The ‘opening clause’ in Article 88 General Data Protection Regulation (GDPR) aims to square this circle. It aims to ensure adequate and consistent protection of employees while also promoting regulatory diversity, respecting national peculiarities, and protecting Member State autonomy.
- This article examines whether the opening clause has delivered on its promises.

- It argues that while the compromise has delivered on some of its promises in promoting diverse and innovative regulatory approaches, it also runs counter to the fundamental objectives of the GDPR itself by creating further fragmentation, legal uncertainty, and inconsistent implementation, interpretation, and enforcement of data protection rules.

Regulation applies in its entirety to the processing of workers’ data, the employer–employee relationship is characterized by a number of specificities which give rise to novel issues that cannot be adequately addressed by an omnibus data protection regime—from the intrusiveness and scale of technologies deployed under the guise of legitimate interests in the workplace and the collective dimension of labour law to the inequality of bargaining power which characterizes nearly all wage-work bargains. These special features have given rise to repeated calls for specific data protection rules that exclusively apply to employment.

Despite general agreement that a specific regulatory framework is needed to complement and particularize omnibus data protection principles for employment matters, disagreement remains as to whether it should be created by a Union legal act or by domestic legislation. This disagreement is demonstrated by the EU’s multiple failed attempts to introduce an employment-specific data pro-

## Introduction

One of the success stories of the General Data Protection Regulation (GDPR)<sup>1</sup> is the harmonized, consistent, and comprehensive regulation of personal data processing. In the employment context, however, the GDPR falls short in fulfilling this promise. Although the

\*Halefom H. Abraha, Bonavero Institute of Human Rights, University of Oxford, Oxford, UK. Email: halefom.abraha@law.ox.ac.uk. The author offers special thanks to Professor Jeremias Adams-Prassl and Aislinn Kelly-Lyth for their invaluable feedback and extensive reviews. The author also thanks Wolfie Christl, Justin Nogarede, and all participants of the Algorithms at Work Reading Group. The usual disclaimers apply. The author acknowledges funding from the European Research Council under the European Union’s

Horizon 2020 research and innovation programme (grant agreement No 947806).

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

tection framework. Consequently, there is currently no EU data protection legislation exclusively targeting employment relations.

In the lead-up to the adoption of the GDPR, European legislators faced a dilemma regarding the harmonization of data protection rules in the employment context. On the one hand, the distinct features of processing workers' data warrant sector-specific regulatory treatment. On the other hand, a combination of legal, pragmatic, political, cultural, and constitutional factors hindered efforts of adopting such sector-specific legislation at the EU level.

The GDPR harmonizes data protection rules throughout the EU and is directly and consistently applicable in all Member States. This means that Member States have the obligation to amend or replace their respective national data protection laws to align with the GDPR.<sup>2</sup> However, there are also certain areas or specific processing situations covered by the GDPR where Member States could not reach a political agreement because of national sensitivities and constitutional issues. The GDPR addresses the disagreements by incorporating specific clauses that explicitly allow Member States to further specify its application in these areas. These specifications, known as 'opening clauses',<sup>3</sup> are commonly used 'in harmonization measures of EU secondary law'<sup>4</sup> as a compromise to facilitate political agreement on the remaining text of the law.<sup>5</sup>

Data processing in the context of employment is one of these few areas where Member States could not reach a political agreement. The legislative compromise the

EU reached to address this predicament is therefore the 'opening clause'<sup>6</sup> under Article 88 of the GDPR, granting Member States regulatory leeway to enact their own legislation in the area of employee data protection, supplementing the GDPR's provisions. Article 88 of the GDPR thus aims to address the specific needs of data processing in the employment context while also promoting regulatory diversity, respecting national industrial relations traditions, and protecting Member State autonomy.

Whether this opening clause has delivered on its promise of a pragmatic compromise remains unexamined both at academic and policy levels.<sup>7</sup> When asked in 2018 whether there was 'a danger of European data protection law becoming fragmented as a result of the piecemeal use of the opening clauses in the GDPR', the Commission suggested that it was 'launching a study to evaluate the use of some of the specification clauses by Member States'.<sup>8</sup> To date, no such report has been released.<sup>9</sup> A 2020 Communication, which noted that 'a degree of fragmentation and diverging approaches' exists due to the 'extensive use' of the various opening clauses of the GDPR, did not cover Article 88.<sup>10</sup> The provision also escaped discussion in a recent report published by the Directorate-General for Justice and Consumers on the implementation of the GDPR.<sup>11</sup>

The present contribution fills this gap in the literature. It does so by systematically mapping how the Member States have utilized the permissive clause in Article 88(1), examining the extent to which national regulatory instruments provide suitable and specific

2 As shall be discussed below, all EU Member States, except Slovenia, have adopted or adapted their national data protection laws following the coming into force of the GDPR.

3 For a complete list of the opening clauses found throughout the GDPR, see Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer International 2017) 220; 'Commission Staff Working Document {COM(2020) 264 Final}' (European Commission 2020) <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0115>> accessed 4 April 2022.

4 see Emilia Mišćenić and Anna-Lena Hoffmann, 'The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation (GDPR)' [2020] EU and comparative law issues and challenges series (ECLIC) 51 [noting that the term 'opening' is used to accentuate the imperfection of legal clauses that are in need of further concretization].

5 It is important to note that opening clauses should be distinguished from the obligation to implement certain other provisions of the GDPR, such as setting up data protection authorities, through Member State legislation.

6 Also known as 'facultative specification clause', 'saving clause', or 'specification clause'. The European Commission is of the opinion that the term 'opening clauses' is misleading since it might give the impression that Member States have margins of manoeuvre beyond the provisions of the Regulation. See 'Commission Staff Working Document {COM(2020) 264 Final}' (n 3) 17.

7 On the numerous opening clauses of the GDPR in general, see Kristina Yuliyanova Chakarova, 'General Data Protection Regulation: Challenges

Posed by the Opening Clauses and Conflict of Laws Issues' (European Union Law Working Papers No 41 2019); Emilia Mišćenić and Anna-Lena Hoffmann, 'The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation (GDPR)' [2020] EU and comparative law issues and challenges series (ECLIC); Voigt and von dem Bussche (n 3); Marian Müller, *Die Öffnungsklauseln der Datenschutzgrundverordnung: Ein Beitrag zur Europäischen Handlungsformenlehre* (Wissenschaftliche Schriften der WWU Münster 2018).

8 'Parliamentary Questions: Question for Written Answer P-003121-18 to the Commission Rule 130 Nadja Hirsch (ALDE)' (*European Parliament*, 8 June 2018) <[https://www.europarl.europa.eu/doceo/document/P-8-2018-003121\\_EN.html](https://www.europarl.europa.eu/doceo/document/P-8-2018-003121_EN.html)> accessed 4 April 2022; 'Parliamentary Questions: Answer given by Ms Jourová on Behalf of the Commission Question Reference: P-003121/2018' (*European Parliament*, 13 July 2018) <[https://www.europarl.europa.eu/doceo/document/P-8-2018-003121-ASW\\_EN.html](https://www.europarl.europa.eu/doceo/document/P-8-2018-003121-ASW_EN.html)> accessed 4 April 2022.

9 The Commission has a public registry of Member States who submit their notification on the specific rules adopted pursuant to Article 88(3). See 'EU Member States Notifications to the European Commission under the GDPR' (*European Commission - European Commission*) <[https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications_en)> accessed 27 January 2022.

10 Communication from the commission {SWD(2020) 115 final} 17–19.

11 TIPIK Legal, 'Report on the Implementation of Specific Provisions of Regulation (EU) 2016/679' (European Commission, Directorate—General for Justice and Consumers 2021).

safeguards within the meaning of the conditional clause in Article 88(2). It argues that while the compromise has delivered on some of its promises in promoting diverse and innovative regulatory approaches, it also runs counter to the fundamental objectives of the GDPR itself by creating further fragmentation, legal uncertainty, and inconsistent enforcement.

Discussion proceeds in four parts. The next section sets out the salient features of personal data processing in the employment context in order to demonstrate why specific regulatory responses are required. ‘Union efforts to regulate data processing in the employment context’ section recounts the efforts made to establish an EU-level framework for the processing of workers’ personal data and considers why such a framework has never materialized.

“Opening Clause” as a compromise solution’ section maps how the Member States regulate workers’ personal data processing through legislation, collective agreements, or a combination of the two, and presents a comparative review of these regulatory approaches. This section also examines existing enforcement mechanisms and institutional arrangements, with a particular emphasis on the role of workers’ representative bodies. ‘Substantive content: “suitable and specific safeguards”’ section turns to the substantive aspects of the ensuing regulatory regimes and examines whether they provide suitable and specific measures to safeguard workers’ human dignity, legitimate interests, and fundamental rights within the meaning of Article 88. Drawing on existing regulatory instruments, other provisions of the GDPR itself, and case law, this section develops four overarching principles against which national regulatory instruments should be measured to determine whether they comply with the substantive requirements stipulated under Article 88(2) of the GDPR. The last section concludes.

## Distinctive features of employee data processing

What is distinctive about personal data processing in the employment context and why does it merit special

regulatory treatment? There are at least three notable aspects in which the processing of personal data in the context of employment relations is distinct from most other contexts.

First, as the European Fundamental Rights Agency (FRA) has noted, ‘some of the most advanced technologies for monitoring and controlling the behaviour of individuals ... are used predominantly in working life’.<sup>12</sup> Employers are increasingly deploying sophisticated technologies, ‘including systems designed to collect vast quantities of data about what goes on in a workplace; when employees leave their work stations; to whom they talk; what they type; how quickly they complete tasks; even their mood’.<sup>13</sup> In 2017, the Article 29 Working Party (WP29) observed that ‘(m)odern technologies enable employees to be tracked over time, across workplaces and their homes, through many different devices such as smartphones, desktops, tablets, vehicles and wearables’.<sup>14</sup>

Further complicating matters, employers often rely on a range of ostensibly legitimate interests to justify the processing of large-scale data, making the line between acceptable and unacceptable data practices harder to draw. Such invasive data practices have been compounded by the COVID-19 pandemic, which has increasingly normalized employee monitoring and surveillance in unprecedented ways and has increasingly blurred the line between workplace and private life, leading to the emergence of people analytics tools and sophisticated algorithms that give rise to the full automation of managerial functions.<sup>15</sup> These new technologies and practices, coupled with the range of legitimate interests applicable to employee data processing, mean that the processing of personal data in the employment context is most likely greater in range, volume, and impact than in other contexts. Moreover, these new and emerging technologies deployed in the workplace give rise to new legal questions as to the sufficiency of existing protections.<sup>16</sup>

A second distinct feature of personal data processing in the employment context is the nature of the employer–employee relationship, which is a relation of power and goes beyond the traditional controller–

12 European Fundamental Rights Agency, ‘Data Protection in the European Union: The Role of National Data Protection Authorities’ (Publications Office of the European Union 2010) 37.

13 Charlotte Garden, ‘Labor Organizing in the Age of Surveillance’ (2018) 63 *St Louis U L J* 55; See also Bart Custers and Helena Ursic, ‘Worker Privacy in a Digitalized World under European Law’ (2018) 39 *Comp Labor L & Pol’y J* 323.

14 Art 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, Adopted on 8 June 2017, 9.

15 Justin Nogarede, ‘No Digitalisation without Representation: An Analysis of Policies to Empower Labour in the Digital Workplace’ (FEPS Policy

Study, November 2021) 9; For a comprehensive study of the ever evolving and ubiquitous use of new technologies in the workplace and their implications for employees’ personal data protection, see Wolfie Christl, ‘Digitale Überwachung Und Kontrolle Am Arbeitsplatz: Von der Ausweitung Betrieblicher Datenerfassung zum Algorithmischen Management?’ (Cracked Labs, September 2021) <<https://crackedlabs.org/daten-arbeitsplatz>> accessed 17 January 2022.

16 For details on this, Ifeoma Ajunwa, ‘Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law’ (2018) 63 *St Louis U LJ*.

data subject relationship recognized in data protection law. Such relation of power challenges some of the key underlying principles of data protection law, such as consent, at their core. The inherent inequality of power grants employers the power to control not only the work but also the physical and mental well-being of their employees. It also means that employees are frequently unable to assert their fundamental rights effectively. As Hendrickx and Van Bever note, 'being an employee implies that one's freedom is partly impaired in the sense that the employer can control personal behaviour'.<sup>17</sup> This means that employees are not just 'data subjects' within the meaning of the GDPR. They are 'double victims once as citizens and consumers and secondly as dependent workers'.<sup>18</sup> Labour law recognizes the subordinate nature of employment relations and tries to rebalance it by providing special protection for employees, effectively limiting contractual freedom by setting minimum standards which cannot be reduced by agreement. Judicial approaches in the employment context may also deviate from ordinary principles of contract law in recognition of the impacts of an inherent inequality of bargaining power.<sup>19</sup>

The third distinguishing feature of data processing in the employment context is its collective dimension, including in particular collective rights to information, participation, and co-determination.<sup>20</sup> While these collective rights and interests are inherent in labour law, they do not easily fit with the GDPR, which almost exclusively focuses on individual data subjects and individual rights.<sup>21</sup> In its recent Directive proposal, the European Commission recognized that the GDPR 'does not encompass important collective aspects inherent in labour law'.<sup>22</sup> Adrian Todolí-Signes aptly summarizes this challenge:

One of the biggest problems with data protection regulations in their application to labour relations is the

utmost lack of collective rights. Indeed, the European regulation has an individualistic character in which rights are granted exclusively to the person concerned without thinking about the possible existence of collective rights. While this may be more or less acceptable when the person concerned is a consumer, it makes little sense when the person concerned is a worker (...).<sup>23</sup>

Because of its individualistic approach, the GDPR is often criticized for failing to offer a 'structural change in the level of employee monitoring'.<sup>24</sup> It is only recently that the collective nature of data protection in the workplace has received more attention.<sup>25</sup>

These salient features—the intrusiveness and scale of technologies deployed under the guise of legitimate interests, the collective aspect of labour law, and the special nature of the employment relationship—render the general data protection rules not fit for purpose, giving rise to repeated calls for specific data protection rules that exclusively apply to employment. Although the need for employment-specific rules has become urgent due to the ever-increasing digitalization of the world of work and its attendant risks to human dignity, fundamental rights, and freedoms of employees, such calls are not new. In their respective 1999 pioneering works, Spiros Simitis and Mark Freedland argued that the omnibus rules of the 1995 Data Protection Directive were not fit for the particular requirements of the employment sector. They made the case for a European directive on the protection of employees' data.<sup>26</sup>

## Union efforts to regulate data processing in the employment context

At a policy level, the Council of Europe pioneered efforts to introduce employment-specific regulations for data processing in the workplace by adopting a Recommendation on the Protection of Personal Data

17 Frank Hendrickx and Aline Van Bever, 'Article 8 ECHR: Judicial Patterns of Employment Privacy Protection' in Filip Dorsemont, Klaus Lörcher and Isabelle Schömann (eds), *The European Convention on Human Rights and the Employment Relation* (Hart Publishing 2013) 185.

18 Clara Fritsch, 'Data Processing in Employment Relations; Impacts of the European General Data Protection Regulation Focusing on the Data Protection Officer at the Worksite' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Reforming European Data Protection Law* (Springer 2015) 149.

19 See eg *CJEU, C-413/13 FNV Kunsten Informatie en Media v Staat der Nederlanden* [2014].

20 As O Kahn-Freund pointed out, the law of labour relations comprises the individual relations between employers and the collective relations between unions and other groups of workers and management. See O Kahn-Freund, 'On Uses and Missuses of Comparative Law' (1974) 37 *Mod L Rev* 21.

21 Art 80 of the GDPR is the only exception. See generally, Salomé Viljoen, 'A Relational Theory of Data Governance' (2021) 131 *Yale L J* 370.

22 Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, COM(2021) 762 final.

23 Adrián Todolí-Signes, 'Algorithms, Artificial Intelligence and Automated Decisions Concerning Workers and the Risks of Discrimination: The Necessary Collective Governance of Data Protection' (2019) 25 *Transfer: Eur Rev Labour Res* 475; Adrián Todolí-Signes, 'Spanish Riders Law and the Right to Be Informed about the Algorithm' 12 *Eur Labour L J* 399, 401.

24 Nogarede (n 15) 16.

25 See for instance, Draft Directive on Platform work; Todolí-Signes (n 23); Nogarede (n 15).

26 Spiros Simitis, 'Reconsidering the Premises of Labour Law: Prolegomena to an EU Regulation on the Protection of Employees' Personal Data' (1999) 5 *Eur L J* 45; Mark Freedland, *Data Protection and Employment in the European Union: An Analytical Study of the Law and Practice of Data Protection and the Employment Relationship in the EU and Its Member States* (European Commission 1999).



Used for Employment Purposes in 1989 (revised in 2015).<sup>27</sup> The International Labour Organization (ILO) and WP29 followed suit by adopting a code of practice on the 'Protection of workers' personal data' in 1997,<sup>28</sup> and 'Opinion 8/2001 on the processing of personal data in the employment context' respectively.<sup>29</sup> Whilst these non-binding instruments addressed many of the salient features of employment relations identified above, however, they remained non-binding.

Multiple attempts to introduce a specific framework at the Union level similarly failed to achieve legally binding rules. The following sections trace back these efforts and identify the reasons why they failed, including (i) the overlap of data protection law with other areas of law, (ii) the need for flexibility at the domestic level, and (iii) constitutional tensions and a lack of political compromise.

### Failed attempts to introduce a European-level framework

At least three attempts to introduce a European-level framework proved unsuccessful. The European Commission first launched a two-stage consultation on the protection of workers' personal data with social partners in 2001. Having examined the EU and national data protection frameworks in operation at that time, the Commission concluded that:

a European framework of common principles and rules [was] needed aiming at the protection of workers' personal data while striking a balance between the employers' legitimate interests and the workers' right to privacy.<sup>30</sup>

The consultation document was met with 'a clear divergence' of views: while employers' organizations dismissed the proposed framework as 'premature',<sup>31</sup> workers' organizations were in favour of the initiative.<sup>32</sup> The Commission dropped the proposal following these divergent responses.

The second attempt was made in 2004 with the Directorate-General Employment and Social Affairs reportedly proposing a draft Directive concerning the processing of workers' personal data and the protection of privacy in the employment context.<sup>33</sup> According to

Paul De Hert and Hans Lammerant, the draft Directive 'was never approved nor even presented to the Commission', the primary reason being the diverging views of social partners, lack of priority, and political compromise.<sup>34</sup>

The last unsuccessful attempt to introduce a European framework of detailed rules on the protection of workers' personal data was made in 2010–12, during the Commission's consultation on the GDPR.<sup>35</sup> In its preparatory works leading to the adoption of the GDPR, the Commission contemplated 'establishing detailed and further harmonised rules for [...] employment relationships'.<sup>36</sup> Among other things, the Commission considered introducing detailed rules on the 'proportionality and legitimacy requirements' and prohibiting 'the processing of data concerning health and the processing of drug and alcohol testing data by the employer [...] subject to limited exceptions'.<sup>37</sup>

### Reasons for failure

Despite these extensive efforts, 'no material changes of data protection rules relating to employment relations (were) proposed' as part of the GDPR.<sup>38</sup> This gives rise to the question of why the EU failed to adopt a harmonized, specialized employee data protection framework. At least three interrelated factors explain this lack of progress.

### Overlap with other areas of law

Data protection in employment relations is inevitably intertwined with other areas of law, which are characterized by the peculiarities of national industrial relations traditions. Data protection in employment relations overlaps with labour law, constitutional law, criminal law, health and safety law, and social security law. Specifically, labour law directly or indirectly influences what data protection in the employment context should look like. It is for this reason that workers' personal data processing is often regulated in the Member States by labour law and collective agreements in addition to data protection law. Discussing the necessary

27 Recommendation No R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes 1989; Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment.

28 ILO Code of practice on the protection of workers' personal data 1997.

29 Art 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final WP 48.

30 European Commission, 'Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data' (2002) 9.

31 'Commission's Second-Stage Consultation on the Protection of Workers' Personal Data' (UNICE 2003).

32 European Commission (n 30).

33 Paul De Hert and Hans Lammerant, 'Protection of Personal Data in Work-Related Relations' (European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 2013).

34 Ibid 25.

35 See 'Commission Staff Working Paper SEC(2012) 72 Final' (European Commission 2012).

36 See *ibid* 47.

37 See *ibid* 48.

38 See *ibid* 150.

interaction between labour law and data protection law, the WP29 observed that:

data protection law does not operate in isolation from labour law and practice, and labour law and practice does not operate in isolation from data protection law. This interaction is necessary and valuable and should assist the development of solutions that properly protect workers' interests.<sup>39</sup>

The overlap between data protection in employment relations and labour law complicates efforts to harmonize the former at the Union level. This is particularly true as the issue of employment is particularly complex and regulated in detail at the national level.<sup>40</sup> Harmonizing data protection in employment relations could also be undesirable in some instances, notably where it upsets domestic laws that are more favourable to employees. In other words, finding a common approach at the Union level could mean identifying the lowest common denominator and thereby undermining more protective national laws.<sup>41</sup> For instance, German workers and trade unions are often reluctant to support a harmonized European framework due to the fear that their co-determination rights guaranteed under domestic law could be undermined.<sup>42</sup> A strong desire to maintain such national peculiarities complicates the efforts to harmonize workers' data protection legislation at the EU level.

It is also important to note that the regulation of data protection issues through labour law and vice versa could result in the emergence of legal lacunae, because data protection law is too generic to cover specific issues arising in employment relations, and conversely, labour law is too specific to address all data protection issues that could arise in the employment context. To the extent that labour laws are not designed to comprehensively address data protection issues, most data processing activities in the employment context fall outside the realm of data protection legislation.<sup>43</sup> Hence, the need for sectoral employment-specific data protection legislation.

### The need for flexibility

Another challenge in establishing an EU-level framework is the need for national flexibility. For instance, allowing

for more flexible and responsive adaptations at the national level was one of the reasons behind the Commission dropping the idea of proposing detailed and harmonized rules for employment relationships as part of the GDPR.<sup>44</sup> The fact that the regulation of data protection in employment relations is left to Member State competence means that the Member States have the flexibility to adopt or amend rules as they see fit to reflect their practices, changing circumstances, and national sensitivities. In their response to the Commission's consultation document launched in 2001, all employers' organizations also emphasized the merits of flexibility, arguing that the rules should be adaptable to diverse contexts.<sup>45</sup>

An EU-level framework, in contrast, would be less responsive to rapidly changing circumstances. As the Commission noted, an EU-level framework 'would increase the risk of the rules becoming outdated and ineffective very quickly in view of rapid technological and economic development'.<sup>46</sup> Furthermore, detailed and harmonized rules for employment relationships 'would not be easily accepted at the national level as it would not leave enough flexibility for national social norms and cultural specificities'.<sup>47</sup> Considering the merits of flexibility, the Commission concluded that leaving specific rules for data protection in employment relations to Member State competence may well be 'more beneficial'.<sup>48</sup>

### Constitutional tensions and lack of political compromise

The feasibility of adopting EU employment-specific data protection legislation also raises sensitive and complex political questions.<sup>49</sup> If anything, the failed attempts highlighted above demonstrate the unlikelihood of stakeholders reaching a consensus around what employment-specific data protection legislation should look like. Revealing such a lack of political agreement, Marian Müller also points out that the proposal of the European Parliament to lay down concrete minimum standards for employee data protection as part of the GDPR 'failed due to the opposition of the member states'.<sup>50</sup>

39 Art 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final WP 48.

40 On the difficulties in harmonising data protection in employment relations, see De Hert and Lammerant (n 33).

41 On the difficulties of transplanting collective aspects of labour law, see Kahn-Freund (n 20).

42 Robert G Schwartz Jr, 'Privacy in German Employment Law' (1992) 15 *Hastings Int'l & Comp L Rev* 152.

43 Art 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context (WP 48) 13 Sept 2001 [noting that 'not all problems that arise in the employment context and

involve the processing of personal data are exclusively data protection ones'].

44 See 'Commission Staff Working Paper SEC(2012) 72 Final' (n 35) 71.

45 European Commission (n 30).

46 See 'Commission Staff Working Paper SEC(2012) 72 Final' (n 35) 112.

47 See *ibid* 73.

48 See *ibid* 112.

49 For detailed analysis on the political processes involved, see De Hert and Lammerant (n 33).

50 Müller (n 7) 179.

The lack of compromise and political sensitivity maps onto the last key factor militating against the introduction of a harmonized employee data protection framework at the EU level: the constitutional tension between EU law and Member State laws. This constitutional tension comes from the principle of ‘conferral’, which dictates that the EU can only act within the limits of the legislative competence given to it by the Member States.<sup>51</sup> Due to the politically sensitive issues they involve, labour laws largely fall outside the legislative competence of the EU.<sup>52</sup> According to Article 153(1) of the Treaty on the Functioning of the European Union (TFEU), the EU has only ‘supporting competence’ in several aspects of employment matters. This is particularly true with regard to the collective aspects of labour law such as co-determination rights, which are ‘linked with the political organisation of a society’, and are hence difficult to ‘transplant’.<sup>53</sup>

### ‘Opening Clause’ as a compromise solution

Due to the combination of these legal, pragmatic, political, cultural, and constitutional reasons, the introduction of a harmonized, employment-specific data protection legislation at the EU level is unlikely, at least in the short term. Article 88 thus emerged as a pragmatic compromise.

### The limits and requirements of Article 88

The opening clause can be broken down into two elements, serving different purposes: a permissive and a conditional dimension, as set out in Article 88(1) and Article 88(2) respectively.

Article 88(1) sets out the permissive or enabling aspect, opening up ‘room for Member States to create laws governing the relationship between the GDPR and national employment law’.<sup>54</sup> This addresses the problems identified in ‘Reasons for failure’ section above by allowing regulatory diversity and protecting Member State autonomy.<sup>55</sup> Utilizing this permissive approach, the Member States have the legislative discretion to

provide specific rules addressing employee data processing through their national regulatory choice.

It is framed as follows:

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organization of work, equality and diversity in the workplace, health and safety at work, protection of employer’s or customer’s property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

Through this opening clause, the GDPR seeks to achieve four aims. In alignment with some of the distinct features identified in ‘Distinctive features of employee data processing’ section, it (i) recognizes that employee data processing merits specific regulation; (ii) stipulates a range of non-exhaustive data processing activities for which rules could be further specified under national law, covering the entire employment lifecycle from recruitment to termination; (iii) explicitly identifies collective agreements as alternative instruments in which such rules might be articulated; and (iv) recognizes for the first time the collective rights and benefits of employees, which were once treated exclusively under the realm of labour law, as data protection issues.

Theoretically, Article 88 thus seeks to address the tension between the need for a consistent approach to employee data protection throughout the EU and the constitutional issues and national peculiarities that the Member States want to preserve. In practice, it has delivered on this promise in promoting diverse and innovative regulatory approaches at the Member State level, whilst also opening the door for further fragmentation.

51 Jeremias Adams-Prassl and Sanja Bogojevic, *The Great Debates in EU Law* (Macmillan International Higher Education, Red Globe Press 2021) 15 (Noting that ‘The Union has no inherent claim to power or “competence”: it can only act where the Member States have delegated their power to it’); See also Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2012/C 326/01 Arts 2–3.

52 Detlev Gabel and Tim Hickman, ‘Chapter 17: Issues Subject to National Law—Unlocking the EU General Data Protection Regulation’ (*White & Case LLP*, 5 April 2019) <<https://www.whitecase.com/publications/article/chapter-17-issues-subject-national-law-unlocking-eu-general-data-protection>> accessed 29 March 2022.

53 Kahn-Freund (n 20) 21–22.

54 Gabel and Hickman (n 52) 7; See also Müller (n 7) 273.

55 Stephen Weatherill, ‘The Fundamental Question of Minimum or Maximum Harmonisation’ in Sacha Garben and Inge Govaere (eds), *The Internal Market 2.0* (Hart Publishing 2020) 1 <<https://ssrn.com/abstract=3660372>> (arguing that ‘Minimum harmonisation is better suited to promote regulatory diversity and to protect local autonomy’).

## Divergent regulatory choices

The logical outcome of Article 88 is that workers' personal data is now regulated by a patchwork of divergent legislative and quasi-legislative instruments across the 27 Member States, providing varying degrees of protection. Member States may utilize the opening clause through domestic legislation, collective agreements, or a combination of the two (see further the tables in [Annex 1](#)). Considerable national variations also exist regarding the enforcement mechanisms and institutional arrangements. Although national data protection authorities (DPAs) are the bodies with primary responsibility for enforcing and clarifying data protection regimes, employee representatives such as works councils and trade unions also play a crucial role. These divergent regulatory choices, together with the mandatory requirements discussed in 'Substantive content: "suitable and specific safeguards"' section below, demonstrate how the opening clause addresses the competing goals of data processing in the employment context while also respecting Member State traditions as separate but integrated systems.

## Regulatory diversity

Almost all EU Member States have adopted or adapted their national data protection laws following the coming into force of the GDPR.<sup>56</sup> Germany was the first Member State to enact national legislation utilizing Article 88.<sup>57</sup> Slovenia and Finland are two outliers, but for different reasons: while Slovenia is the only EU Member State which has not yet aligned its data protection legislation with the GDPR,<sup>58</sup> Finland has adopted comprehensive (at least in form) and freestanding data protection rules that apply exclusively to employment relations.<sup>59</sup> No specific employee personal data protection legislation exists in the remaining Member States,

although Germany could follow the example of Finland, according to a recently released report.<sup>60</sup>

Eleven Member States do not even include any employment-specific provisions in their respective data protection laws.<sup>61</sup> Even in the Member States that have incorporated specific provisions on employment relations in their general data protection laws, considerable divergence exists in terms of scope and substantive detail. While some Member States (eg Germany, Greece, and Spain) include relatively detailed rules on workers' data processing and go beyond the data practices listed in Article 88(1), others (eg Croatia, France, and Luxembourg) address only specific elements such as biometric data or data practices such as monitoring and surveillance.<sup>62</sup> Still, other Member States (eg Sweden and Denmark)<sup>63</sup> make a simple reference to the corresponding GDPR provisions, which neither constitute 'more specific rules' within the meaning of Article 88(1) nor add value in practice, as the GDPR applies in any event. Some national laws (eg German's BDSG<sup>64</sup>) explicitly cover the entire employment lifecycle from application to termination, while others do not have such explicit reference. Only a few Member States (such as Germany, Greece, and Italy) have made explicit reference to Article 88 GDPR in their respective data protection legislation.

Data protection legislation is furthermore not the only mode of regulation for workers' personal data. While some Member States regulate workers' personal data through their respective GDPR implementing legislation, others do so through a patchwork of other sectoral laws and non-statutory regimes. For instance, albeit varied in scope and substance, 17 Member States have incorporated employee data processing provisions in their respective labour laws, most of which predate the GDPR.<sup>65</sup> Considering these various regimes holistically, one can identify that only a small number of countries, such as Cyprus and Malta, do not include

56 Communication from the commission {SWD(2020) 115 final}.

57 Van Eecke Patrick and Anrijs Šimkus, 'Article 88. Processing in the Context of Employment' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020) 1231.

58 A new Slovenian Data Protection Act is currently in the legislative pipeline. See 'Law in Slovenia - DLA Piper Global Data Protection Laws of the World' <<https://www.dlapiperdataprotection.com/index.html?t=law&c=SI>> accessed 27 January 2022.

59 Act on the Protection of Privacy in Working Life (759/2004; amendments up to 347/2019 included).

60 'Bericht des Unabhängigen Beirats zum Beschäftigtendatenschutz' <<https://www.denkfabrik-bmas.de/en/schwerpunkte/beschaeftigtendatenschutz/bericht-des-unabhaengigen-interdisziplinaeren-beirats-zum-beschaeftigtendatenschutz>> accessed 13 February 2022; See also 'German BMAS Publishes Independent Advisory Board's Employee Data Protection Recommendations' <<https://iapp.org/news/a/german-bmas-publishes-independent-advisory-boards-employee-data-protection-rec>

ommendations/> accessed 13 February 2022. The committee of experts was set up by the Federal Ministry of Labour and Social Affairs to examine whether an independent law on employee data protection should be enacted.

61 These Member States are Austria, Belgium, Cyprus, Czech Republic, Estonia, Hungary, Ireland, Latvia, Malta, Portugal, Sweden, and Slovenia.

62 Eurofound, 'Employee Monitoring and Surveillance: The Challenges of Digitalisation' (Publications Office of the European Union, Luxembourg, 2020).

63 Law (2018: 218) with supplementary provisions to the EU Data Protection Regulation, Chapter 2; Danish Data Protection Act 2018, Art 12.

64 Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (DSAnpUG-EU) of 30 June 2017, Art 26(1).

65 Austria, Belgium, Croatia, Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, Luxembourg, Netherlands, Poland, Portugal, Romania, and Slovakia.



## Annex I. Comparing national modes of regulation

Member State	Modes of regulation	
	Does the national data protection law have employment-specific provisions?	What other instruments do regulate personal data processing in the employment context?
<b>Austria</b>	NA (except Processing of images, Art12)	<ul style="list-style-type: none"> <li>• Labour Constitution Act 1974</li> <li>• Labour Contract Amendment Act 1993</li> </ul>
<b>Belgium</b>	NA	<p>4 pre-GDPR collective bargaining agreements:</p> <ul style="list-style-type: none"> <li>• National Collective Bargaining Agreement No 81 on the Protection of Workers' Privacy Regarding Control of Networked Electronic Communication Data (26 Apr 2002)</li> <li>• Collective Bargaining Agreement No 38 on the Recruitment and Selection of Workers (6 Dec 1983)</li> <li>• Collective Bargaining Agreement No 68 on the Protection of Workers' Privacy Regarding CCTV in the Workplace (1998)</li> <li>• Collective Bargaining Agreement No 100 on the Implementation of a Preventive Policy Regarding Alcohol and Drugs Inside the Company (1 Apr 2009)</li> <li>• Collective agreement No 39 on the information and consultation with regard to the social consequences of the introduction of new technologies (13 Dec 1983)</li> </ul>
<b>Bulgaria</b>	Art 25	
<b>Croatia</b>	Arts 23, 25 to 30 (employee biometric data, and workplace surveillance)	<ul style="list-style-type: none"> <li>• Employment Act</li> <li>• Occupational Safety Act</li> </ul>
<b>Cyprus</b>	NA	
<b>Czechia</b>	NA	<ul style="list-style-type: none"> <li>• Labour Code Sec 316(4) prohibits employers from requesting employee information not directly related to work performance and the employment relationship directly or from a third party</li> </ul>
<b>Denmark</b>	Art 12	<ul style="list-style-type: none"> <li>• The Salaried Employees Act</li> <li>• The Health Information Act</li> <li>• The Anti-Discrimination Act</li> <li>• Video Surveillance Act 2018</li> </ul>
<b>Estonia</b>	NA	<ul style="list-style-type: none"> <li>• Employment Contracts Act</li> <li>• Occupational Health and Safety Act</li> </ul>
<b>Finland</b>	Art 30 DPA	<ul style="list-style-type: none"> <li>• Act on Electronic Communications Services (917/2014)</li> </ul>
<b>France</b>	Article 44(4), Amended FDPA 2019) on biometric data	<ul style="list-style-type: none"> <li>• French Labour Code</li> </ul>
<b>Germany</b>	Art 26 (1-4) of the Federal Data Protection Act 2017	<ul style="list-style-type: none"> <li>• Works Constitution Act (BetrVG) 2017</li> <li>• Collective Agreements Section 26(4), BDSG</li> </ul>
<b>Greece</b>	Art 27, Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data,	
<b>Hungary</b>	NA	Labour Code
<b>Ireland</b>	NA	<ul style="list-style-type: none"> <li>• The Organisation of Working Time Act 1997.</li> <li>• The Safety, Health and Welfare at Work Act 2005.</li> <li>• The Employment Equality Act 1998.</li> </ul>

Continued

Table 1. Continued

Member State	Modes of regulation	
	Does the national data protection law have employment-specific provisions?	What other instruments do regulate personal data processing in the employment context?
<b>Italy</b>	Art 2-sexies, Arts 111, 113, 114, 115 Legislative Decree no 196/2003	<ul style="list-style-type: none"> <li>the Statute of Workers Law no 300/1970</li> </ul>
<b>Latvia</b>	NA	<ul style="list-style-type: none"> <li>Latvian Labour Law</li> </ul>
<b>Lithuania</b>	Art 5, Lithuania's Law on Legal Protection of Personal Data No XIII-1426 (pre-employment, video surveillance)	<ul style="list-style-type: none"> <li>Labour of the Republic of Lithuania 2017 (Art 27, 52, 206)</li> </ul>
<b>Luxembourg</b>	Arts 14, 66, 71 (amends Labour law): electronic surveillance, genetic, biometric data, health data	<ul style="list-style-type: none"> <li>Luxembourg Labour law</li> </ul>
<b>Malta</b>	NA	
<b>Netherlands</b>	Art 30(1), 33(3), Implementation Act General Data Protection Regulation 2018	<ul style="list-style-type: none"> <li>Works Council Act 2018</li> </ul>
<b>Poland</b>	The Act of 10 May 2018 on the Protection of Personal Data, Art 111, Amends labour law to specify workplace monitoring, consent, special categories, biometric data, specify what categories of employee and candidate personal data employers can process	<ul style="list-style-type: none"> <li>Labour code (also relevant are The Social Security Act 1998, and The Social Benefits Fund Act 1994)</li> </ul>
<b>Portugal</b>	Art 28 Law No 58/2019	<ul style="list-style-type: none"> <li>Labour Code Law No 7/2009 and</li> <li>other sectoral legislation (Articles 28(1), (2), Portuguese Law) art,17,18</li> </ul>
<b>Romania</b>	Art 5, Law no 190/2018	<ul style="list-style-type: none"> <li>Romanian Labour Code Law No 53/2003</li> </ul>
<b>Slovakia</b>	Sec 78(3), Act No 18/2018 Coll. on Personal Data Protection and on Amendments to Certain Acts	<ul style="list-style-type: none"> <li>The Labour Code .</li> <li>Act No 307/2014 Coll. on Reporting of Anti-Social Activities, as amended.</li> <li>Act No 461/2003 Coll. on Social Insurance, as amended.</li> <li>Act No 595/2003 Coll. on Income Tax, as amended</li> </ul>
<b>Slovenia</b>	NA	NA
<b>Spain</b>	Arts 22, 24, 87–91 Organic Law 3/2018, (use of employer-provided media, right to disconnect, workplace surveillance, whistle-blower)	<ul style="list-style-type: none"> <li>Royal Legislative Decree 1/1995, of 24 March 1995, the Workers' Statute</li> <li>Royal Decree Law (RDL) 9/2021 (Riders law)</li> </ul>
<b>Sweden</b>	NA	<ul style="list-style-type: none"> <li>Camera Surveillance Act 2018</li> <li>collective bargaining agreements (see Video Surveillance Act 2018: 1200)</li> <li>Employment (Co-Determination in the Workplace) Act (1976:580)</li> </ul>

any employment-specific provisions in either their respective data protection law or labour law.

A closer examination of the national regulatory instruments thus reveals that most Member States have utilized the opening clause, albeit in different ways and to different extents. Domestic regimes regulate employee data processing through a combination of omnibus data protection laws, labour law, and other sectoral legislation (such as social security laws, occupational health and safety laws, employment equality laws, and electronic communications laws).<sup>66</sup> In this regard, it can be argued that the opening clause has delivered on its promise to promote regulatory diversity at the Member State level and in addressing the legal, political, and constitutional tensions discussed in 'Reasons for failure' section above.

### The Collective dimension

Article 88(1) also allows Member States to regulate employee data processing through collective agreements. Member States taking advantage of this approach include Spain, Belgium, Germany, Austria, Sweden, Denmark, and the Netherlands. Collective agreements can be negotiated at national, industry, or company levels. For unionized workers, trade unions or employers' associations negotiate the terms of such agreements based on the requirements set out under domestic law.<sup>67</sup> Collective agreements can be negotiated either through collective bargaining between an employer/employers' association and a trade union or between an employer and works council (if provided for by national law) representing the employees of said employer.<sup>68</sup>

For instance, the Spanish Organic Law 3/2018 leaves the modalities of exercising the 'right to disconnect' in the workplace to collective bargaining or, in the absence of it, to agreement between the company and the workers' representatives.<sup>69</sup> Article 91 of the Organic Law also provides that 'Collective agreements may establish additional guarantees of the rights and freedoms related to the processing of personal data of workers and the safeguarding of digital rights in the workplace'.<sup>70</sup> In Belgium, at least four collective agreements regulate different aspects of data processing in the employment

context.<sup>71</sup> Germany is another Member State that regulates the processing of workers' personal data, including special categories of data, through collective agreements. Section 26(4) of Germany's Federal Data Protection Act (BDSG) provides that '[t]he processing of personal data, including special categories of personal data of employees for employment-related purposes, shall be permitted on the basis of collective agreements'.<sup>72</sup>

While the GDPR recognizes collective agreements as alternative regulatory instruments, their practical value in the effective implementation of data protection laws in the workplace is more relevant in countries with high union density.<sup>73</sup> Furthermore, the binding effect and legal significance of collective agreements vary across countries.<sup>74</sup>

### Institutional arrangements: the role of workers' representatives and DPAs

National DPAs are the main institutions entrusted with ensuring the effective application of data protection rules across all sectors. When it comes to employment matters, however, many national DPAs often lack the legitimacy and interest to do so. These legitimacy and interest issues are particularly significant in light of the extensively reported gap between the resources and expertise required to enforce the GDPR, and those available to DPAs.<sup>75</sup> The 'legitimacy problem'<sup>76</sup> of DPAs comes from the collective aspects of the workplace, which often fall outside the realm of data protection law. This means that DPAs cannot effectively enforce data protection laws in the workplace without the involvement of social partners.

Compounding the legitimacy problem is the lack of interest on the side of DPAs to prioritize data protection in the employment context. In a recent report, Justin Nogarede found that 'many DPAs do not consider the workplace a priority domain for their enforcement activities'.<sup>77</sup> A survey by the Future of Privacy Forum also revealed that of the 12 European DPAs involved in their study, only three featured employment as strategic and operational priorities.<sup>78</sup> Nogarede provides a telling illustration of such a lack of priority: the Berlin DPA failed to act for over a year after concerns were raised

66 See Annex 1.

67 Sanjay Sharma, *Data Privacy and GDPR Handbook* (Wiley 2020) 312.

68 Voigt and von dem Bussche (n 3) 226; On the difference between trade unions and works councils, see Schwartz Jr (n 38).

69 Organic Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Digital Rights, Art 88(2).

70 Ibid.

71 These are Collective Bargaining Agreement No 38 (1983), Collective labour agreement No 68 (1998), Collective Bargaining Agreement No 81 (2002), and Collective Bargaining Agreement No 100 (2009).

72 Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (DSAnpUG-EU) of 30 June 2017.

73 Nordic countries such as Denmark, Finland, and Sweden have the highest trade union density (64.7%) in Europe. See Torsten Müller, 'Collective Bargaining Systems in Europe: Some Stylised Facts' (ETUI 2021).

74 See *ibid*.

75 See generally Nogarede (n 15).

76 De Hert and Lammerant (n 33) 6, 10.

77 Nogarede (n 15) 18.

78 Cited in *ibid*; See also Charlotte Kress, Rob Van Eijk and Gabriela Zanfir-Fortuna, 'New Decade, New Priorities: A Summary of Twelve European Data Protection Authorities' Strategic and Operational Plans for 2020 and Beyond' (Future of Privacy Forum, 12 May 2020).

publicly about an employee performance system deployed by a private company called Zalando. Even when the DPA eventually acted, it did not impose any fines on the company, despite finding non-compliance with the GDPR.<sup>79</sup>

The vacuum created by DPAs' lack of legitimacy and interest can be filled, at least in part, by workers' representatives. These organizations are best placed to uphold data protection rules at the workplace and have the incentives, interest, resources, and legitimacy to do so. Workers' representatives also have the expertise to identify the data protection risks that their members might encounter, assess the origin, nature, likelihood and severity of these risks, and articulate solutions to mitigate such risks. The European Commission has long recognized the need for the involvement of workers' representatives to ensure the effective application of data protection rules. In its first attempt to introduce a European framework on workers' personal data protection, the Commission noted that:

Important as the individual rights of workers are, taking into account the specificity of the employment context, the effectiveness of their protection relies to a great extent on collective rights regarding involvement of workers' representatives in the processing of workers' personal data.<sup>80</sup>

The role of employee representative organizations in data protection has recently received more traction, specifically in the context of algorithmic systems. For instance, both the Spanish Royal Decree-Law 9/2021 (also known as Riders law) and the EU Draft Directive on Platform work make it mandatory for platform companies to inform the employees' legal representatives of the parameters, rules, and instructions used as a basis for the algorithms or artificial intelligence systems.

However, the role, scope of involvement, and significance of employee representative organizations vary across the Member States (see [Annex 2](#)). For instance, while works councils or other workplace employee representatives in Austria, Germany, Sweden, Italy, and Croatia have agreement or co-determination roles over the introduction and/or use of new technologies for monitoring purposes, this role is limited to mere consultative or participatory function in other countries such as France and Finland.<sup>81</sup> In most other Member

States, works councils are either non-existent or their involvement in data protection is minimal.<sup>82</sup>

The German and Austrian labour systems are particularly notable for providing a wide range of rights to works councils in protecting employees' personal data. For instance, the German Works Constitution Act 1972 (BetrVG) requires employers which have more than five full-time workers to allow for the establishment of employee-represented works councils.<sup>83</sup> The works councils have the general responsibility to, among other things, ensure the effective implementation of statutory instruments (including data protection), safety regulations and collective bargaining agreements and works agreements concluded for the benefit of the employees.<sup>84</sup> The works councils play this 'watchdog role'<sup>85</sup> through a wide range of co-determination, participation, consultation, and information rights. The works councils have 'the right to be informed about most aspects of the employer's operations'.<sup>86</sup> Section 80(2) of the Works Constitution Act requires the employer to provide the works council with any information necessary to discharge the council's duties.<sup>87</sup> Furthermore, the employer must grant the works council 'access at any time to any documentation it may require for the discharge of its duties'.<sup>88</sup> However, the participation and information rights of the works council do not lead to a binding decision on the employers.<sup>89</sup>

Works councils also enjoy co-determination rights through which they can veto decisions of the employer in certain situations.<sup>90</sup> Pursuant to section 87 of the Works Constitution Act, the introduction and use of technical devices designed to monitor the behaviour or performance of the employees are illegal unless an agreement called a 'works agreement' is reached between the employer and the works council. This provision is often interpreted broadly to include the introduction of any technology that may potentially be used to collect or store the personal data of employees as such collection often leads to monitoring employees.<sup>91</sup> The works council has the right to stop any activity by the employer that requires mandatory co-determination.<sup>92</sup> In cases where no agreement is reached, the works council has the right to injunctive relief.<sup>93</sup>

79 Nogarede (n 15) 17.

80 European Commission (n 30) 11.

81 For more details on this, see Eurofound (n 62).

82 Nogarede (n 15) 28.

83 Works Constitution Act 1972 (BetrVG) s 1.

84 Ibid 80(1)1.

85 Schwartz Jr (n 42) 151.

86 Ibid 152.

87 BetrVG s 80(2).

88 Ibid.

89 Voigt and Bussche (n 68) 227.

90 Schwartz Jr (n 42) 154.

91 For some of the examples that would trigger co-determination rights, See Voigt and Bussche (n 68) 228. Also BetrVG s 87(1) No 14, 94.

92 The veto may only be overridden by a ruling of a mediation committee.

93 BetrVG s 87(2).



## Annex 2. The role of works councils in employee data protection

Member State	The works council's role in protecting employees' personal data
<b>Austria</b>	<p>Works councils have a range of data protection-related rights under the <i>Labour Constitution Act</i> 1974 including:</p> <ul style="list-style-type: none"> <li>• <b>Co-determination rights:</b> the introduction of control measures and technical systems to control workers that affect the human dignity of workers require the approval of the works council to be legally effective (sec 96(1)).</li> <li>• <b>informational:</b> employers are required to inform the works council of the types of personal employee data they hold, and upon request, the bases for processing (sec 91)</li> <li>• <b>monitoring:</b> the Works council has the right to monitor compliance with the legal provisions affecting employees (Sec 89)</li> <li>• <b>advisory/consultation:</b> employees must consult the works council on a range of issues that can have data protection implications (Sec 90-92)</li> </ul>
<b>Germany</b>	<p>Under the <i>Works Constitution Act</i> (BetrVG), works councils have:</p> <ul style="list-style-type: none"> <li>• <b>Co-determination rights</b> in the introduction and use of technical devices designed to monitor the behaviour or performance of the employees (Sec 87), Staff questionnaires, and assessment criteria (Secs 87, 91, 94, 99,102).</li> <li>• <b>Participation, information, and consultation rights:</b> the employer has to inform the works council in due time of any plans concerning . . .working procedures and operations including the use of artificial intelligence (Sec 90, Sec 80(2))</li> <li>• <b>Monitoring</b> the effective application of law including data protection laws, and collective agreements (Sec 80(1))</li> </ul>
<b>France</b>	<p>The Labour Code provides:</p> <p>The social and economic committees have <b>information and consultation rights over:</b></p> <ul style="list-style-type: none"> <li>• the use of the methods or techniques for assisting the recruitment of candidates for employment as well as of any modification thereof,</li> <li>• the introduction of automated processing of personnel management and of any modification thereof, and</li> <li>• the decision to implement the means or techniques allowing control of the activity of the employees (Art L. 2312-38)</li> </ul> <p>The works councils have <b>information and consultation rights over</b> the introduction of any new technologies when these technologies are likely to have consequences on employment, qualifications, remuneration, training or working conditions (L2323-29)</p>
<b>Sweden</b>	<p>Employment (Co-Determination in the Workplace) Act Sec 11:</p> <ul style="list-style-type: none"> <li>• employers must obtain the consent of and enter into an agreement with employees' organisations before taking any decision regarding significant changes in working or employment conditions for employees.</li> </ul>
<b>Italy</b>	<p>Statute of Workers Law no 300/1970, Art 4</p> <p>Employers can use monitoring technologies only if</p> <ul style="list-style-type: none"> <li>• monitoring activity is used exclusively for the purpose of organizational and production needs, or occupational safety reasons, or for protecting company's assets, and</li> <li>• a prior collective agreement is reached between the employer and trade unions, or an administrative authorization is obtained</li> </ul>
<b>Croatia</b>	<p>Labour Act (No 758/95): employees' councils have</p> <ul style="list-style-type: none"> <li>• <b>information and consultation</b> rights on decisions that are important for the position of employees, including the 'introduction of new technologies and change of organization and methods of work' Art 145(1), (2)</li> <li>• <b>co-determination</b> rights over the 'collection, processing, use and forwarding to third persons of information concerning an employee' Art 146(1). Co-determination is required for continuous monitoring.</li> </ul>

Similar to the German system, the Austrian Labour Constitution Act 1974 grants works councils co-determination, participation, consultation, and information rights over a wide range of issues, including workers' personal data protection.<sup>94</sup> Works councils have the right to monitor the implementation of, and compliance with, the legal provisions, collective agreements, and works agreements affecting a company's employees.<sup>95</sup> In order to carry out these responsibilities, the works councils have information rights, and the employer is legally required to inform works councils of a range of issues including the types of personal employee data the employer is processing.<sup>96</sup>

According to Section 96(1)3 of this Act, works councils furthermore enjoy veto powers over 'the introduction of control measures and technical systems for the control of workers, which affect human dignity'. Co-determination rights under the Austrian system can be triggered only when the monitoring measure touches on human dignity. In other words, the employer can unilaterally implement data processing monitoring systems that do not affect the human dignity of the employee.<sup>97</sup> Therefore, the scope of co-determination rights under the Austrian system can be broad or narrow depending on the interpretation of what constitutes 'touching human dignity'.<sup>98</sup>

French law, on the other hand, represents a good example of a system where the role of workers' representatives is limited to a merely consultative function. Although the Labour Code allows for the establishment of several workers' representative bodies,<sup>99</sup> they do not enjoy co-determination rights, unlike their German and Austrian counterparts. For instance, the Labour Code requires employers to inform and consult the social and economic committee and works councils prior to making significant decisions that affect employees.<sup>100</sup> While consultation of workers' representatives is mandatory, the employer is not legally bound to accept their recommendations.

## Lessons learned

Several lessons can be drawn from the analysis above. First, Article 88(1) (read together with Rec. 155) can be characterized as a legislative novelty designed to address (at national level) the collective aspect of employee data processing. By permitting collective agreement as a possible regulatory instrument and thereby recognizing the collective rights and benefits related to employment relations as data protection issues, the opening clause paves the way for the collective exercise of data protection rights in the workplace. It also provides the opportunity to bring worker representatives to the decision-making table in matters of data protection.<sup>101</sup> Secondly, it recognizes and promotes regulatory diversity. The opening clause thus enables Member States to maintain their regulatory peculiarities and legal traditions and enjoy 'the necessary flexibility [...] to adapt their domestic labour framework and traditions to the new EU data protection regime'.<sup>102</sup> This in turn would also help to address the political sensitivities and legislative competency issues identified above. Considering the politically sensitive matters of data protection in employment matters, the opening clause is often described as a 'pragmatic approach',<sup>103</sup> whereby Member States are given the discretion to adopt specific rules subject to the minimum standards of the GDPR.

The opening clause has a further benefit: it enables and encourages 'regulatory experimentation and learning'.<sup>104</sup> Such experimentation is particularly evident in national systems where works councils play a special role in upholding data protection laws in the workplace through co-determination rights. Drawing on these best practices, there are calls for all the Member States to introduce and enforce co-determination into their respective labour laws.<sup>105</sup> The regulatory experimentation is also evident in some of the recently introduced 'responsive solutions to the emergence of new instruments and practices that may significantly affect workers'.<sup>106</sup> Two recent Spanish legal instruments are of particular note in this respect: The Spanish Riders Law 9/2021 and

94 Labour Constitution Act 1974 ss 89, 90, 91, 92, 96.

95 Ibid 89.

96 Ibid 91.

97 Eurofound (n 62) 16.

98 Austrian jurisprudence interprets the concept of 'human dignity' in accordance with EU law, specifically Art 8 of the ECHR. For this reason, any processing of employees' personal data can affect human dignity. 'European & Middle East Guide to Monitoring of Employees in the Workplace' (Meritas Law Firms Worldwide 2018) 2.

99 For details on this, see Voigt and Bussche (n 68) 229.

100 Code du travail, Art L 2312-38. Art L2323-2.

101 Valerio De Stefano and Antonio Aloisi, 'Artificial Intelligence and Workers' Rights' (*Social Europe*, 8 November 2021) <<https://socialeu>

[rope.eu/artificial-intelligence-and-workers-rights](https://rope.eu/artificial-intelligence-and-workers-rights)> accessed 19 January 2022.

102 Chakarova (n 7) 42.

103 'REPORT on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (COM(2012)0011 C7-0025/2012 2012/0011(COD))' (Committee on Civil Liberties, Justice and Home Affairs 2013) 199.

104 Weatherill (n 55) 19.

105 Mihalīs Kritikos, 'Data Subjects, Digital Surveillance, AI and the Future of Work' (European Parliament's Panel for the Future of Science and Technology 2020) 92.

106 Stefano and Aloisi (n 101).

Organic Law 3/2018 introduce (i) new disclosure obligations on platform companies using algorithmic management,<sup>107</sup> and (ii) novel regulatory lessons on the ‘right to disconnect’<sup>108</sup> respectively. As a legislative process, the pragmatic compromise also facilitated consensus on the rest of the provisions of the GDPR.<sup>109</sup> Therefore, one can argue that the permissive clause under Article 88(1) has delivered on some of its promises.

## Substantive content: ‘suitable and specific safeguards’

Diversity of regulatory models and instruments is to be welcomed in principle: but to what extent do national regulatory instruments provide adequate protection for workers’ personal data? In particular, what substantive requirements must national rules meet in order to be regarded as ‘suitable and specific safeguards’ within the meaning of Article 88(2)? Member States have a wide discretion to determine the specific rules regulating workers’ personal data processing—but they are not completely free to do so. This is where the conditional aspect of the opening clause arises. By setting out specific substantive requirements, the conditional aspect stipulated under Article 88(2) serves as a ‘safety valve’ to ensure that the extensive use of the opening clause does not undermine the overall objectives of the GDPR.<sup>110</sup> Article 88(2) stipulates that:

[National] rules shall include suitable and specific measures to safeguard the data subject’s human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing [...] and monitoring systems at the workplace.

Two crucial questions that arise from the opening clause itself must be addressed before examining the adequacy of specific national rules. The first relates to the extent to which domestic law can deviate from the GDPR as

regards the level of specification and safeguards: does the opening clause permit Member States to enact stricter and more protective rules than those provided for in the GDPR? This question emanates from the requirement of ‘more specific rules’ under Article 88 and the lack of clarity thereof. It remains nebulous whether the requirements of ‘more specific rules’ are only meant to clarify and concretize the provisions of the GDPR in employment matters or whether more stringent rules could also be introduced.

Marian Müller argues that the Member States can go beyond the level of protection of the GDPR.<sup>111</sup> analysed thus, the opening clause under Article 88 is a ‘strengthening’ or ‘reinforcement’ clause.<sup>112</sup> This interpretation can be inferred from multiple sources including relevant provisions of the TFEU, the objectives of the GDPR, its legislative history, relevant labour law provisions, and the functions of minimum harmonization measures.<sup>113</sup>

Therefore, while the Member States are free to adopt diverse regulatory mechanisms, the substantive content of these regulatory models can either stick to the minimum requirements of the GDPR or provide stricter and more protective provisions.<sup>114</sup>

This takes us to the second substantive question: what are ‘suitable and specific measures’ within the meaning of Article 88(2)? The GDPR does not provide clear guidance as to how these substantive requirements and standards should be interpreted and transposed into the national provisions. The notion of ‘suitable and specific measures to safeguard the data subject’s human dignity, legitimate interests and fundamental rights’ is left undefined.<sup>115</sup> This lack of clarity prompted the Administrative Court of Wiesbaden (Germany) to ask the Court of Justice of the European Union (CJEU) to clarify whether German domestic data protection law complies with Article 88 of the GDPR.<sup>116</sup> The referring court has sought a preliminary ruling on whether Paragraph 23(1) of the Law of Land Hessen on the

107 Draft Directive on Platform work, Art 9.

108 Organic Law 3/2018, Art 88(2).

109 Paul Nemitz, presentation at Algorithms at Work Reading Group, Oxford (20 Jan 2022).

110 Art 88 (3) also sets out a formal notification obligation. At time of writing, 17 Member States (Austria, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Lithuania, Luxembourg, Poland, Romania, and Slovakia) have so far notified the Commission of their respective national provisions. See ‘EU Member States Notifications to the European Commission under the GDPR’ (n 9).

111 Müller (n 7) 152.

112 Ibid 178 et seq. Art 9(4) GDPR is another ‘strengthening’ clause.

113 TFEU, Art 153(4); European Parliament, Draft report on the proposal for a regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service

providers for the processing of personal and other data for the purpose of combatting child sexual abuse online, PE661.791v01-00 2020; Council Directive 2001/23/EC of 12 March 2001 on the approximation of the laws of the Member States relating to the safeguarding of employees’ rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses, Art 8; Weatherill (n 55).

114 According to Paul Nemitz, even though the Member States often ask for broad opening clauses under the pretext of doing more at a national level, most member states have neither availed themselves of the opportunity to do so nor pushed for a stronger EU framework. Paul Nemitz, presentation at Algorithms at Work Reading Group, Oxford (20 Jan 2022).

115 The provision only mentions three examples that should be addressed by Member State laws or collective agreements.

116 Referral C-34/21 (*Hauptpersonalrat der Lehrerinnen und Lehrer*, 20 Jan 2021) (CJEU). <<https://curia.europa.eu/juris/showPdf.jsf?text=&docid=238481&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=26537418>> accessed 20 March 2022.

protection of data and freedom of information (HDSIG),<sup>117</sup> which provides specific rules for personal data processing in the employment context, meets the requirements stipulated under Article 88 GDPR. Arguing that ‘Article 88(2) of the GDPR has [...] not been transposed into the national provisions’, the referring court asked the following two questions:<sup>118</sup>

- Is Article 88(1) of the GDPR to be interpreted as meaning that, in order to be a more specific rule for ensuring the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context within the meaning of Article 88(1), a provision must meet the requirements imposed on such rules by Article 88(2)?
- If a national rule clearly does not meet the requirements under Article 88(2) of the GDPR, can it nevertheless remain applicable?

The hearing of the case took place in the CJEU’s Grand Chamber on the 30th of June 2022.<sup>119</sup> Although the exact date is not determined, one would expect that the court will soon deliver its decision. The scene is thus set for a framework on how the requirements under Article 88(2) GDPR should be interpreted and transposed into national rules, well beyond Germany’s HDSIG. The request for a preliminary ruling furthermore provides a prime opportunity to address existing tensions between the need for an equal level of protection to employees across the Union and diverse regulatory approaches adopted at the national level. The Court of Justice is also expected to interpret what constitutes ‘suitable and specific measures’ within the meaning of 88(2) and flesh out a concrete framework for interest balancing. In doing so, the CJEU should draw useful lessons from existing regulatory instruments,<sup>120</sup> other provisions of the GDPR itself,<sup>121</sup> and case law.

The WP29’s Opinion 2/2017 is particularly instructive in this regard: it explicitly provides ‘guidelines for the legitimate use of new technology in a number of specific situations, detailing suitable and specific measures to safeguard the human dignity, legitimate interest

and fundamental rights of employees’.<sup>122</sup> The Opinion establishes a set of principles, outlines a list of risks posed by new technologies, and provides a framework for proportionality assessments in several scenarios. It also offers a useful guide and concrete examples about what could constitute ‘legitimate monitoring activities and the acceptable limits of workers’ surveillance by the employer’.<sup>123</sup>

Similar proportionality requirements and principles can be drawn from the jurisprudence of the ECtHR. For instance, in its landmark privacy ruling in *Bărbulescu v Romania*, the ECtHR found that ‘domestic authorities should ensure that the introduction by an employer of measures to monitor correspondence and other communications, irrespective of the extent and duration of such measures, is accompanied by adequate and sufficient safeguards against abuse’.<sup>124</sup> The Court then set out a list of criteria that employee monitoring must meet in order to be proportionate, including prior notification, limits on the extent of the monitoring and the degree of intrusion, a legitimate interest, necessity, consequences for the employee, and adequate safeguards.<sup>125</sup> In addition to these principles, useful frameworks can be found in information and consultation requirements. The Council of Europe’s Recommendation, the ILO’s Code of Practice, and the Commission’s recently proposed Directive on Platform Work all include specific provisions as regards information and consultation with employees’ representatives in accordance with domestic law or practice.<sup>126</sup>

Amongst the principles which can be drawn from these instruments, four overarching normative requirements stand out:

- that workers’ personal data should be processed only for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes (the principle of finality);
- that the processing must be strictly necessary for these legitimate purposes and proportionate to the risks faced by the employer (the principle of necessity and proportionality);

117 This provision corresponds to para 26(1) of the German Federal Law on data protection (BDSG).

118 *Referral C-34/21 (Hauptpersonalrat der Lehrerinnen und Lehrer, 20 Jan 2021)* (n 116).

119 See ‘CURIA Judicial Calendar’ <[https://curia.europa.eu/jcms/jcms/Jo1\\_6581/en/?dateDebut=30/06/2022&dateFin=30/06/2022](https://curia.europa.eu/jcms/jcms/Jo1_6581/en/?dateDebut=30/06/2022&dateFin=30/06/2022)> accessed 13 July 2022.

120 For instance, Art 29 Working Party Opinion 2/2017 on data processing at work (WP 249) 8 June 2017; ILO Code of practice on the protection of workers’ personal data 1997; Council of Europe’s Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment.

121 Regulation (EU) 2016/679, Art 5.

122 WP 249 9 [emphasis added].

123 Art 29 Working Party Working document on surveillance and monitoring of electronic communications in the workplace (WP55) 29 May 2002.

124 *ECtHR, Bărbulescu v Romania, Appl No 61496/08* Judgement of 5 September 2017, para 120.

125 *Ibid*, para 121.

126 Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, COM(2021) 762 final Sec 21; ILO Code of practice on the protection of workers’ personal data 1997, Sec 12; Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, sec 21.



- that the employer must inform the employee in advance about the processing operations (the principle of transparency); and
- that workers' representative bodies (if applicable) must be informed and consulted in advance about specific data practices such as monitoring and surveillance (the principle of information and consultation).<sup>127</sup>

The main objective of these criteria is to strike the right balance between mutually legitimate but often conflicting rights and interests. Although employers will often have a multitude of legitimate interests to process workers' personal data, the existence of such 'a legitimate interest' in itself is not sufficient to override the rights and freedoms of employees.<sup>128</sup> Hence, the need for a balancing exercise.

Measuring against the requirements identified above, the remaining part of this section seeks to address the question of whether and how national regulatory instruments provide safeguards for employees' dignity, legitimate interests, and fundamental rights. It does so by focusing on the issues of employee monitoring and consent. The focus on these two issues is purposeful: (i) Article 88(2) requires that specific national rules on the protection of employee data should have particular regard to, among others, monitoring systems at the workplace, and (ii) Recital 155 permits Member States to specify the conditions under which employee data may be processed on the basis of the consent.

### Safeguards with respect to employee monitoring and surveillance

A number of studies have described the protection of domestic norms against intrusive employee monitoring and surveillance, mapping the baseline approach of Member State regulations.<sup>129</sup> But how are the substantive requirements identified in the previous section reflected in national legislation, and what best practices and cautionary lessons can be gleaned?

Belgium stands out as a good example, regulating different types of employee monitoring through collective agreements which provide suitable and specific

measures that fit within the principles outlined above. Collective Agreement (CBA) No. 68 (1998) aims to guarantee respect for the fundamental right of workers to privacy in the employment relationship by determining the purposes and conditions under which video surveillance may be introduced.<sup>130</sup> This collective agreement explicitly spells out the principles of 'finality', 'proportionality', 'transparency', and 'information and consultation' as suitable safeguards for the protection of workers' privacy.

Under the principle of 'finality', the CBA requires workplace monitoring and surveillance to be carried out only for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes. It sets out an exhaustive list of purposes for which workplace monitoring is permitted. Pursuant to Article 4 of CBA No. 68, for instance, camera surveillance at the workplace is permitted only for (i) the protection of health and safety; (ii) the protection of the company's assets; (iii) control of the production process; and (iv) control of the work performed by employees.

The CBA also includes the principles of necessity and proportionality by requiring employers to use video monitoring systems that entail the least possible interference with the private sphere of the worker.<sup>131</sup> The CBA prohibits continuous or permanent monitoring of employees in all circumstances as it would most likely fail to meet the proportionality test.<sup>132</sup> It also imposes information and consultation requirements at both the individual and collective levels. Prior to, and at the start of, any monitoring and surveillance, the employer is required to provide workers' representatives (the works council, the committee for prevention and protection at work, or the trade union delegation, as the case may be) with information on all aspects of the monitoring and surveillance, and specifically on the intended purpose, duration, and scope of monitoring; and whether or not personal data are stored, where, and for how long.<sup>133</sup> Workers' representatives are also tasked with responsibility for regularly evaluating the monitoring systems used and making proposals for revisions in line with technological developments. In all circumstances, workers must be informed beforehand about the existence,

127 Although the principle of information and consultation is common in labour law, it has also recently gained importance in the data protection context. See, for instance, European Commission (n 30); Draft Directive on Platform work. Requirements (i)–(iii) are also principles underpinning the GDPR, and would therefore most likely influence the CJEU's interpretation of Art 88(2); the applicability of the last requirement depends on national law and practice.

128 WP 249 4.

129 Eurofound (n 62); 'European & Middle East Guide to Monitoring of Employees in the Workplace' (n 98).

130 Collective Bargaining Agreement No 81 on the Protection of Workers' Privacy Regarding Control of Networked Electronic Communication Data (26 Apr 2002) Art 1.

131 Collective Bargaining Agreement No 68 on the Protection of Workers' Privacy Regarding CCTV in the Workplace (1998) Art 8.

132 Ibid, arts 2 and 6.

133 CBA No 68, Arts 9–11; CBA No 81, Arts 7–9.

the purpose and the duration of the monitoring. Setting out specific requirements for interest balancing and providing works councils with information and consultation rights, the Belgian system goes beyond the level of protection of the GDPR.

Finland is another Member State with specific measures for ‘camera surveillance in the workplace’ that largely fit within the principles outlined above. The Finnish Act on Protection of Privacy in Working Life provides a strict ‘necessity requirement’ as a precondition for processing employee personal data. According to Section 3 of the Act, the employee is allowed to process personal data that is ‘directly necessary for the employment relationship’. Personal data is directly necessary for the employment relationship if it is connected (i) with managing the rights and obligations of the parties to the employment relationship, (ii) with the benefits provided by the employer for the employee or (iii) arises from the special nature of the work concerned. The most important part of this ‘necessity’ requirement is that it cannot be overridden with the employee’s consent. In the absence of the purposes identified above, processing employee personal data is unlawful even if the employee consents. These generally worded requirements are further concretized under Section 16, which permits camera surveillance in the workplace ‘for the purpose of ensuring the personal security of employees and other persons on the premises, protecting property or supervising the proper operation of production processes, and for preventing or investigating situations that endanger safety, property or the production process’.<sup>134</sup>

Finnish law also requires employers to explore less intrusive means before the introduction of camera surveillance and ensure that the privacy of employees does not outweigh the aim of the measures. The Act also includes specific provisions as regards prior notification of employees and consultation with workers’ representatives in certain circumstances.<sup>135</sup> As shall be highlighted below, this Act prohibits the surveillance of a particular employee or particular employees subject to certain exceptions, and the surveillance of spaces designated for personal use, such as lavatories and changing rooms.<sup>136</sup>

German law, on the other hand, is less concrete in fleshing out the requirements for interest balancing compared to its Belgian and Finnish counterparts. Although often referred to as a ‘gold standard’ for affording works council co-determination rights, there is no clear framework for the balancing exercise.<sup>137</sup> For instance, the German Federal Data Protection Act (BDSG) sets out the purposes for which employee personal data may be processed before, during, and after the employment relationship. Pursuant to Section 26(1) BDSG, for example, the employer may process workers’ personal data where necessary for (i) purposes of entering into, performing, or terminating the employment contract, or (ii) exercise rights and obligations of employees. The BDSG also allows the processing of workers’ data on the basis of collective agreements as long as the negotiating partners comply with Article 88 (2) GDPR.<sup>138</sup> However, this legislation does not go beyond setting out the generally-worded purposes.

For this reason, the German approach is often criticized for not providing a concrete balancing test within the meaning of Article 88(2).<sup>139</sup> For instance, the Administrative Court of Wiesbaden states that the legislation merely cites ‘necessity’ as a legal basis, instead of fleshing out a framework for the balancing exercise.<sup>140</sup> Although both the Law of Land Hessen and the German Federal Law on data protection law (BDSG) stipulate that personal data may be processed if necessary for the purposes of an employment relationship, the referring court argues that the balancing of interests goes beyond mere ‘necessity’ and the legislature fails to stipulate specific provisions for such a balancing exercise.<sup>141</sup> The referring court also notes that mere reference to the specific provision of the GDPR ‘does not achieve anything’.<sup>142</sup>

The recently established Advisory Committee of experts also found Section 26 BDSG to be insufficient, arguing along similar lines: lack of concretization of the necessity criterion. According to the Advisory Committee, ‘[t]t is primarily up to the legislator to weigh up and fairly balance the rights and interests of employees protected by human dignity and other fundamental rights against the rights and interests of

134 Act on the Protection of Privacy in Working Life (759/2004; amendments up to 347/2019 included) Sec 16.

135 Ibid, sec 17 and sec 21.

136 Ibid.

137 The only exception is employees’ personal data processed to detect criminal activities, which requires rigorous interest balancing against specific criteria. See sec 26(1) BDSG.

138 BDSG, sec 26(4).

139 Lukas Middel, ‘Workplace Surveillance in the Light of Employee Data Protection’ (Center for Interdisciplinary Labour Law Studies). [noting ‘it is more than questionable whether the general balancing test that lies behind the necessity requirement of section 26 of the 2017 Act sets out specific rules for the employment context’].

140 *Referral C-34/21 (Hauptpersonalrat der Lehrerinnen und Lehrer, 20 Jan 2021)* (n 116).

141 Ibid.

142 Ibid.

employers protected by fundamental rights<sup>143</sup> and Section 26. BDSG fails to do so. The Committee recommends that a separate law on the protection of employee data is needed within the framework of the possibility opened up by Article 88 of the GDPR.<sup>144</sup> Therefore, although Germany is the first country that has explicitly utilized the opening clause, the BDSG has not provided stricter regulation than the GDPR, except in the case of employee consent.<sup>145</sup>

### Specific safeguards for employee consent

The GDPR gives the Member States the discretion to provide specific rules on employee data processing based on consent. As stipulated under Recital 155 of the GDPR, ‘Member State law or collective agreements, including “works agreements”, may provide for specific rules on the processing of employees’ personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee [...]’. Member States could provide specific conditions under which consent can be used as a legal basis, restrict the use of consent in certain situations, or even prohibit using employee consent altogether if the processing involves sensitive data.<sup>146</sup> They can do so through domestic data protection laws and supervisory authority guidance, labour laws, judicial decisions, and sectoral rules.<sup>147</sup>

Finland stands out among the 27 Member States by explicitly excluding consent as a general ground for the legitimate processing of workers’ personal data. According to the Finnish Act on Protection of Privacy in Working Life, the requirement of strict necessity for employment relations cannot be circumvented even if the employee gives free, specific, informed, and unambiguous consent. This does not mean that the Finnish Act abolishes consent as a lawful basis altogether, but it requires an additional requirement of necessity. Furthermore, ‘written consent’ is a precondition to processing health data<sup>148</sup> and collecting employee personal data from third parties.<sup>149</sup> These

requirements are stricter and far more protective than the GDPR.

In Germany, Section 26(2) of the BDSG provides the criteria for determining whether consent is freely given or not: (i) the employee’s level of dependence in the employment relationship, and (ii) the circumstances under which consent was given. The BDSG considers consent is freely given when it is associated with a legal or economic advantage for the employee, or when both the employer and employee are pursuing the same interests.<sup>150</sup> Although the BDSG provides that consent is considered freely given when the employee pursues his/her own economic advantage, the recently established Committee of experts warns that this justification could risk ‘consent being bought off’.<sup>151</sup> Going beyond the general conditions for consent under Article 7(2) of the GDPR, the BDSG requires employee consent to be in a written form, unless special circumstances dictate otherwise.<sup>152</sup>

Portugal presents an interesting case study that appears to reflect the concerns about employee consent being bought off. The Portuguese national Data Protection Act explicitly prohibits the employer from using consent as a legal basis for processing the employee’s personal data if there is an economic or legal advantage for the employee.<sup>153</sup> Article 28(3) of the Act provides that:

Unless legal rule to the contrary, the worker’s consent does not constitute a requirement for the legitimacy of the processing of his personal data:

- a) If the treatment results in a legal or economic advantage for the worker; or
- b) If such processing is covered by the provisions of Article 6(1)(b) of the GDPR.

Interestingly, this requirement is the exact opposite of the German approach, which considers employee consent to be freely given if there is an economic or legal advantage for the employee emerging from such processing. The underlying assumption behind the Portuguese prohibitive approach seems that employee

143 ‘Bericht Des Unabhängigen Beirats zum Beschäftigtendatenschutz’ (n 56); See also ‘German BMAS Publishes Independent Advisory Board’s Employee Data Protection Recommendations’ (n 56).

144 ‘Bericht Des Unabhängigen Beirats zum Beschäftigtendatenschutz’ (n 56).

145 Müller (n 7) 241.

146 GDPR, Art 9(2)a; For instance, under Order no 146/2019, the Italian DPA prohibits the processing of genetic data by an employer in order to assess the candidate’s application, even with the data subject’s consent. see Laura Spagnoli, ‘The Italian DPA Issued Instructions on the Processing of Special Categories of Data’ (*Martini Manna Law firm*, 16 September 2019) <<https://martinimanna.com/the-italian-dpa-issued-instructions-on-the-processing-of-special-categories-of-data/>> accessed 16 March 2022.

147 ‘Employee Consent Under the GDPR, Practical Law Practice Note w-004-5144’ (*Thomson Reuters, Practical Law*, 2021) <[http://uk.practical-law.thomsonreuters.com/w-004-5144?transitionType=Default&contextData=\(sc.Default\)](http://uk.practical-law.thomsonreuters.com/w-004-5144?transitionType=Default&contextData=(sc.Default))> accessed 15 March 2022.

148 Act on the Protection of Privacy in Working Life, Sec 3.

149 Ibid, sec 4. ‘The employer shall collect personal data concerning the employee primarily from the employee himself or herself’.

150 BDSG s 26(2).

151 ‘Bericht Des Unabhängigen Beirats zum Beschäftigtendatenschutz’ (n 56) [in text quotes removed].

152 BDSG s 26(3).

153 Law No 58/2019 <<https://dre.pt/dre/detalhe/lei/58-2019-123815982>>

consent contingent on any offer or benefits provided by the employer cannot be considered freely given. However, a prohibitive approach could also risk intervening with the rights, freedoms, and interests of the employees. In fact, this concern prompted the Portuguese national DPA to issue a decision suspending the application of Article 28(3)(a) for being excessively restrictive on the employee's right to informational self-determination and for being in contradiction with Articles 6(1)(a) and 9(2)(a) of the GDPR.<sup>154</sup>

## Lessons learned

The foregoing analysis reveals that while many Member State laws include principles such as legality, necessity, and proportionality, some of these laws are generally worded and fail to flesh out concrete frameworks for interest balancing. This means that these laws could be considered inadequate in providing suitable and specific measures to safeguard workers' human dignity, legitimate interests, and fundamental rights within the meaning of Article 88(2). While the Belgian CBA No 68 can be considered a good example of an instrument setting out an exhaustive list of purposes for which workplace monitoring is permitted, for example, providing suitable and specific safeguards for workers and laying down a concrete framework for interest balancing, the German BDSG lacks such particularization.

One can also observe a convergence of Member State laws around a prohibitive approach to some of the most intrusive forms of monitoring and surveillance systems in the workplace. For instance, several Member States explicitly prohibit, as a principle or in all circumstances, intrusive systems such as covert monitoring, constant (both covert and overt) monitoring, and monitoring for the sole purpose of assessing employees' behaviour. Several countries also prohibit video surveillance of private spaces in the workplace such as bathrooms, changing rooms, rest areas, and bedrooms under all circumstances.

Regarding the requirement of consent, a closer look at national laws reveals that Member States follow a wide range of approaches when introducing additional conditions or restrictions on the validity of employee consent. Differences range from excluding consent altogether in certain circumstances to requiring explicit consent, and from written consent (not merely explicit) to implicit consent. This means that while some

Member States provide stricter and more protective measures than the GDPR (eg requiring written consent or excluding it altogether), others either stick to the minimum requirements of the GDPR or remain vague in their specifications.

Member States thus continue to offer differing degrees of protection and safeguards. This divergence is contrary to the fundamental objective of the GDPR to provide for an equal level of protection to individuals across the Union. This divergence could have far-reaching implications for workers, employers, and the functioning of the internal market. The absence of uniform, consistent EU law protecting workers' personal data means that employees are treated differently on the basis of applicable national law.

## Conclusion

Personal data processing in employment matters across the EU is regulated by complex, multi-level, and fragmented systems, drawn from different theories, regulatory models, and sources of law. Such fragmentation exists not only in the regulatory models but also in the degree of substantive protections and safeguards. Contrary to what the GDPR is designed to achieve, data protection rules in the employment context are far from harmonized, consistent, and comprehensive.

For this reason, the legislative compromise under Article 88 can be characterized as a double-edged sword. From a labour law perspective, the opening clause is responsive to the employment-specific needs discussed in Sections 2 and 3 by promoting diverse and at times innovative regulatory approaches. It also fills the gap in the GDPR in addressing the collective dimension of employee data processing, specifically in some Member States that have a strong tradition of involving workers' representatives in the collective governance of workplace data protection. However, the opening clause also invites further fragmentation, legal uncertainty, and inconsistent enforcement, running counter to the fundamental objectives of the GDPR itself.

Although the opening clause seeks to limit such fragmentation by setting specific conditions under Article 88(2), these conditions are met only to varying degrees in the different Member States. Considering such a high level of regulatory fragmentation and differing degrees of protection, the opening clause is yet

154 'CNPD's Deliberation 2019/494' (*Servulo & Associados—Law firm, Portugal*) <<https://www.servulo.com/en/knowledge/CNPDs-Deliberation-2019494/6716/>> accessed 16 March 2022 See also; 'CNPD Issued a Deliberation (Deliberation No 494/2019, of September 3)

Stating That They Will Not Apply Some of the Rules of the Portuguese Law Implementing GDPR' (24 September 2019) <[https://www.garrigues.com/en\\_GB/new/cnps-issued-deliberation-deliberation-no-4942019-september-3-stating-they-will-not-apply-some](https://www.garrigues.com/en_GB/new/cnps-issued-deliberation-deliberation-no-4942019-september-3-stating-they-will-not-apply-some)> accessed 16 March 2022.



to deliver on its promises. However, it has the potential to do so, provided that the pending CJEU case enforces the principles delineated above. In the final analysis, there is a need to strike the right balance between two policy objectives: promoting diverse regulatory approaches and regulatory experimentations in labour law and ensuring consistent implementation,

interpretation, and enforcement of the GDPR. Although Article 88 represents a valiant attempt to reconcile these policy objectives, it only partially achieved the former objective and left the latter unresolved.

*<https://doi.org/10.1093/idpl/ipac015>  
Advance Access Publication 16 August 2022*