MANAGING DATA PROCESSING
IN THE WORKPLACE THROUGH
INDUSTRIAL RELATIONS

Assessment Comparative Report

D2.2

Co-funded by the
European Union

The GDPiR project has received funding from the European Commission under the grant agreement No 101048690. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Document Information

Project Acronym	GDPiR
Grant Agreement	101048690 – GDPiR – SOCPL-2021-INFO-WK
Deliverable number and title	Assessment Comparative Report (D2.2)
Dissemination level	PU – Public
Organisation Name	ADAPT, KU Leuven
Submission date	27.11.2023
Authors	I. Armaroli, D. Gillis, K. Lenaerts, D. Porcheddu
Contributors	E. Bakay, L. Hanulova, J.R. Mercader Uguina, T. Meszmann, L. Moore Blasco, A.B. Muñoz Ruiz, I. Ozgoren Kinli, N. Ramos Martin, A. Šumichrast
External expert	E. Dagnino

Co-funded by the European Union

Table of contents

Introduction **3**

Datafication and business deployment of workplace and workers' data in Europe ... **7**

Legal framework on data processing in the workplace at the European and national level **15**

1. European legal framework on personal data protection 16
2. Legal framework on data processing in the workplace at the national level 24
   - 2.1. The intersections between data protection law and employment law 25
   - 2.2. The role granted to industrial relations actors and processes 39

The role of industrial relations in workers' data protection and processing **47**

1. European trade union organisation's approach and practices 48
2. Institutional features of industrial relations in the manufacturing sector across countries 51
3. National trade union organizations approach towards workers' data protection and processing 60
4. Main topics and trends in social dialogue practices in selected countries 67
5. The role of European Works Councils in Multinational Companies 70

Conclusions **72**

References **76**

Co-funded by the European Union

Introduction

The problem with data protection laws
is that it presumes the data collection was ok
E. Snowden[1]

On 5 March 2015, the Commission initiated an initiative for *A New Start for Social Dialogue* at a high-level conference. "At that High-Level Conference, the Social Partners and the Commission agreed that the new start for social dialogue should aim for among others, a stronger emphasis on capacity building of national social partners, a strengthened involvement of social partners in EU policy and law-making and a clearer relation between social partners' agreements and the better regulation agenda"[2].

A few years later, the *European Social Dialogue Work Programme 2019-2021* indicated both digitalisation and capacity-building for a stronger social dialogue as priorities[3] and stated that in the world of work "digitalisation can be an opportunity and a challenge" while at the same time "many aspects of the ongoing digitalisation process are not yet clear or understood"[4]. The *European Social Dialogue Work Programme 2022-2024* explicitly mentions among others work-related privacy and surveillance as an issue to focus upon while stressing that "social dialogue at all levels is particularly relevant for fair, responsible and effective labour markets" and "social partners are particularly well placed to accompany the process of transformation of the economy and design balanced measures and solutions that contribute to economic and social progress"[5].

Over the last years, social partners have become increasingly aware of the challenges that increasing digitalisation brings with it. The European Social Partners Framework Agreement on Digitalisation focuses on AI and data processing, stating

[1] Cited in Fainmesser, Galeotti & Momot (2019), p. 1.

[2] Statement of the Presidency of the Council of the European Union, the European Commission and the European Social Partners, *A New Start for Social Dialogue*, Brussels, 27 June 2016. Also see the Declaration on a new start for a strong Social Dialogue approved by the SPs at Thematic Group meeting on 26-27 January 2016.

[3] Along with improving the performance of labour markets and social systems, skills, addressing psycho-social aspects and risks at work and circular economy, cf. the *European Social Dialogue Work Programme 2019-2021*, p. 3.

[4] *Ibidem*, p. 4.

[5] *European Social Dialogue Work Programme 2022-2024*, p. 3.

Co-funded by the European Union

that "Social partners at the level of the enterprise and at other appropriate levels should pro-actively explore the potential of digital technology and AI to increase the productivity of the enterprise and the well-being of the workforce, including a better allocation of tasks, augmented competence development and work capacities, the reduction of exposure to harmful working conditions and to ensure the protection of the rights and freedom with regards to the processing of personal data of employees in the context of employment relationships"[6].

However, effective and efficient social dialogue and collective bargaining depend on the capacity of employers' and workers' organisations to address the challenges posed by the new reality of work. Both at different levels from the workplace, from the transnational and European one, and, ultimately, on the knowledge and skills of individual representatives.

The GDPiR-project[7] fits within this framework, conceiving digitalisation and datafication in the employment context both as a challenge and an opportunity for social partners to collectively shape the future of work and aiming to provide them with the proper skills and knowledge to effectively act in this context. Notably, effective social dialogue and collective bargaining over data processing in the workplace can only be achieved if workers' representatives and trade unionists in different countries are adequately trained and get a deep knowledge of the national and European legislation in this field as well as of the best practices performed by social partners at the national and transnational level.

Since the use of data and big data is spreading pervasively in any business activity and is gaining importance in decision-making processes impacting on workers, data processing is due to become a fundamental subject of collective negotiations. Consequently, as a new field comes to enrich industrial relations, also the knowledge and skills needed by trade unionists and workers representatives must be enlarged. Providing workers' organisations with the proper skills to effectively address the challenges posed by digitalisation and datafication thus contributing to fill a gap in the praxis of industrial relations, is the main rationale of the GDPiR-project. By deepening the issues related to data processing in the workplace and, specifically, the role and prerogatives exerted by trade unions and workers' representatives, GDPiR aims at improving collective bargaining and social dialogue initiatives in this field and enhancing the adoption of collective solutions for the protection of workers'

[6] Cf. §§ 3-4 of the European Social Partners Framework Agreement on Digitalisation.
[7] *GDPiR. Managing data processing in the workplace through industrial relations*.

Co-funded by the European Union

rights in the midst of technological surveillance and a sustainable digital transformation.

Well-known and recently restated in the documents mentioned above, information and training activities are essential for an effective and efficient social dialogue and as such prerequisites to harness the potential of small and big data in workplaces. Information and training on data processing are also essential to trade unionists and workers' representatives in order to spur a more proactive attitude by workers' representation on the matter, and such without neglecting the importance of defensive actions, for instance in cases of intensified monitoring or exclusively data-driven or even automated decision making. In turn, all these are pivotal for the implementation of the Framework Agreement.

To this end the output of the GDPiR-project includes Guidelines on the negotiation of data processing, a Comparative Assessment Report and Country-Fiches gathering the national and European rules governing these processes and the best practices of negotiation over data processing in the workplace in the selected countries[8]. The Guidelines, the Comparative Assessment Report and the Country-Fiches are primarily designed as capacity building tools to be used during the training sessions foreseen in the project and to be used as tools or a basis for further development or adaptation after the project finished.

This present Comparative Assessment Report compiles the information gathered through desk research, surveys and interviews conducted in the framework of the GDPiR-project. In total 12 countries[9] are researched of which 5 form the core of the project – and where proper training activities will be provided to trade unionists and workers' representatives.

In the next section, we will take a brief look at the concept of 'datafication' and the use of workers' data. Subsequently, we will look into the legislative framework on data protection on national and supra-national levels. In the last section, we will discuss

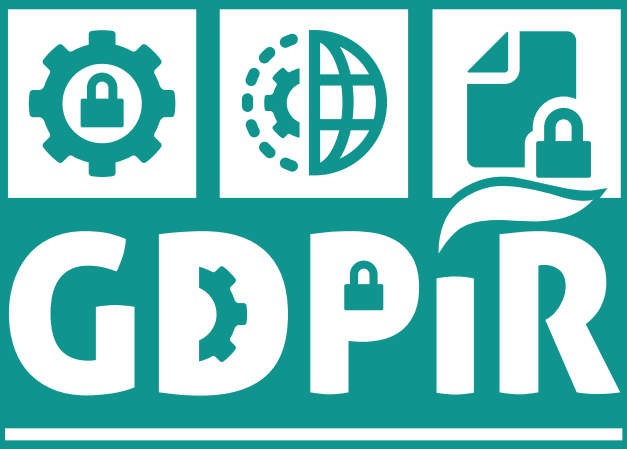
[8] In total 12 countries Belgium, Czech Republic, Germany, Hungary, Ireland, Italy, Luxembourg, Malta, Portugal, Slovakia, Spain and Turkey of which 5 (Belgium, Italy, Slovakia, Spain and Turkey) are considered the 'core-countries' of the project where the trainings and the national events will take place.

[9] The legal analysis of § 3.2 also comprehends data concerning France, Denmark and the Netherlands: the research concerning those countries was carried out by a research partner (Universiteit van Amsterdam) which was a research partner in the first phase of the project (M1-M15) (AMD 101048690-7).

Co-funded by the European Union

the role of industrial relations in workers' data protection and processing. Finally, we will formulate some conclusions and recommendations.

Co-funded by the European Union



MANAGING DATA PROCESSING
IN THE WORKPLACE THROUGH
INDUSTRIAL RELATIONS

DATAFICATION AND BUSINESS DEPLOYMENT OF WORKPLACE AND WORKERS' DATA IN EUROPE

Historically, the processing of personal data can be dated back to the earliest civilisations: as soon as there was a way of putting things down in writing, humankind started making lists. From anonymous shopping lists to the list of the names of slaves of slave owners[10]. The oldest surviving census data dates back to China's Han Dynasty[11].

Since the advent of digital technology, however, the means of processing data have been increasing dramatically[12].

The processing of personal data by employers far outdates the use of electronic tools such as digital processors: for instance, for the payment of wages or the monitoring of absenteeism, etc. A now infamous example was the '*livret d'ouvrier*'[13] which by some is considered as a tool for monitoring – and even surveillance and oppression of – workers and by others as one of the first official social documents. "The workers' record booklet dates back to an Ordinance of 2 January 1749 under the French king Louis XV which imposed on workmen the obligation to prove with a booklet that they had finished work with their former employers and which they had to carry with them at all times. Clients or employers were forbidden to hire workmen who could not prove, by means of the booklet, that they had performed their assignment with their previous clients or employers. Indeed, the worker's booklet was a useful means of proof. It listed all enlistments and departures. In this way, the workman could easily prove his professional career [14]. And the potential employer could conveniently

[10] Cf. *List of oldest documents*, in *en.wikipedia.org*.

[11] Showing a population of 57.7 million people living in 12.4 million households (cf. *Milestones and Moments in Global Census History*, in *www.prb.org*).

[12] Moore's Law can be mentioned by way of illustration (cf. *Moore's law*, in *en.wikipedia.org*).

[13] In Dutch '*werkboekje*' of '*dienstboekje*'. A possible English translation would be 'worker's booklet', 'service record booklet' or 'work(er's) record booklet'. For this publication, we opt for the use of the term 'workers' booklet' because, while it is meant to keep track of the worker's work record – or allow the monitoring of the worker's track record – the fact that a name like the '*livret d'ouvrier*' literally translated meaning the booklet of the worker literally indicates how normal the monitoring of the workers' track record was: there could clearly be only *one* worker's booklet.

[14] Or rather, the worker's professional career could easily be monitored by third parties. The reason why some scholars consider the worker's booklet also to be a tool allowing for the surveillance of the worker is the fact that workers were obliged to carry the booklet with them at all times. Workers could then be asked, e.g. by a policeman when walking in the street, to provide his booklet, which would show if the workers was employed or not and if so, potentially being absent from work without proper reason.

Co-funded by the European Union

check where a workman had worked before [15]. The compulsory use of the worker's booklet was maintained until the year 1883 when the compulsory use of the booklet was abolished while its optional use was retained" (Nevens, 2008).

Nevertheless, it is clear the evolution of technology and the speed of digitalisation of all aspects of our lives have an impact on the processing of workers' data by employers[16]. The 'worker's booklet' now being abolished has been replaced by online databases[17] who not only keep track of the worker's professional career, previous employers, but also allow for the monitoring of wages earned, social security contributions and taxes paid.

The evolution described above, from the use of a physical document to a digital one, is an example *digitalisation*, which can be described as "the adaptation of a system to be operated with the use of computers and the internet"[18]. The term digitalisation has been first recorded in 1956[19] and should not be confused – though it often is – with the term *digitisation*, which is used for the process of converting information into a digital (i.e., computer-readable) format[20]. "While *digitisation* focuses on *converting and recording* data, *digitalisation* is all about *developing processes and changing workflows.* An example of this would be using digitised customer data from different sources to automatically generate insights from their behaviour" (Monton, 2022).

---

[15] And then contact previous employers if he wished to do so, even without the worker's knowledge let alone consent.

[16] At the same time and as a result of business practices such as, among others, outsourcing and platformisation the typical employment relationship is also being transformed increasingly, resulting in many workers no longer being protected by long fought for rights enshrined in labour law and other legislative frameworks which typically do take the position of the worker as an employee into account.

[17] For instance, in Belgium, the Dimona-database which is connected to the Crossroads Bank for Social Security and allows various instances different levels of access. Dimona stands for 'Déclaration Immédiate/Onmiddellijke Aangifte' (in English: 'instantaneous or immediate declaration'). The Dimona online service allows an employer can notify the competent administrations that an employee is entering or leaving his employment or will be working longer or shorter than planned (cf. *A propos de Dimona*, in *www.socialsecurity.be*). Employers be advised that although the Dimona online service *allows* for such notifications, legally employers are *obliged* to notify as soon as possible or face severe fines (violation of said obligation is punished by a level 4 sanction as per Article 181 ff. of the Belgian Social Criminal Code. Cf. Dutch version, French version or see the version by De Coninck, Gillis & Jorens, 2013).

[18] Definition from Oxford Languages.

[19] Cf. *Digitalization*, in *www.oed.com*.

[20] Cf. *Digitization*, in *en.wikipedia.org*.

Co-funded by the European Union

Digitalisation and *datafication* gave rise to *digital transformation*, whose "primary aim is to integrate technology to most, if not all, business operations. In digital transformation, digital technology is incorporated into all areas of the business to fundamentally improve efficiency in workflows where organisational, and operational changes are implemented through the integration of digital technologies" (*idem*).

With the ongoing evolution of ICT-systems, *digital transformation* eventually gave rise to what we now know as *Big Data*. "Put simply, big data is a concept describing data sets that exceed the size that can be managed by traditional tools. It is defined by three Vs: variety, volume, and velocity. The growing variety of data sources that arrive in increasing volumes and with more velocity (the high rate at which data is received and acted on)" (Oracle, 2022, p. 3).

Eventually, in an essay by Viktor Mayer-Schönberger and Kenneth Cukier, they discuss the role of big data, first coining the term *datafication*. They describe it as information "that is sourced from a large array or resources and which is put to use in very extraordinary ways, far beyond the regular or intended use that the data was collected for". In their words: datafication "refers to taking information about all things under the sun – including ones we never used to think of as information at all, such as a person's location, the vibrations of an engine, or the stress on a bridge – and transforming it into a data format to make it quantified. This allows us to use the information in new ways, such as in predictive analysis: detecting that an engine is prone to a break-down based on the heat or vibrations that it produces. As a result, we can unlock the implicit, latent value of the information" (Mayer-Schönberger & Cukier, 2013, p. 15).

A few things are important to highlight. First of all, the concept of Big Data was first use to describe big datasets, for instance the large amount of data *produced* by the LHC at CERN (Stewart & Hegner, 2018) and evolved to *collecting* as much digital data as possible. The next step is then logically to not only collect and aggregate but also to digitise as much data as possible. Or: to datafy 'all things under the sun'.

Another important thing to highlight is the reasons Mayer-Schönberger and Cukier put forward for doing so: "to un-clock the implicit, latent value of the information": "There is a *treasure hunt* under way, driven by the insights to be extracted from data and the dormant value that can be unleashed *by a shift from causation to correlation*. But it's *not just one treasure*. Every single dataset is likely to have some intrinsic, hidden, not yet unearthed value, and the race is on to discover and capture all of it. Big data changes the nature of business, markets, and society. In the

Co-funded by the European Union

twentieth century, value shifted from physical infrastructure like land and factories to intangibles such as brands and intellectual property. That now is expanding to data, which is becoming a significant corporate asset, a vital economic input, and the foundation of new business models. It is *the oil of the information economy. Though data is rarely recorded on corporate balance sheets, this is probably just a question of time*" (Mayer-Schönberger & Cukier, 2013, pp. 24-25, emphasis added).

A lot is stated by Mayer-Schönberger and Cukier and a lot of it is repeated since they have said it, and often without much critical reflection. First of all, what they propose is a significantly different conception and use of Big Data. Second, their views are, from a European point of view, definitely trans-Atlantic: Big Data is all about profit, "the oil of the information economy", and just like with oil, profit can be found and made just about everywhere[21]. Last but not least, apart from intrinsic ideological implications of their statements, their views are at least partially based on several fallacies which, through the history of our species, have proven to have serious to extremely unkind consequences[22]. "Big data marks an important step in humankind's quest to quantify and understand the world. A preponderance of things that could never be measured, stored, analysed, and shared before is becoming 'datafied'. Harnessing vast quantities of data rather than a small portion, and privileging more data of less exactitude, opens the door to new ways of understanding. It leads society to abandon its time-honoured preference for causality, and in many instances tap the benefits of correlation" (Mayer-Schönberger & Cukier, 2013, p. 27). According to Naimi, Mayer-Schönberger and Cukier confuse issues of precision and validity (Naimi & Westreich, 2014).

Bad as this is, what is even worse, is the conclusions Mayer-Schönberger and Cukier pretend to be able to draw from their proposed use of Big Data. According to them, the scientific view of looking for the cause of an effect has become outdated: "a move away from the age-old search for causality. As humans we have been conditioned to look for causes, even though searching for causality is often difficult

[21] And just as with oil, they do not seem to care much about the consequences.

[22] For instance, in the field of psychiatry and criminology. But there's other fallacies, driven most probably by a typical Weltanschaaung. "After all, Amazon can recommend the ideal book, Google can rank the most relevant website, Facebook knows our likes, and LinkedIn divines whom we know" (Mayer-Schönberger & Cukier, 2013, p. 20). Everyone who has used search engines extensively or has looked for a very particular item on an online shop knows very well the results of their queries are not at all as efficient and successful as Mayer-Schönberger and Cukier stated, but are also, and in many cases mostly, driven by *other factors beside providing the searcher with the optimal result for his query*.

Co-funded by the European Union

and may lead us down the wrong paths. In a big-data world, by contrast, we won't have to be fixated on causality; instead, we can discover patterns and correlations in the data that offer us novel and invaluable insights. The correlations may not tell us precisely why something is happening, but they alert us that it is happening. And in many situations, this is good enough" (Mayer-Schönberger & Cukier, 2013, p. 21). A bit further into their publication, they formulate it even harsher and without any reservation: "The ideal of identifying causal mechanisms is a self-congratulatory illusion; big data overturns this" (*ibidem*, p. 27). The fact that such ways of thinking have not caused major upheaval in the scientific world might be justified by the fact scientists, to whom this publication was not addressed in the first place, failed to grasp its implications[23]. What Mayer-Schönberger and Cukier stated, was already happening at the time of the publication of their book.

What now is the relevance of all this to the subject at hand, i.e., the processing of (personal) data of workers by employers?

First of all, as with most persons, most workers are not aware of what data and how much of it is being processed. Second, and also in line with most persons, workers are not aware of why that data is being processed and what said processing leads up and amounts to. Looking at the views expressed by Mayer-Schönberger and Cukier, this is also becoming harder and harder. "The correlations may not tell us precisely why something is happening, but they alert us that it is happening. And in many situations, this is good enough" (Mayer-Schönberger & Cukier, 2013, p. 22). In other words, the outcome of the analysis of Big Data does not care about the why, nor do users of said means of analysis. Neither do they care about the accuracy of the outcomes. They are satisfied with 'good enough'. As such, decisions are being made about individuals on the basis of rough and potentially extremely faulty forms of 'deduction'. Which is not surprising, since users of Big Data and Data Analytics do not care about individuals specifically: "Big data gives us an especially clear view of the granular: subcategories and submarkets that samples can't assess" (Mayer-

[23] Maybe because in many cases, scientists are 'locked in' their 'silo's', as can be illustrated by the conclusion of Naimi's otherwise very good book review: "We agree with the authors that science and public health are at the cusp of a major and important change, in which 'big data' will play an integral role. Yet it seems equally clear that the perspectives offered in this book would benefit from a firmer grounding in existing scientific approaches and perspectives, and thus at present they may have relatively little utility for the practicing epidemiologist" (Naimi & Westreich, 2014, p. 1144). If only the author would have added a line warning the greater public and even more so policy makers of the dangers of Mayer-Schönberger and Cukier views and the uses of data they described.

Co-funded by the European Union

Schönberger & Cukier, 2013, p. 21). When it comes to the targeting of advertisements, this might work. After all, if you can convince the advertiser that your way of advertising will reach a significant part of his target audience (and probably convincing him you know the target audience better than the advertiser while you are at it), said advertiser will be tempted to grant your advertising firm at least a part of his advertising budget. However, when it comes to making decisions that will have direct effect on people's life, this should not and cannot be tolerated[24]. Nevertheless, we can observe the process of datafication taking place, if only we look carefully enough. And we can observe the use and abuse of Big Data permeating society. And thus, also, the workplace.

The means of collecting and processing (personal) data from workers have increased dramatically[25]. Yet, at the same time, we have become so unaware of our personal data being processed and remain mostly ignorant to the means and ways of processing our data and the implications of said processing. Even more surprising is the fact that the employers also seem to remain ignorant of the implications for their business of the ICT-tools they implement. Even after the revelations of whistle-blowers like Snowden, and in times of declining cybersecurity and rising means of cybercrime and digital industrial espionage, almost every company has moved or is moving their data 'into the cloud', thereby relying on and only on legal documents, contracts, which guarantee their data will be protected. At the same time, their employees are being confronted with privacy policies that are often far from being transparent and in most cases little to no means of declining, limiting or withdrawing consent.

Workers who fail to grasp the importance of data literacy and data awareness only need to take a peek at the world of platform work and look at the consequences of tools such as Algorithmic Management (AM)[26]. It is important to know that AM is not

[24] Unfortunately, Mayer-Schönberger and Cukier are far from the only authors sliding down this slippery slope. Another well-known publication that should also make every scientist should be outraged, and scientist who have some knowledge of the history of science and/or the philosophy of science even more so, and also an example of what we could call scientific barbarism (apologies to the barbarians) was also a best seller (Stephens-Davidowitz, 2018).

[25] From company and office cars, computers, cell phones and software allowing for severe monitoring to wearables allowing for the continuous and in-real-time collecting of data.

[26] "Algorithmic management is defined in the literature as oversight, governance and control practices conducted by software algorithms over many remote workers. It is characterised by the continuous monitoring and evaluation of workers' behaviour and performance through digital technologies (such as digital surveillance). Based on this data, platforms are able to rank platform

a phenomenon restricted to the world of platform work, but is or has been being implemented in more and more sectors, not in the least the manufacturing sector, hence the term 'Industry 4.0'. Among the risks for workers', for instance in the field of health and safety, Christenko *et al.* (2022) mention, among others, the intensification of work, the loss of job control and autonomy, the dehumanisation of workers, the 'datafication' of workers, discrimination and the use of private and sensitive data, performance monitoring and the use of worker rating systems, a lack of transparency and trust, and power asymmetry.

Clearly, it is important for workers, their representatives and trade union employees to understand the importance of the processing of (personal) data by employers – and where applicable, their clients or suppliers – and the effects, outcomes and implications thereof. Data subjects' rights enshrined in the GDPR allow or should allow for at least some means to gain insight into said processing in cases employers are not or not sufficiently transparent. However, the legislative framework on data protection is only one side of the coin[27] and one that suffers from both a scary and a bad reputation.

In the next section, we will briefly set out the legal framework on data protection and its main principles.

workers and issue rewards or penalties. Platforms are able to give preference to high-ranking platform workers when allocating tasks or can be set up so clients can see the profiles of workers with the highest ratings only. Additionally, as these decisions are usually implemented with minimal human intervention, platform workers interact with a 'system' rather than humans, which reduces transparency and causes asymmetries in information and power between the parties involved. Platform workers often have no insight into the rules governing the algorithm, with few opportunities for recourse or conflict resolution to challenge decisions" (Waeyaert, Hauben, Lenaerts & Gillis, 2022, pp. 5-6).

[27] The other side being the technicality of the ICT and other tools used for the processing of (personal) data.

Co-funded by the European Union

MANAGING DATA PROCESSING
IN THE WORKPLACE THROUGH
INDUSTRIAL RELATIONS

LEGAL FRAMEWORK ON DATA PROCESSING IN THE WORKPLACE AT THE EUROPEAN AND NATIONAL LEVEL

1. European legal framework on personal data protection

The 50th anniversary of the birth of the first data protection act in the world took place in 2020 in Hessen, a German Bundesland[28]. The 1986 version of the Hessen Data Protection Act for the first time contained a specific regulation on data protection at the workplace[29].

The first legal instrument on a supra-national scale with relevance for Europe was the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data concluded in 1981[30] and amended in 2018[31]. In 1989, the Committee of Ministers to Member States of the Council of Europe issued a Recommendation on the Protection of Personal Data Used for Employment Purposes which was updated in 2015[32].

The landmark judgement in which the European Court of Human rights (ECtHR) made clear 'the place of work' does fall within the scope of Article 8 of the European Convention on Human Rights (ECHR) was the case of Niemietz v. Germany[33] where

[28] Limited, however, to the processing of personal data by public bodies of the Bundesland (Flink, 2021, p. 32; also see the GDPiR National Report on Germany, p. 8, and GDPiR Country Fiche – Germany, p. 3.

[29] The scope of which, however, was still limited to the processing of personal data by public bodies of the Bundesland (Flink, 2021, p. 34; also see the GDPiR National Report on Germany, cit., p. 8, and GDPiR Country Fiche – Germany, cit., p. 3.

[30] 28 January 1981. For an overview of the protocols to said convention, see *Convention 108 and Protocols*, in *www.coe.int*.

[31] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 10 October 2018. Also see European Court of Human Rights (2023), European Court of Human Rights (2022), and the Council of Europe Data Protection website (*https://www.coe.int/en/web/data-protection*).

[32] Cf. Recommendation No. R (89) 2 of the Committee of Ministers to member States on the protection of personal data used for employment purposes, 18 January 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, 1 April 2015.

[33] The landmark judgement in which the ECtHR made clear 'the place of work' does fall withing the scope of Article 8 of the European Convention on Human Rights (ECHR) was the case *Niemietz v. Germany*, 16 December 1992, where it stated that "respect for private life comprises to a certain degree the right to establish and develop relationships with others and that there is no reason of principle why the notion of private life should be taken to exclude professional or business activities, since it is in the course of their working lives that the majority of people have a significant opportunity of developing such relationships. To deny the protection of Article 8 on the ground that the measure

Co-funded by the European Union

it stated that "respect for private life comprises to a certain degree the right to establish and develop relationships with others and that there is no reason of principle why the notion of private life should be taken to exclude professional or business activities, since it is in the course of their working lives that the majority of people have a significant opportunity of developing such relationships. To deny the protection of Article 8 on the ground that the measure complained, of related only to professional activities could lead to an inequality of treatment, in that such protection would remain available to a person whose professional and non-professional activities could not be distinguished […] and that narrow interpretation of Article ECHR could give rise to the same risk of inequality of treatment" (European Court of Human Rights, 1992). More recently, the European Fundamental Rights Agency (FRA) stated that "some of the most advanced technologies for monitoring and controlling the behaviour of individuals […] are used predominantly in working life" (European Union Agency for Fundamental Rights, 2010, p. 37)[34].

Other, more recent relevant judgments of the ECtHR concerning the processing of personal data of workers concern, among others, the use of GPS data of a medical representative's company vehicle as grounds for dismissal[35], the monitoring of

complained, of related only to professional activities could lead to an inequality of treatment, in that such protection would remain available to a person whose professional and non-professional activities could not be distinguished […] and that narrow interpretation of Article ECHR could give rise to the same risk of inequality of treatment" (European Court of Human Rights, 1992).

[34] Also see Abraha (2022), p. 278.

[35] "The Court held, by four votes to three, that there had been: no violation of Article 8 (right to respect for private life) of the European Convention on Human Rights (ECHR); no violation of Article 6 § 1 (right to a fair hearing)" (*Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 13 December 2022).

Co-funded by the European Union

employees' computer use[36], video surveillance[37] and the processing of medical data[38].

It was only in 1990 when the European Community took the initiative to adopt legislation[39] resulting in a directive in 1995[40]. Already, the Directive stressed the necessity of striking a balance between the free movement of data and the fundamental and the well-being of individuals (Recitals 2 and 3, Directive 95/46/EC). Despite the lightning speed of data processing technology, it took more than 2 decades for a new legal initiative to see the light[41] and more than 20 since the

[36] See the case *Bărbulescu v. Romania*, 5 September 2017, in which the court held that there had been a violation of Article 8 ECHR due to the fact the national courts had failed to determine whether Mr. Bărbulescu had received prior notice from his employer of the possibility that his communications might be monitored, that he had not been informed of the nature nor the extent of the monitoring. Furthermore, the national courts had failed to determine both the specific reasons for the introduction of the monitoring measures and whether the employer could have used less intrusive measures.

[37] See the case *Köpke v. Germany*, 5 October 2010. This case concerned a video recording of a cashier suspected of stealing money from the till which had been made without prior notice by her employer. "At the relevant time, the conditions under which an employer could resort to the video surveillance of an employee in order to investigate a criminal offence the employee was suspected of having committed in the course of his or her work had not yet been laid" down in German law. The ECtHR rejected the applicant's complaint under Article 8 of the Convention as inadmissible (manifestly ill-founded). Cf. European Court of Human Rights (2023), p. 13.

[38] See the case *Radu v. The Republic of Moldova*, 15 April 2014, in which the Court held that there had been a violation of Article 8 ECHR. Medical information of a lecturer at the Police Academy had not only been disclosed to her employer the information was also widely circulated at the applicant's place of work (allegedly to everyone at the Police Academy). Shortly afterwards, she had a miscarriage due to stress. The medical information comprised of a copy of the applicant's medical file from the hospital where she had been hospitalised, containing a detailed description of all the medical procedures she had undergone and of all the medical analyses, the fact that she was was carrying twins; that this was her first pregnancy and that the pregnancy had resulted from artificial insemination and that the she was suffering from hepatitis B that she had obstetrical complications and that she had a negative blood type.

[39] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data COM(90)314 final – SYN 287, 5 November 1990.

[40] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[41] 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), 25 January 2012, COM(2012)11 final.

Co-funded by the European Union

Directive, before the GDPR[42] finally saw the light in the legal universe of what had become the European Union[43] in the meantime[44].

Nevertheless, the GDPR is an improvement compared to Directive 95/46/EC. The biggest reason is already there in its name: the GDPR is a Regulation, which means it is valid in all Member States and does not need to be transposed into national law. Although the GDPR does not do away with the core principles of Directive 95/46/EC[45], under the directive there was much more disparity with regard to, among others, the concept of (processing of) personal data and data subjects' rights[46]. The fact the GDPR provides sanctions is also a big improvement[47].

---

[42] 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).

[43] A lot has changed since the days of Directive 95/46/EC. In the meantime, the Charter of Fundamental Rights of The European Union saw the light and, however not without controversy and upheaval, the European Community (again) has shed its skin and became the European Union. Hence the references made, in Recital 1 GDPR, to Article 8(1) of the Charter of Fundamental Rights of the European Union and to Article 16(1) of the Treaty on the Functioning of the European Union (TFEU).

[44] Not without any controversy due to heavy lobbying and unlawful forms of interference with the legislative procedure. Notably, the scandal where an MEP and allegedly one of his aids filed numerous amendments to the then proposal for the GDPR which were all in favour of data processing companies, is an infamous part o the history of data protection legislation in the European Union. Also remarkably according to some is that a member of the same political family is now, as a member of the Belgian Government, competent for digitalisation and privacy.

[45] See, for instance, Recital 5 GDPR, which states: "The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State". Also see Recital 9 GDPR.

[46] As is often the case when a legal instrument is 'updated', the Regulation consolidated the jurisprudence of the Court of Justice of the European Union on the matter. For a very brief summary of the GDPR, see *Summary of: Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data*. For further reading, cf. for instance Hoofnagle, van der Sloot & Zuiderveen Borgesius (2019).

[47] That does not mean the GDPR is perfect. For instance, data processing of workers is not the GDPR's strongest point. Or at least, also here still much depends on the Member State where the processing takes place. Furthermore, leaving the monitoring of the correct application and imposing sanctions to national Data Protection Authorities – and the way DPA's are devised and set up – also leaves room for critique and thus improvement. One of the biggest flaws, however, concerns the processing of workers' personal data. For a good overview of the issues in this field, see Abraha (2022).

Regarding the concept of the processing of personal data, Article 4 GDPR provides definitions of, inter alia, personal data, processing, etc.[48]. Note both the concept of personal data and the concept of processing are very wide, which allows for an extensive interpretation by competent courts. For instance, in several judgments, the Court of Justice of the European Union has stressed the fact that almost any data that can lead back to a natural person or data-subject, falls within the scope of the GDPR. For instance, in the field of HR and recruitment, and when Directive 95/46/EC was still in force, the Court of Justice considered: "the scope of Directive 95/46 is very wide and the personal data covered by that directive is varied"[49] and that "the use of the expression 'any information' in the definition of the concept of 'personal data' […] of Directive 95/46, reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, *but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject* [50]. As regards the latter condition, it is satisfied where the information, by reason of its content, purpose or effect, *is linked to a particular person*"[51].

In this case, a candidate who failed an exam requested access to 'all the personal data relating to him held' by the institute that organised the examination. Which refused to give Mr. Nowak said access. In order to consider the right of access, the Court of Justice needed to first consider whether the data requested by Mr. Nowak had to be considered 'personal data' under the Directive. As mentioned above, the court considered it did and eventually ruled that "the *written answers* submitted by a candidate at a professional examination *and any comments made by an examiner with respect to those answers* constitute personal data, within the meaning of that provision"[52].

In other words: *all data* linked to a particular person, even as remotely as the comments made by an examinator, are to be considered *personal data.* Since the

[48] Several websites and tools provide an easy and practical overview of the GDPR. Cf. for instance www.privacy-regulation.eu or gdprhub.eu, to name but two.

[49] The Court of Justice referring to judgment of 7 May 2009, Case C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, § 59 and the case-law there cited. Cf. CJEU 20 December 2017, Case C-434/16, Peter Nowak v. Data Protection Commissioner.

[50] Case Nowak, cit., § 34 (emphasis added).

[51] Ibidem, § 35 (emphasis added).

[52] Ibidem, § 62 (emphasis added).

Co-funded by the European Union

Nowak case, the CJEU has upheld and broadened this jurisprudence[53]. In a recent case the CJEU reiterated "the broad definition of the concept of 'personal data' covers not only data collected and stored by the controller, *but also includes all information resulting from the processing of personal data relating to an identified or identifiable person*"[54].

The Nowak case is not only important because of its broad interpretation of the concept of personal data, but also with regard to a data subject's right of access. In its jurisprudence, the Court of Justice considers the right of access of primordial importance. Indeed, without access, the data subject cannot exercise the other rights provided by the GDPR[55].

In the same vein, already prior to the GDPR, the Court of Justice considers the right to information of primordial importance: "the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed […] and their right to object to the processing of those data"[56].

In a recent judgment, the CJEU confirmed its jurisprudence on the interpretation of the concept of 'personal data' and on the right to access[57]. Although the facts of

---

[53] "The present approach in the EU appears to be capable of encompassing all information in its ambit, thus potentially transforming it into a universal regulation on the processing of information" (Wong, 2019, p. 517). An extensive overview of the CJEU's jurisprudence falls outside the scope of this report.

[54] CJEU 22 June 2023, Case C-579/21, *Proceedings brought by J.M.*, § 45, with reference to CJEU 4 May 2023, Case C-487/21, *F.F. v. Österreichische Datenschutzbehörde and CRIF GmbH*, § 26.

[55] "In particular, that right of access is necessary to enable the data subject to exercise, depending on the circumstances, his or her right to rectification, right to erasure ('right to be forgotten') or right to restriction of processing, conferred, respectively, by Articles 16 to 18 of the GDPR, as well as the data subject's right to object to his or her personal data being processed, laid down in Article 21 of the GDPR, and right of action where he or she suffers damage, laid down in Articles 79 and 82 of the GDPR (judgment of 4 May 2023, Österreichische Datenschutzbehörde and CRIF, C-487/21, EU:C:2023:369, paragraph 35 and the case-law cited)" (*Proceedings brought by J.M.*, cit., § 58) and "the exercise of a right of access which ensures the effectiveness of the rights conferred on the data subject by the GDPR" (*ibidem*, § 80).

[56] CJEU 1 October 2015, Case C-201/14, *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others*, § 33. In this case, personal data was transferred between state institutions (i.c. social security and tax administrations) without the data subjects being provided adequate information about said data transfer. The CJEU also considered that "it follows that the requirement of fair processing of personal data laid down in Article 6 of Directive 95/46 requires a public administrative body to inform the data subjects of the transfer of those data to another public administrative body for the purpose of their processing by the latter in its capacity as recipient of those data" (§ 34).

[57] Cf. *supra* and the *Proceedings brought by J.M.*, cit.

Co-funded by the European Union

this recent case predated the entry into force of the GDPR, the Court concurred with the Advocate-General's Opinion "that the right to information regarding the processing of personal data is a procedural right. Procedural rules, in contrast to substantive rules, *apply from the date on which they enter into force*"[58].

Furthermore, the Court of Justice stated that in said case, it was "not disputed that the consultation operations carried out on the personal data of the applicant in the main proceedings constitute 'processing' within the meaning of Article 4(2) of the GDPR, with the result that they confer on him, pursuant to Article 15(1) of that regulation, *not only a right of access to those personal data, but also a right to be provided with the information linked to those operations*, as referred to in the latter provision"[59].

Although in said case, where it ruled the right of access does not entail a right in respect of information relating to the identity natural persons it added unless that "information is essential in order to enable the person concerned effectively to exercise the rights conferred on him or her by that regulation and provided that the rights and freedoms of those employees are taken into account"[60], the Court of Justice does to a certain degree limit the right of access. Clear data subjects that are provided with strong legal rights regarding the processing of information primarily concerns them.

The broad definition of the concept of (the processing of) personal data, the extent of the right of access and the obligation for controllers to provide data subjects with information about said processing and the broad interpretation of said information all are strong rights and effective tools, the disrespect of which by data controllers is liable to be sanctioned with severe fines.

There is some disagreement regarding Article 80 GDPR which allows data subjects to mandate a not-for-profit body, organisation or association to, inter alia, lodge the complaint on his or her behalf (Article 80(1) GDPR) and the question whether trade unions can do so independently of a data subject's mandate as provided and under the conditions set in Article 80(2) GDPR. In a recent case, the Court of Justice had to rule on a case were representative action was brought by a consumer protection association in the absence of a mandate and independently of the infringement of specific rights of a data subject, where said action based not based primarily on the

[58] *Proceedings brought by J.M.*, cit., §§ 29-36.
[59] *Ibidem*, § 61.
[60] *Ibidem*, cit., § 90.

Co-funded by the European Union

GDDPR but on the prohibition of unfair commercial practices, the infringement of a consumer protection law and the prohibition of the use of invalid general terms and conditions. In its judgement, "the referring court observed that Article 80(2) of the GDPR such an action of the GDPR does not provide for an association's standing to bring proceedings in order to secure the application, objectively, of the law on the protection of personal data since that provision presupposes that the rights of a data subject laid down in the GDPR have actually been infringed as a result of the processing of specific data"[61]. Despite the fact the Member State had not explicitly implemented Article 80(2) GDPR[62] the Court of Justice observed that "it must be held that a consumer protection association […] may fall within the scope of that concept in that it pursues a public interest objective consisting in safeguarding the rights and freedoms of data subjects in their capacity as consumers, since the attainment of such an objective is likely to be related to the protection of the personal data of those persons"[63] and that "authorising consumer protection associations […] to bring, by means of a representative action mechanism, actions seeking to have processing contrary to the provisions of that regulation brought to an end, independently of the infringement of the rights of a person individually and specifically affected by that infringement, undoubtedly contributes to strengthening the rights of data subjects and ensuring that they enjoy a high level of protection"[64]. It is hard to imagine a reason why this reasoning is not applicable to a trade union.

In other words, the GDPR provides strong rights and legal means allowing data subjects to monitor its sound application and to monitor its principles[65] are observed and in case they are not, to take legal action and/or lodge a complaint.

Finally, of importance to the processing of workers' personal data, Article 88 GDPR provides for the possibility for Member States to provide "by law or by collective agreements […] 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

---

[61] CJEU 28 April 2022, Case C-319/20, *Meta Platforms Ireland Limited v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV*, § 43.

[62] *Ibidem*, §§ 59-61.

[63] *Ibidem*, § 65.

[64] *Ibidem*, § 74.

[65] Among others, lawfulness, fairness and transparency, data minimisation, accuracy, etc. See Chapter II, *Principles* (Articles 5-11 GDPR). For further reading, see for instance, Hoofnagle, van der Sloot & Zuiderveen Borgesius (2019).

Co-funded by the European Union

performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation 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" (Article 88(1) GDPR).

Whether or not Article 88 GDPR is a good or a bad thing, is a question an (elaborate and grounded) answer to which falls outside of the scope of this report but nevertheless worth a profound debate. In particular if we look at the wording of the second paragraph of said Article[66] and the iterations of said Article in the different Member States, which we will discuss in the next section[67].

2. Legal framework on data processing in the workplace at the national level

After a brief overview of European legislation concerning data protection and processing in the workplace, it is now time to provide some information concerning national legislations on the matter. The analysis outlined in the following paragraphs, which covers 15 countries (14 European Union member states and one candidate country), was carried out by the research partners of the GDPiR project, through the means of a desk research completed between M2 and M11 of the project.

---

[66] Article 88(2) provides: "Those 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, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place".

[67] Throwing the cat among the pigeons. Hoofnagle *et al.* observed: "the GDPR is constitutionally skeptical of U.S. lawyers' favorite tool: consent, particularly of the low-quality or 'take it or leave it' variety" (Hoofnagle, van der Sloot & Zuiderveen Borgesius, 2019, p. 68). Confronting this statement to the discussions regarding employees' consent during the debates on the implementation of Article 88 GDPR in certain Member States, could be sufficient grounds for (re-)opening said debate. Throwing another cat among the same pigeons, one could ponder the question if certain (clauses of) CLAs not amount to a form of implicit 'consent' to forms of processing which in the absence thereof would not be permissble under the GDPR. Such debates, however, fall outside the scope of this report. For further reading on Article 88 GDPR, see for instance Abraha (2022), p. 278.

Co-funded by the European Union

In more detail, KU Leuven analysed the legislative frameworks of Belgium, Luxembourg and Germany; ADAPT analysed the legislative frameworks of Italy, Ireland and Malta; CELSI analysed the legislative frameworks of the Czech Republic, Hungary and Slovakia; UvA analysed the legislative frameworks of Denmark, France, and the Netherlands; UC3M analysed the legislative frameworks of Spain and Portugal; IKCU analysed the legislative framework of Turkey.

2.1. The intersections between data protection law and employment law

Firstly, specific attention was dedicated to the connections between data protection and employment legislation of the different countries analysed, as interpreted by rulings of National Data Protection Authorities and relevant judicial organs. This choice was made in order to provide as comprehensive an overview as possible of legislative provisions regulating data processing in the employment context, all while taking into account the role of relevant national actors on the matter.

Therefore, the GDPiR research teams collected the different national provisions concerning workers' data processing and classified them as belonging to data protection legislation and/or to labour legislation, all while underlining the cases where the two intertwine. Moreover, in order to complement this data, relevant rulings by Data Protection Authorities and judicial organs on the matter have been identified and synthetized[68].

The more frequently regulated topics in the different sources which have been analyzed are video-surveillance/monitoring and geo-location. Provisions and rulings concerning algorithmic management and AI-powered tools are instead to be more rarely found – thus signalling a lower level of awareness and attributed importance from the different stakeholders involved.

In more detail, the general regulatory trends in workers' data protection can be described as follows.

- The legislative frameworks here are characterised by a different level of contact between employment and data protection legislation.

[68] Data collected from GDPiR research partners has also been integrated through the information included in Hendrickx, F., Mangan, D., & Gramano, E. (eds.) (2023). Privacy@work. A European and Comparative Perspective. Alphen aan den Rijn: Wolters Kluwer.

Co-funded by the European Union

  - Some national data protection legislations do not include additional employment-specific provisions other than those already included in the GDPR; in those cases, issues related to data protection in the workplace are solved through the application of the general principles in terms of data protection outlined in the GDPR or other relevant legislation (Czech Republic, Ireland, Malta, Turkey, The Netherlands).
  - When data protection legislations include only a few employment-specific provisions, they usually concern the restriction of the use of employees' genetic (Luxembourg) or biometric data (Portugal). Moreover (and coherently with Recital 155 GDPR) some Member states limit the use of consent as a legal basis for workers' data processing (Germany; Portugal), while others have a different view on the matter (Denmark).
  - The countries which show most intersections between labour and data protection legislations usually foresee that employers can only process employees' personal data which is pertinent to the employment relationship (Italy, Slovakia, Czech Republic, Denmark) and/or for employment-related purposes (Germany, Portugal). Employee surveillance and monitoring is instead usually allowed only for distinct purposes (Italy, Slovakia, Portugal), and following the principle of transparency (Portugal, Spain, France).
- When intervening on employment-related disputes, National Data Protection Authorities often ground their decisions on both labour and data protection legislative provisions (Czech Republic, Italy). Their rulings often concern workers' monitoring and surveillance through technological tools (e.g. CCTV, geo-location or e-mail systems, fingerprint scanners) (Germany, Italy, Czech Republic, Slovakia, Turkey), the use of their data for disciplinary actions (Ireland), workers' representatives information and consultation rights (Luxembourg). Sometimes, the activities of Data Protection Authorities with regard to workers' data processing also entail the issuing of guidance documents/self-assessment tools directed at relevant stakeholders (Hungary, Ireland, Portugal, Malta, Slovakia, Spain, Denmark): in one particular case, the DPA issued a Guideline directed to works councils, aimed at facilitating the exercising of their statutory prerogatives linked to data protection (The Netherlands).

Relevant case law concerning data processing in the workplace usually focuses on admissibility of proof obtained through employee surveillance, carried out by CCTV or e-mail (Belgium, Luxembourg, France); applicability of data protection and labour legislation to employers' monitoring activities (Czech Republic, Ireland, Italy, Turkey);

Co-funded by the European Union

employees' right of access to their personal data (Germany); disclosure of employees' personal data to workers' representatives (Spain) or to other employers (Turkey); the balance between employees' data protection rights and the legitimate interests of the employer (The Netherlands).

Co-funded by the European Union

	Employment-specific provisions in national data protection law	Other legal provisions regulating personal data processing in the employment context	Role of data protection authorities in employment disputes	Employment-specific provisions in national data protection law
Belgium	Data processing in Belgium is mostly regulated **by Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data**. However, the Act does not include provisions specifically dedicated to the employment context; **this last issue is therefore almost exclusively regulated by CLAs** (see table below).	Relevant employment legislation linked to data protection was already in force before the issuing of the GDPR (e.g., the **Act of 15 January 1990 on the establishment and the organisation of a Crossroads Bank of Social Security**)	The **Belgian Data Protection Authority** (Gegevensbeschermings autoriteit/ Autorité de protection des données) was established by **Act of 3 December 2017**. This body **does not often issue decisions aimed at solving disputes on personal data in the employment context**. However, a specific section of the DPA's website provides FAQ and Guidelines on the matter.	**Belgian judicial authorities often decide on issues linked to data processing in the workplace – and, specifically, to the breach of respective provisions included in CLAs.** The most relevant decisions deal with the topics of the **admissibility of proof obtained through video-surveillance** (e.g., 'Le Chocolatier Manon-case', which gave rise to two judgments by the Belgian Court of Cassation) and **access/screening of employees' e-mails** (BBTK v. ING, currently being treated by the competent Labour Court).
Czech Republic	The **Transposition Act No. 110/2019 on the Processing of Personal Data (PDPA)** clarifies and further regulates the processing of personal data in conformity with the EU GDPR. However, the **PDPA does not offer exhaustive rules or specifications with regard to data protection in the employment context.**	**Section 316 of the Czech Labour Code restricts the employer's ability to do background checks of job candidates.** The code is also **stringent in the matter of the processing of the personal data of current employees by an employer**: the gathering of personal data is expected to be **as limited as possible, taking into account the purpose for their collection.** The employer is required to inform the	**The Czech Personal Data Protection Authority is tasked with upholding the PDPA as well as the Labour Code and looking into complaints of data protection violation.** A relevant ruling by the DPA concerns the **use of fingerprint scanners by an organization to track employee attendance** – which was classified as processing of biometric data ex art. 9 of the GDPR. Since the organization had not	The Czech Supreme Administrative Court determined in 2019 that **the employer's monitoring of an employee's email and internet activity qualified as processing of personal data and was therefore subject to the PDPA and GDPR's regulations.** Namely, **t**he company was found to have done a poor job of conducting a DPIA and not obtaining sufficient employee consent for the monitoring of their

Co-funded by the European Union

		data subject of the purpose for which the data will be used, who will have access to it, and how long it will be stored. However, according to **Article 316, Sections 3161, II and III of the Labour Code**, **the employer has the right to monitor employee adherence to the rule against using company equipment (e.g., computers)** for personal purposes, which lays the ground for open surveillance of employees.	undertaken a data protection impact assessment (DPIA) and had not obtaining sufficient employee agreement for the processing of their biometric data before adopting the fingerprint scanning technology, the Czech Personal Data Protection Authority **ordered the organization to stop using the scanners and erase any previously gathered biometric information.**	personal data; the employer was therefore required by the court to discontinue monitoring and to destroy all personal data that had been gathered.
Denmark	The 'Danish Data Protection Act' of 17th May 2018 implements the GDPR. Its Section 12 (2) states that, **in order for the controller or a third person to pursue a legitimate interest derived from other statutory acts or collective agreements,** data processing should be **balanced against the rights of the employee as in GDPR** (art. 6 (f). Moreover, the Danish Data Protection Act (in Section 12(3)) **allows consent to be used as a legal basis in an employment context,** provided consent is given **in accordance with the conditions laid down in Article 7 of the GDPR.**	The Health Information Act of 1996 includes **specific limitations concerning the processing of employees' health data during the recruiting phase and whole duration of the employment relationship** (e.g., only relevant data for the employee's ability to perform the job he was hired for can be in fact processed, applying the principle of confidentiality) which can be **partly overcome only in the presence of a relevant public interest or specific requirements included in collective agreements.** Moreover, the **TV surveillance Act of 1998** supplements **specific rules on TV monitoring, also in the employment context.**	The DDPA (Danish Data Protection Authority) is responsible for **the supervision of all processing operations covered by the Danish Data Protection Act and the GDPR** – including those arising in the employment context – and enforcing those acts. **Several guidelines have been published by the same Authority regarding data processing in the workplace** (The DDPA Guideline on Employment, 2023).	Danish judicial authorities often decide on issues linked to **data processing in the workplace,** especially those in the field of **technological monitoring** through social media, cameras, e-mail surveillance, geo-location (which can't be used to assess the activities of the employees) and the **processing of employees' health data.**

Co-funded by the European Union

France	The main legislation regulating data protection in France is the **Act on Information Technology, Data and Freedoms 1978** (Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés) which was modified by **Law 2018-493**, transposing the GDPR into French law. This Act **does not include provisions applicable specifically to the employment context.**	**Article L1221-6 of the Labour Code** states that the **information asked to job candidates during the recruiting phase can only be used to assess the employee's ability to do the job offered or his/her professional aptitudes.** This information must have a direct and necessary link with the job offered or with the assessment of professional skills. With regard to technological monitoring, art. 1222-4 of the Labour Code states that **no information concerning an employee personally may be collected by a system that has not been brought to the employee's attention beforehand.**	The **Commission Nationale de l'Informatique et des Libertés (CNIL)** is the **French Data Supervisory Authority.** The CNIL expresses opinions on a variety of matters concerning data protection in the employment context, such as **electronic surveillance by telephone** – establishing several ground rules on the matter. Moreover, in 2020, the CNIL, together with the French Ombudsman, **issued a report recommending a set of measures aiming at limiting potential discriminatory algorithm bias –** including a proposal for reform of article L1132-1 of the Labour Code. However, the CNIL has also more substantial powers: according to the Data Protection Act 1978, **when an electronic device in the workplace carries out or allows the processing of personal data, a declaration procedure with the CNIL is required.**	In January 26, 2016, the Court of Cassation ruled that **employers are prohibited from basing their decisions on e-mails from the employee's personal e-mailbox**, even in the case it is installed on the employee's work computer. The French Courts have also stated that **the employer might monitor the websites visited by the employee during working hours through his/her work computer, also outside his/her presence**. Several rulings also deal with limitations concerning **the use of camera surveillance** (e.g., purpose limitation, conservation period etc).
Germany	With regard to data processing in the employment context, according to Sec. 26 of the new BDSG (**Federal Data Protection Act 2018** – Bundesdatenschutzgesetz), employees' **personal data can only be**	No employment-specific provisions on data processing in the employment context in other legislative instruments.	In Germany, there is **one federal Data Protection Authority, while each Bundesland has its own independent DPA.** The DPAs operating on state-level often deal with **data protection in the employment context (e.g., workers'**	Relevant German case law concerning data processing in the employment context often deals with **the employees' right of access to their personal data and the need for the employers' response to be comprehensive**

Co-funded by the European Union

	processed for employment-related purposes such as the start and end of employment, employee performance and for carrying out a collective agreement. Moreover, with regard to consent, sec. 26 states that if the processing of personal data of employees is based on consent, **the assessment of the voluntariness of the consent shall in particular take into account the dependency of the employee in the employment relationship as well as the circumstances under which the consent was given** (e.g., if a legal or economic advantage is achieved for the person employed).		**monitoring and surveillance through technological tools** – see Hamburg DPA, 2020, and Saxony DPA, 2021). The DSK (Conference of the Independent Data Protection Authorities of Germany) is a **coordinating body dealing with and commenting on current issues of data protection in Germany**, which comprehends the federal and all state-competent DPAs. On 4 May 2022, the DSK published a call for the creation of an Employee Data Protection Act, declaring unambiguously their view on the matter.	**and on time** (Labour Court Düsseldorf, 2020), **exception made for data which should be kept secret because of overriding legitimate interests of a third party** (e.g., whistleblowers) (Labour Court of Baden-Württemberg, 2021).
Hungary	**Law No. XXXIV of 2019 on the data protection reform** introduced **§§ 10-11** (which now compose a separate section on Data Processing) **and § 44/A in the Hungarian Labour Code** (Law No 1 of 2012). This reform **did not cause significant changes in the general definition regarding preconditions** for restricting employee's rights related to personality, but introduced **stronger justification and information requirements** for those restrictions.	No employment-specific provisions on data processing in the employment context in other legislative instruments.	The National Authority for Data Protection and Freedom of Information (NAIH), established in 2012, is a **key player in the implementation of Hungarian data protection law**, as it **provides interpretative and practical guidelines for affected stakeholders**, including industrial relations actors. For example, during the COVID-19 pandemic, the NAIH issued a guidance **document concerning employers' entitlement to be informed about**	Even before the 2019 data protection reform, **a judicial practice regarding employers' unlawful employee control and data processing had already developed in Hungary** – also including relevant Supreme Court rulings on the matter. Pre-2019 court rulings on employee personal data protection and data processing appear to be **retrospectively in line with requirements of the later introduced data protection legislation.**

Co-funded by the European Union

			employees immunity against Covid-19 (vaccination).	
Ireland	**No employment-specific provisions in national data protection law** – the issue of data processing in Irish workplaces is managed through the **application of the general principles of the GDPR and of national data protection law**, i.e.: the Data Protection Act 2018, the Data Protection Acts 1988-2003 (largely repealed, which however continue to apply in relation to limited purposes, as national security and defence) and the ePrivacy Regulations (S.I. No. 336 of 2011).	No employment-specific provisions on data processing in the employment context in other legislative instruments. However, if considered and applied jointly with **national employment equality law (Equality Employment Acts 1998-2011),** the GDPR might be a useful tool for the **protection of workers from undesirable effects of Artificial Intelligence,** especially during the recruitment phase – given the many of transparency and risk assessment obligations it foresees. References to the GDPR are also included in the current versions of the Organization of Working Time Act and in the Safety, Health and Welfare at work Act.	**Data protection issues concerning Irish workers can arise equally in the Data Protection Commission or labour adjudication settings** – in the context of traditional employment law disputes concerning for example wrongful dismissal or the issuing of disciplinary actions. The Data Protection Commission often issues **Guidelines** on topics linked to data processing in the employment context (e.g., use of CCTV, Vehicle Tracking, COVID-19). The case studies included in the Data Protection Commission's **annual reports** also often deal with data processing in the workplace.	**Irish case law concerning data protection in the employment context builds on the general principles of EU and national law.** For example, in one recent case on the matter, the Irish courts affirmed how **data shall be collected and processed only for one or more specified and lawful purposes** (in the specific case, crime prevention) **and not be used or disclosed in any manner incompatible with those purposes** (e.g., disciplinary actions) (Doolin v. the Data Protection Commissioner, 2022).
Italy	The **Italian national legislation on data processing** (Legislative Decree n. 196/2003 – Personal Data Protection Code) **includes several provisions concerning data processing in the employment context, covering a vast array of issues,** such as the delivery of curricula by prospective workers (art. 111bis) and the safeguarding of	**Law 300/1970 (Workers' Statute)** includes two provisions which are closely linked to workers' data processing and surveillance. Firstly, art. 4 of the Workers' Statute deals with the **regulation of monitoring of workers' activities by technological means** – which is made possible only for **distinct purposes** (e.g. health and safety, organizational and	The Italian National Data Protection Authority (GPDP) **frequently deals with issues concerning data processing in the employment** context, grounding its decisions not only on provisions of the Personal Data Protection Code, **but also on art. 4 of the Workers' Statute or other employment law provisions.** Those decisions are usually	**The Italian case law concerning data processing in the employment context is usually grounded on employment law provisions:** for example, a judicial interpretation of art. 4, § 2, of the Workers' Statute resulted in the principle that each hardware and software component of technological devices used during the

Co-funded by the European Union

	teleworkers and agile workers' personal data (art. 115). It is also to be noted how **Articles 113 and 114 of the Code directly refer to the provisions of the Italian Workers' Statute** (art. 4, art. 8) which deal with remote surveillance and data processing, making them effectively part of Italian data protection legislation.	productive reasons, protection of company assets) and **within strict boundaries** (see table below). Then, art. 8 of the Workers' statute includes a **ban of employers' investigations on facts not relevant to the assessment of the workers' professional attitude.** Lastly, it is to be noted how Legislative Decree n. 152/1997 (as modified by Legislative Decree 104/2022) provides workers with **information rights regarding fully automated decision-making or monitoring systems in the workplace** (art. 1bis).	linked to the **impact of technological tools** (e.g. geo-localization; e-mail systems) **on workers' data protection rights (**n. 38/2017; n. 303/2016; n. 139/2018).	employment relationship must be individually considered as autonomous working (and potentially monitoring) tools (**Court of Milan, 24/10/2017)**.
Luxembourg	The main national law concerning data processing in Luxembourg is **Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework**. However, the only provision concerning data processing in the employment context is **Art. 66 of the Act,** which **prohibits the processing of genetic data for the purposes of the exercise of the specific rights of the controller in the field of labour law and insurance.**	Following the publication of Act of 1 August 2018, **the Luxembourg Labour Code (Article L261-1) was amended in the sense that it now includes consent among the legal basis for data processing in the employment context – which was not the case before 2018.**	The organization and procedures of **the Luxembourg Data Protection Authority (CPND)** have significantly changed after 2018. With regard to the employment context, it is to be noted **that the processing of employees' data is no longer subject to an *ex-ante* control mechanism by the CNPD, but only to an ex-post check.** The **information rights of employees' and workers' representatives concerning remote surveillance have been object of recent decisions by the CPND** (Délibération n° 11FR/2022 du 22 avril 2022).	The current case law of Luxembourg concerning data protection is mainly focused on the **private character of digital correspondance in the workplace**. In fact, recent decisions of the Luxembourg Court of Appeal have stated that **the employer may occasionally monitor the employee's computer**, including his or her work e-mail; **any document discovered in the course of this control which relates to strictly professional data is in principle lawful evidence**.

Co-funded by the European Union

Malta	**No employment-specific provisions in national data protection law** – the issue of data processing in Maltese workplaces is managed through the **application of the general principles of the GDPR and of data protection law**, i.e., the Data Protection Act 2018 – Chapter 586 of the Laws of Malta.	No employment-specific provisions on data processing in the employment context in other legislative instruments.	The Maltese National Data Protection Authority (Information and Data Protection Commissioner – IDPC) (Article 11) is invested with the tasks enumerated by Article 57 of the GDPR and by part. V of the Data Protection Act 2018. **The Decisions made by the IDPC on data protection complaints are not publicly available.** The IDPC recently coordinated a **European-funded project** directed towards Maltese micro and small and medium enterprises, called 'GDPRights': **the main output of the project was the creation of an Online Self-Assessment Compliance tool** which could help enterprises understand their obligations under European and national data protection law, currently available on the IDPC website.	No relevant case law concerning data processing in the employment context.
The Netherlands	In the Netherlands the GDPR is implemented through the **Implementation Act (*Uitvoeringswet AVG – UAVG*):** the provisions of the previously existing legislation, the Dutch Data Protection Act (*Wet bescherming persoonsgegevens*), are maintained insofar as they are compatible with the GDPR. **The**	The **Dutch Working Conditions Act**, in conjunction with the **Medical Treatment Agreement Act**, include some specific requirements concerning the processing of employees' health data.	To support works councils in the considerations they have to make regarding data processing and privacy at the workplace (and especially electronic monitoring –see table below) **the Dutch Data Protection Authority (AP) has developed a guide explaining the role of the works councils on the 'regulation regarding the**	Some relevant cases related to **data processing and privacy in the context of an employment relationship** have justified the processing of workers' data in light of the presence **of legitimate interests of the employer** (e.g., addressing the transgressive behaviour of an employee creating a threatening and

Co-funded by the European Union

	UAVG does not include provisions concerning data processing in the employment context – exception made for a reference of employee consent in Recital 43. However, it states that employee health data may be only processed for the performance of legal obligations, pension arrangements and/or collective labor agreements that provide specific entitlements to the employee dependent on their health situation; for the purpose of the employer's re-integration and/or support of the employee during sickness and/or work incapacity (art. 30, § 1).		**processing of personal data' at the workplace**. The AP also issues decisions concerning **data processing in the workplace**: one of the most relevant decisions on the matter is related to alcohol and drugs testing in the workplace – which, being considered as data related to the health of the employee (and therefore protected under art. 9 of the GDPR) is only allowed for certain professions in accordance with the Shipping Act, Railway Act, Local Rail Act and Aviation Act.	intimidating working environment, controlling workers on sick leave). However, in other cases Dutch courts have been stricter towards the employer: this is the case, for example, of **rulings concerning biometrical data control systems** (e.g., finger scanning authorization systems) **or remote work** (the employer's instructions to leave the camera on during working hours were decided to be in violation of the right to respect for private life).
Portugal	The Portuguese national legislation providing for specific rules with regard to data protection is **Law No. 58/2019 of 8 August 2019**, whose article 28 sets special rules on the processing of employees' personal data. Article 28 states that, unless otherwise provided by law, **the employee's consent shall not constitute a requirement for the lawfulness of the processing of his/her personal data** if the processing results in a legal or economic advantage for the employee, or if such processing is covered by	**Articles 17 and 18 of the Lei nº 7/2009, de 12 de fevereiro, Aprova a revisão do Código do Trabalho**, include some references to data protection in the workplace. Art. 17 states that **the employer may not require a jobseeker or worker to provide information relating to their private life, except where this is strictly necessary and relevant to assessing their suitability for the performance of the employment contract;** the reasons for the request must be provided in writing.	The Portuguese data protection authority is constituted by an independent administrative entity called **Comissão Nacional de Protecção de Dados (CNPD).** The CNPD most important decision with regard to employees' data processing is **resolution nº 7680/2014 concerning the geolocation of employees.** In addition, the CNPD has issued **several guidelines and recommendations on employment issues.**	No relevant case law concerning data processing in the employment context.

Co-funded by the European Union

	Article 6(1)(b) of the GDPR. Moreover, it is established that **recorded images and other personal data recorded through the use of video systems or other technological means of remote surveillance may only be used in the context of criminal proceedings** – also for the purposes of establishing disciplinary responsibility. Lastly, **the processing of employees' biometric data is only considered legitimate for attendance control and for controlling access to the employer's premises**.	Art. 18 deals with the issue of employees' biometric data, stating that **the employer may only process them after notifying the National Data Protection Commission and within the boundaries outlined in the GDPR and in national legislation**. Lastly, art. 20 of the Labour Code states that **the employer may not use means of remote surveillance in the workplace, for the purpose of monitoring the worker's professional performance**, but only for the protection and safety of people and property or when particular requirements inherent to the nature of the activity justify it. In any case, **the employer shall inform the worker of the existence and purpose of the means of surveillance used**, especially with regard to CCTV.		
Slovakia	**The Personal Data Protection Act (No. 18/2018),** which implements the GDPR, **provides general rules concerning the gathering, use, and storage of personal data.** With regard to the processing of personal data in the workplace, it states that **employers are only permitted to gather information about employees'**	The **Slovakian Labour Code Act (No. 311/2001)** regulates data protection and processing in the workplace mainly by **establishing requirements for employers to protect employees' personal data and privacy**. Article 11 of the Labour Code offers **basic guidelines for processing employee personal data** that are	Employers who **disregard the Slovakian legislation** concerning data protection may be subject to fines or other sanctions ruled by the **Office for Personal Data Protection of the Slovak Republic (DPA)**, which is the national Data Protection Authority responsible for enforcing GDPR and the Personal Data Protection Act in Slovakia. **The role of the**	No relevant case law concerning data processing in the employment context.

Co-funded by the European Union

	qualifications, work history, and other personal data that may be pertinent to the work the employee is performing or will be performing. Moreover, **section 78(3)** of the Personal Data Protection Act includes a detailed **list of the types of employees' personal information that may be disclosed by the employer** (e.g., sharing of information about an employee on a website or exchanges of contact information over electronic communication) **and the limits in that regard** (respect of the principles of respectability, dignity, and security of the data subject).	**consistent with the principles of legality, legitimacy, and proportionality.** The Code also includes provisions regarding **monitoring systems** (section 13(4)) and pre-contractual relations (section 41). Section 41 states that **an employer may only demand, from a natural person seeking his/her employment, information relating to work that is to be performed**; section 13 (4) instead **prohibits employers to intrude upon the privacy of an employee in the workplace by monitoring him/her** – except for grave reasons linked to the specific character of the employer"s activities.	**DPA is described in Chapter 5 (sections 80-106) of the Personal Data Protection Act.** Relevant rulings of the Slovakian DPA in the employment context concern **the use of biometric data, such as fingerprints, for timekeeping purposes (IBL, s.r.o. v. Slovak Data Protection Authority).** Lastly, the Slovak DPA recently released **administrative practice guidelines on several subjects relating to the protection of workers' data** (e.g., monitoring devices at work; handling of employee health information).	
Spain	**The Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales,** which implements the GDPR, includes specific rules on **professional electronic devices (computer, phone, tablet, etc.), video surveillance and geolocation** (articles 87, 89, 90). In those articles the Spanish regulation allows employers to install this technology to monitor employees in the workplace, **following the principles of proportionality,**	According to Spanish freedom of association law, **employee consent is required for the processing of information on employer trade union-membership** (Article 11(2) Ley Orgánica 11/1985, de 2 agosto, de Libertad Sindical).	The **Spanish Data Protection Agency (AEPD)** is an administrative agency which has the authority to determine administrative penalties following the breach of data protection rights. **This agency has approved numerous guides, reports and decisions on data protection, including a Guide on data protection on labour relations in 2021.** The AEPD operates on a national level: however, in Spain **three additional autonomous agencies exist, which operate on a**	According to Spanish case law, **employers do not have the right to disclose employee personal data if this disclosure is unnecessary, also towards workers representatives.** In this sense, a massive request for employee personal data breaches personal data protection laws unless worker representatives provide justification for the same and detail the purpose of said processing (Judgement of the Constitutional Court 29/2008, of 28 January).

Co-funded by the European Union

	transparency and limitation of purposes. For example, in the case of video surveillance to monitor crimes by employees, there is no violation of the transparency principle if workers are properly warned of the presence of cameras.		**territorial level** (Autoridad Catalana de Protección de Datos, Agencia Vasca de Protección de Datos, Consejo de Transparencia y Protección de Datos of Andalusia).	Judgements have also been issued with regard to **information on trade union-membership** – which may not be processed to reduce the wage of employees who are trade union members when a strike is called (Judgement of the Constitutional Court 11/1998).
Turkey	The main Turkish data protection legislation is the **Personal Data Protection Law No. 6698** (KVKK, n.d.), which entered into force in 2016, and whose **general principles of lawfulness, proportionality, limitation of purposes and conservation period** are also applicable to the employment context. Namely, the Law states that **a data controller (and potential representatives) must be nominated in each workplace.** The data controller is obliged to provide the following information to data subjects (including employees) during the acquisition of personal data: **identity of the data controller and its representatives; purposes for which personal data can be processed and/or transferred; the subjects to whom personal data can be transferred; methods and legal basis for collecting personal**	**Article 75 of the Labour Act No. 4857** states that the employer should prepare a personal file for each of his employees, where he must keep all kinds of documents and records concerning them. **The employer is obliged to use the information obtained about the employee by the rules of honesty and law and not to disclose the information that the employee has a justified interest in keeping confidential.**	The Turkish data protection authority is the **Personal Data Protection Authority, whose decision-making body is the Personal Data Protection Board (KVKK)**. Many decisions of the Data Protection Board are aimed at solving disputes on personal data in the employment context. For example, through **Decision n. 2020/915** the KVKK stated that **the processing of fingerprints (biometric data) for overtime control is contrary to the principles of proportionality and purpose limitation** outlined in the Personal Data Protection Law. In addition, in 2023 the Board imposed **fines on a company that shared an applicant's CV with the other group companies through a mutual electronic platform without the applicant's consent.**	Issues concerning employees' data protection have recently been the object of decisions of the Turkish Constitutional Court. For example, in 2021, the court ruled that **there are no violations of the right to the protection of personal data and the freedom of communication due to the employer's monitoring of the applicant's corporate e-mail account**. However, in the same year, the Constitutional Court also stated that **terminating an employee's contract due to their employer accessing their WhatsApp messages violated the employee's right to privacy and freedom of communication.** For what concerns the Turkish Supreme Court, the most relevant decision in terms of data protection concerns the **employer's disclosure of an employee's confidential information**

Co-funded by the European Union

	data. These principles are also applicable when data processing activities are carried out under conditions different from the employee's consent, specifically indicated by the law (e.g., fulfillment of the data controller's legitimate interests; establishment of the employment contract)			**to a new employer, which was considered to have damaged the employee's rights** (Hukuki haber, n.d.).

2.2. The role granted to industrial relations actors and processes

Given the goal of the GDPiR project, i.e., endowing trade unions and workers' representatives with sufficient knowledge to have a proper voice with regard to employee data processing in the workplace, a relevant part of the research activities has been focused on investigating which provisions included in the national legislations of the 15 countries object of our research could be exploited to that end. In other words, in analyzing those legislative sources, we isolated and classified the provisions allowing industrial relations actors (trade unions; workers' representative bodies) a more or less substantial role on the topic – both through collective bargaining and/or information and consultation procedures. Lastly, building on the analysis of case law on data processing outlined in the previous subparagraph, the GDPiR research teams identified some strategic litigation trends which could be applied by workers' representatives in the different countries covered by our project. Here is a summary of the trends detected during the above-mentioned analysis.

- It is to be noted how only a few legislations among those analyzed explicitly endow trade unions and/or workers' representatives with the right to conclude collective agreements with regard to data processing in the workplace. (e.g., Czech Republic; Spain). In other cases (e.g., Germany; Italy) the stipulation of a collective agreement – including the conditions and limitations for data collection and use – is instead considered as a prerequisite for workers' data processing or for their remote monitoring. Lastly, some countries consider as sufficient legal basis for data processing – and thus not requiring additional testing – the specific provisions on the matter included in existing collective agreements (Denmark).

Co-funded by the European Union

- Information and consultation rights in favour of trade unions and workers' representatives appear to be more frequently included in national data protection legislations (and/or in nationally applicable collective agreements – see the case of Belgium).

With regard to information rights, it is to be noted how those are usually granted to company-level workers' representative bodies (Germany; Luxembourg; Slovakia; The Netherlands); however, these rights can be limited to specific issues, such as, for example, the profiling workers through algorithms or AI-powered tools (Spain) or the use of fully automated decision-making and/or monitoring systems in the workplace (Italy). Sometimes, however, information rights are also granted to trade unions (Hungary).

Consultation rights in favour of trade unions and workers' representative bodies are instead more rarely found in national data protection legislation. Those rights are sometimes enforceable only when the employer is taking a decision affecting a large group of employees (Hungary), when monitoring activities are concerned (France, Slovakia), or when the processing of particularly sensitive data (e.g., biometric data) occurs (Portugal); sometimes, the law states that the conditions and procedures for the consultation may also be included in collective agreements (Slovakia).

As with regard to trade unions' legal standing, they sometimes use strategic litigation[69] in order to safeguard their members' economic and social interests with concern to data protection (Hungary) or to sanction breaches of collective agreements regulating the matter (Denmark); strategic litigation has also been used to define the employer's refusal to provide information about automated decision-making or monitoring systems to territorial trade union members as anti-union behaviour (Italy). Lastly, in some countries workers' representative bodies can also turn to the National Data Protection Authority to exercise their information rights (Luxembourg).

[69] According to Dukes and Kirk (2023), in the field of labour law and work relations, strategic litigation may be broadly understood to encompass any legal action that is taken, defended or supported by a trade union acting in furtherance of aims that are broader than the dispute in question.

Co-funded by the European Union

	Role in data protection granted to collective bargaining in national law	Information and consultation rights foreseen by law in favour of trade unions and workers' representatives	Role of trade unions in engaging in strategic litigation to safeguard workers' data protection rights
Belgium	Other than by legislative instruments (see table above) **the processing of personal data in the workplace is governed by several collective agreements** – stipulated between 1998 and 2021 – dealing with a variety of issues, including for example camera surveillance, electronic on-line communication data, telework, etc. Naturally, **employees retain the rights granted them by the GDPR and all obligations imposed by the GDPR on data controllers and processor apply**; hence those not already enshrined in CLAs are derived from or imposed by the GDPR and relevant national legislation.	Article 9 of CLA No. 68 provides for an **information procedure prior to the installation of the camera surveillance**, while Article 10 defines a **prior consultation procedure**. With regard to control of online electronic communication data, CLA No. 81 also provides for **rules on information, both to the employees collectively and to the employees concerned individually,** and on consultation.	N/A
Czech republic	Trade unions have the **legal right to bargain with employers over issues relevant to the processing of employee data, including the use of new technology.** The **Czech Labour Code grants trade unions the right to take part in collective bargaining agreements** that address issues like working hours, pay, and working conditions and so **may contain clauses about data protection and emerging technology.**	N/A	N/A
Denmark	Section 12(1) of the Danish Data Protection Act provides an **automatic legal basis to process data which is already lawful processing under existing collective agreements**	N/A	Breaches of **collective agreements on employee control and monitoring**, or potential abuses of managerial prerogatives on the matter, **can be the object of trade union claims to the**

Co-funded by the European Union

	(e.g., the Control Agreement) or other statutory acts.		**Labour court, which can assess them as industrial disputes.**
France	N/A	According to the CNIL (see table above) **employee representative bodies must be informed and consulted** before any decision is taken to **install a listening or call-recording device in the workplace**. Similarly, art. L2312-38 of the Labour Code states that **the employee representation in the workplace (Comité social et économique – CSE)** must be informed and consulted **before any decision is taken to install cameras or automated personnel management processes in the workplace.**	N/A
Germany	According to Sec. 26 of the new BDSG (see table above), **the processing of personal data, including special categories of personal data of employees for the purposes of the employment relationship**, shall be permitted on the basis of **collective agreements.** Namely, **personal data of employees may be processed for purposes of the employment relationship** if this is necessary for the decision on the establishment of an employment relationship or, after the establishment of the employment relationship, for its implementation or termination or **for the exercise or fulfilment of the rights and obligations of the employees' representation resulting from a law or a collective agreement on wages, on company level or in the public sector.**	According to Sec. 26 of the new BDSG (see table above), when dealing with workers' data processing, **the participation rights of the employee representative bodies** (e.g., Betriebsräte – regulated by the Works constitution Act) **shall remain unaffected.**	N/A
Hungary	N/A	According to article 268, § 1, of the Hungarian Labour Code, **the employer shall consult the works council at least 15 days before taking a decision affecting a large group of employees**	As **works councils are not registered entities, they cannot turn to courts to safeguard Hungarian workers' data**, but only turn to

Co-funded by the European Union

		and especially when it comes to the introduction of new technology, upgrading existing technology, **the management and protection of employees' personal data, and the use of technical means to monitor employees.** Moreover, article 272 of Labour Code states that **the trade union may request information from the employer concerning the economic and social interests of the employees in connection with the employment relationship** (§ 4). Trade unions also have **the right to communicate their opinion on the employer's measure or decision and to initiate consultations on them** (§ 5), the right to represent material, social, life and health and safety rights of employees, as well as rights and obligations concerning their living and working conditions against the employer or its representative organisation (§ 6).	volunteer experts for advice and to the interest conflict reconciliation body. Works councils may exert pressure only via trade unions, which, according to article 272 of the Labour Code, **have the right to represent their members, in the defence of their economic and social interests before the courts, public authorities and other bodies** (§ 7).
Ireland	N/A	**Irish labour law does not provide trade union members or employee representatives any specific prerogatives in the field of workers' data protection.** However, the national transposition of Directive 2002/14/EC establishes **'Information and Consultation Forums', company-level bodies composed of elected workers' representatives, with the right of information and consultation on decisions likely to lead to substantial changes in work organisation,** (Employees (Provision of Information and Consultation) Act 2006 – Schedule 1, art. 3, lett. C)) **in accordance with the EC Directive (Art. 4, n. 2).**	N/A
Italy	**The introduction of technologies allowing an indirect monitoring of workers' activities in the workplace** – possible only for organisational, productive or safety-related purposes – **is conditional on the**	**Legislative Decree 104/2022** (see table above), **provides workers and their representatives with information rights regarding fullyautomated decision-making or monitoring systems in the workplace.** More specifically, it imposes employers 1) **to inform workers and their**	**Leg. Decree 104/2022, if applied in conjunction with other labour law provisions,** gives unions a useful instrument for the judicial defense of workers' data protection rights. For example,

Co-funded by the European Union

	stipulation of a company-level collective agreement between individual employers and workers' representatives. If the agreement is not reached, employers can only introduce those technologies after receiving authorisation by the Labor Inspectorate. However, **these conditions are not applicable to devices aimed at registering the access and presence of employees at work and for working tools potentially leading to workers' monitoring** (art. 4, Law 300/1970).	**representatives of the use of fully automated decision-making or monitoring systems** with an impact on the working relationship, together with **information regarding their exact functioning, purposes and level of security** – before the establishment of the working relationship itself 2) **to inform workers and their representatives of any variations in the use of those systems** at least 24 hours in advance 3) to **provide access to workers' data to workers and their representatives on their request.**	by applying art. 28 of the Workers' Statute, **unions have been able to make Italian courts recognize that the employer's refusal to provide information about automated decision-making or monitoring systems to territorial trade union members is to be considered anti-union behaviour** (Court of Palermo – Ruling n. 14491 of 2023). Moreover, trade unions also have the possibility to **report potential data protection legislation violations to the Italian Data Protection Authority.**
Luxembourg	N/A	L261-1 of the Luxembourg Labour Code states that, for **planned processing concerning employees' surveillance**, the joint staff committee, or failing this, the staff delegation, or the staff representative organisations **should receive prior notice and information from the employer**, which should include a detailed description of the purposes of the planned processing, as well as the implementing measures of the surveillance system and, if necessary, the length of and criteria for data retention, along with a formal commitment from the employer that the data collected will not be used for purposes other than those explicitly mentioned.	The staff delegation or failing this, the employees concerned**, can also submit a request to the National Data Protection Commission for a prior opinion on the compliance of the planned processing** for the purposes of surveillance of employees in the employment context. **Employees affected by the monitoring and/or surveillance mechanisms have the right to file a complaint at the CNPD.** The Labour Code explicitly provides that such a complaint cannot constitute a serious nor a legitimate reason for dismissal (L261-1).
Malta	N/A	**Maltese labour law does not provide trade union members or employee representatives with any specific prerogatives in the field of workers' data protection.** However, the national transposition of Directive 2002/14/EC **provides workers' representatives with the right of information and consultation**	N/A

Co-funded by the European Union

		on decisions likely to lead to substantial changes in work organisation, (Employee Information and Consultation Regulations – Subsidiary legislation 452.96 – art. 4, § 1, lett. C)) in accordance with the EC Directive (Art. 4, n. 2).	
The netherlands	N/A	In the Netherlands, **art. 27 of the Works Councils Act (WOR)** stipulates that "regulations relating to the **handling and protection of personal information of persons working in the enterprise requires endorsement (or consent) of the Works Council**" as well as "regulations relating to **measures aimed at or suitable for monitoring and checking the attendance, behaviour or performance of persons working in the enterprise**".	N/A
Portugal	N/A	Art. 18 of the Portuguese Labour Code states that **the notification to the National Data Protection Commission, referring to the processing of employees' biometric data** (see Table 1) **must be accompanied by an opinion from the works council** or, **if this is not available 10 days after consultation, proof of the request for an opinion.**	N/A
Slovakia	N/A	According to **Section 51 of the Slovak Labour Code**, **employers are required to consult with employee representatives, such as trade unions or works councils, regarding issues that affect the employee's interests:** this also covers the introduction of new technologies at work. Moreover, Section 54 also **requires employers to provide employee representatives with relevant information about the proposed changes**, including the reasons for the changes, the expected impact on workers, and any measures that will be taken to mitigate negative impacts – the employer must also give employee representatives the opportunity to express their views and provide feedback on the proposed changes.	N/A

Co-funded by the European Union

		The specific procedures and requirements for the consultation process may also be set out in collective agreements or other agreements between the employer and employee representatives. Lastly, section 13 (4) of the Labour Code states that, **if an employer implements a control mechanism, he/she shall consult with employees' representatives on the extent of the control**, its method of implementation and its duration.	
Spain	Following article 88 GDPR, art. 91 of the Ley Orgánica 3/2018 states that **collective agreements may increase the level of protection in matters of personal data protection of employees.** However, it is to be noted how **the Spanish Constitutional Court has recently devalued the power of collective agreements to provide improvements in personal data protection**, concluding that **those improvements have not been integrated into the personal data protection such as a human right** (Judgement 160/2021, 4 October) Moreover, according to article 64(9) of the Workers' Statute, **provisions of collective agreements may constitute the legitimate purpose of the transfer of employee personal data to workers' representatives**.	Article 64(4) of the Workers' Statute establishes that **workers' representatives must be informed by the company of the parameters, rules and instructions on which algorithms or artificial intelligence systems are based that affect decision-making** that may have an impact on working conditions, access to and maintenance of employment, including profiling.	N/A
Turkey	N/A	N/A	N/A

Co-funded by the European Union

MANAGING DATA PROCESSING
IN THE WORKPLACE THROUGH
INDUSTRIAL RELATIONS

THE ROLE OF INDUSTRIAL RELATIONS IN WORKERS' DATA PROTECTION AND PROCESSING

1. European trade union organisation's approach and practices

IndustriAll Europe is the European trade union federation representing workers in the manufacturing sector. From the interviews conducted with two IndustriAll Europe representatives, it emerges that the trade union considers data processing and the whole digital transformation as a priority. The issue is perceived as cross-cutting different organisational departments, including the Industrial Policy Department, which focuses on developmental policies, and the Collective Bargaining Department, which deals with more social and labour issues and industrial relations practices. This is also the reason behind the absence of a specific unit dedicated to digitalisation and instead, the presence of a team gathering around three people coming from the above-mentioned departments. IndustriAll Europe's commitment to workers' data protection and processing has strengthened with the adoption of the GDPR.

> For us digitalisation is a horizontal issue with files which could be more industrial policy oriented and other more focused on social issues. And that's why we don't have one specific department exclusively dealing with digitalisation, but we are working together as a team comprising people from various departments (IndustriAll Europe senior policy advisor).

Today, IndustriAll Europe operates in this field mainly by providing information, training and guidance for its affiliated trade unions. Indeed, the interviewees report a lack of good practices of industrial relations and collective bargaining in the sectors covered by the European trade union federation, although some problems related to workers' surveillance have already emerged, for instance, in the mechanical engineering industry.

> The best practices I know do not generally come from our sectors. And this is why we have started awareness-raising activities. We have the feeling that since the adoption of the GDPR and with the Covid-19 pandemic, digitalisation and data processing have accelerated in European companies, but we don't see agreements on these issues. We are still waiting (IndustriAll Europe senior policy advisor).

Co-funded by the European Union

> In a multinational company, for instance, a problem emerged in relation to the instalment of a software notifying mechanical engineers of the need of maintenance of specific lifts. However, this software allowed the company also to track the time spent by single employees carrying out the maintenance on the lift, with serious implications in terms of additional pressures on workers (IndustriAll Europe policy advisor).

An important example in the area of information and training is provided by a project initiated by IndustriAll Europe in 2022 in collaboration with the Competence Center – Future of Work of the Friedrich-Ebert-Stiftung, which implied the organisation of a Spring School in March 2022 in Florence (Italy) on collective bargaining and digitalisation, an online workshop in June 2022 on GDPR with a researcher from the European Trade Union Institute (ETUI) and a training session in September 2022 in Bratislava (Slovakia), specifically focused on how the GDPR can be used in collective bargaining. The project is now continuing with the development of a toolbox for bargainers in the context of digitalisation. Though not targeted at national trade unions, some recommendations were also produced in December 2020 by IndustriAll Europe with the aim to provide EWCs with key suggestions on how to interact with central management on issues related to digitalisation and artificial intelligence. Analyses on the impact of digital transformation on the world of work and recommendations targeted to trade unions have also been produced within the framework of the project *Making digitalisation work for industrial workers*, which was conducted from 2018 to 2020 in collaboration with the European consulting firm, Syndex. Further collaborations with research centres and universities are also activated by IndustriAll Europe in EU-cofunded projects.

As regards IndustriAll Europe's involvement in lobbying activities, it is worth mentioning the various position papers issued on the topic of digitalisation (for instance, in June 2022, a position paper on artificial intelligence was adopted with the title *All eyes on AI*), as well as the participation of the European trade union federation in public consultation procedures on EU regulations, the formulation of letters addressed to EU lawmakers and the organisation of events with the participation of rapporteurs and co-rapporteurs, like the one organised on the Artificial Intelligence Act at the presence of the member of the European Parliament, Brando Benifei.

With reference to social dialogue structures and procedures, the European trade union participates in more than ten sectoral committees, where digitalisation is high on the agenda. In some industries, joint statements with European employers'

federations came out from the meetings of these committees. Examples are the joint position *The impact of digitalisation on the world of work in the met industries* concluded in November 2020 with the European employers' association CEEMET, and the statement signed in July 2022 for the TLCF (textiles, clothing, leather, and footwear) sectors on green and digital transitions. Importantly, from 2018, European social partners in the TLCF sectors have also carried out an Erasmus Plus project for the development of digital competences (*digitaltclf.eu*). Similarly, IndustriAll Europe and the European Chemical Employers Group (ECEG) jointly conducted a project named *Digital Transformation in the Chemical Industry* from January 2018 to December 2019. Moreover, IndustriAll Europe participated in the negotiations of the European Autonomous Framework Agreement on Digitalisation, signed in June 2020 by the European Trade Union Confederation (ETUC), which IndustriAll Europe is part of, and the employers' associations, BusinessEurope, Ceep and SmeUnited, and it is now working on the monitoring of this agreement's implementation in single EU member states. However, as regards transnational corporate agreements possibly signed in multinational companies by IndustriAll Europe and with a focus on digitalisation and data processing, the two interviewees do not report any experiences.

Overall, in relation to data protection and processing, IndustriAll Europe is making efforts to convey the idea that the GDPR is not negative for workers and by contrast, it can be a resource for worker representatives at the bargaining table to protect workers' data and have a say in this field. Practice-oriented events and publications on this issue are therefore sought by the European trade union and largely welcome by national affiliates. Unfortunately, IndustriAll Europe's ability to effectively engage national trade unions in these activities is not always constant.

> The problem sometimes relates to the engagement of national trade unions, which acknowledge the importance of the issue but say that it is not a priority at the moment. I understand that with the outbreak of the war in Ukraine and the rising inflation, our affiliates' interests have shifted to other problems. But this situation makes more difficult for us to organise activities and initiatives on data processing and protection (IndustriAll policy advisor).

Co-funded by the European Union

2. Institutional features of industrial relations in the manufacturing sector across countries

Going down to the national level, our analysis has concentrated on the following 15 countries: Belgium, Czech Republic, Denmark, France, Germany, Hungary, Ireland, Italy, Luxembourg, Malta, the Netherlands, Portugal, Slovakia, Spain and Turkey. According to the classification of industrial relations regimes prepared by Jelle Visser for the European Commission in 2009 and further developed by Eurofound (Caprile *et al.*, 2018), these countries belong to all five different identified clusters. We assume that these institutional features, complemented with the various legal frameworks on workers' data protection and processing (previously described), exert an influence on the role of trade unions and industrial relations in these topics.

Notably, Denmark is classified as an 'organised corporatism' model, displaying relatively high rates of employers' association (53% in the private sector) and trade union density (68%) as well as collective bargaining coverage (74% in the private), and boasting a long tradition of tripartite social dialogue over major economic and social issues and a significant degree of autonomy from the state as regards collective bargaining structure (which is three-tier) and dynamics.

Belgium, Germany, Luxembourg and the Netherlands are classified as 'social partnership' models, given their structural social partner integration in public policy making via tripartite or bipartite advisory bodies at the national and/or regional level. Collective bargaining coverage rates are generally high, even with differences between Belgium (97% in the whole economy) and the Netherlands (91% in the whole economy) on the one hand, and Germany (46% in the manufacturing sector) and Luxembourg (55% in the private sector) on the other hand. Moreover, Germany and the Netherlands share a dual channel of labour representation, with trade unions operating at the sectoral level (via collective bargaining) and works councils operating at the company level (via information, consultation and codetermination rights), although the role of trade unions in companies has increased over the past decades due to the introduction of derogatory opportunities for company-level collective bargaining. In Belgium and Luxembourg, instead, workplace labour representation appears to be more influenced by trade unions and collective bargaining occurs at three different levels (cross-sectoral, sectoral and company). Finally, union density is quite high particularly in Belgium (55% in the whole economy), compared with Luxembourg (32% in the whole economy) and the Netherlands (18%

Co-funded by the European Union

in the whole economy). Despite the poor figure in the whole economy (17%), German trade unions still boast a high-density rate in the manufacturing sector (55%). France, Italy, Portugal and Spain are considered as 'state-centred' models, although the role of the state in industrial relations is significantly lower in Italy than in the other countries. They are all characterised by union pluralism and quite low trade union density rates (31,4% in Italian manufacturing sector; 13% in Spain; 11% in France and 8% in Portugal). By contrast, collective bargaining coverage rates are pretty high, amounting to around 90% or more in all four countries, which also share a multi-tier and (largely) coordinated collective bargaining structure.

Ireland and Malta are regarded as 'liberal pluralism' models, both displaying quite low rates in trade union density (19% in Irish manufacturing sector and 40% in Malta's economy) and collective bargaining coverage (34% in Ireland and between 50% and 60% in Malta), a collective bargaining structure centred on company level, the presence of tripartite advisory forums on economic and social issues at national level, and a workplace labour representation ensured via shop stewards.

Czech Republic, Hungary and Slovakia are described as 'transition economies'. They are all characterised by low rates of trade union density (11% in Czech Republic, 17% in Hungary and 13% in Slovakia) and collective bargaining coverage (33% in Czech Republic, 18.5% in Hungary and 47% in Slovakia's private sector), a collective bargaining structure largely centred at company level, although sectoral collective bargaining occurs in some manufacturing industries in Slovakia and Czech Republic, and the presence of tripartite advisory bodies at the national level, despite their contested influence in both Hungary and Slovakia.

Finally, Turkey is not included in the typology of industrial relations regimes provided by Eurofound, since it is not an EU Member State. Industrial relations in Turkey are not particularly developed, with very low rates of trade union density (less than 5% in the private sector) and collective bargaining coverage (between 10% and 15% in the private sector), and collective agreements being signed only at establishment level. However, there are tripartite bodies aiming at guaranteeing a certain degree of social partner involvement in public policy making.

Co-funded by the European Union

	Trade union and employer representation and their density	Role of social partnership in public policy and role of the state in industrial relations	Collective bargaining structure and coverage	Workplace level representation and industrial relations procedures
Belgium ('social partnership' model in the centre-west cluster)	**Union pluralism. Three main trade union confederations** (ACV-CSC, ABVV-FGTB, ACLVB-CGSLB) and three main employers' confederations (FEB-VBO, UNIZO, UCM) with federations operating in the manufacturing sector. **Union density (not specifically in the manufacturing sector): 55%.**	**A number of bipartite or tripartite national/regional bodies with advisory powers in governmental policies.** Notably, within the National Labour Council, employers' confederations and trade unions can reach agreements, which can be transposed into law. Integration of Belgian social partners in the social security system with trade unions playing a role in the organisation and payment of unemployment benefits.	**Three-tier structure, with collective bargaining taking place at the cross-sectoral** (both national and regional, via bipartite or tripartite councils and bodies), **sectoral** (via bipartite sectoral committees) **and company level. Collective bargaining coverage (not specifically in the manufacturing sector): 97%.**	**Workplace labour representation is ensured via works councils, trade union delegates, and committees for prevention and protection at work,** both composed of managers and workers' representatives.
Czech Republic ('transition economies' model in the centre-east cluster)	**Two main trade union confederations** (ČMKOS, ASO), **with affiliates in the manufacturing sector.** Problems related to the proliferation of trade unions, given the very low threshold set for creating one. **Two main employers' confederations. Union density (not specifically in the manufacturing sector): 11%. Employers' association density (not specifically in the manufacturing sector): 67%.**	**There is a tripartite Council of Economic and Social Agreement, which in the early 1990s set a general framework for collective bargaining.** Today, it still plays a role in influencing governmental social and economic policy.	**Very decentralised structure, with collective bargaining taking place mainly at company level, although sectoral-level collective bargaining occurs in some industries** (e.g., glass and ceramics, textile, etc.). Problems of coordination. Trade unions often opt for legislative solutions for improving labour conditions. **Collective bargaining coverage (not specifically in the manufacturing sector): 33%.**	**Workplace labour representation is ensured via trade unions.**
Denmark ('organised corporatism' model in the	**One main trade union confederation** (FH), which CO-industri, operating in the	**The state has a relatively withdrawn role in the regulation of the Danish labour market.** It delivers	**Three-tier structure, with collective bargaining taking place at cross-**	**Workplace labour representation is ensured via trade unions.** Cooperation

Co-funded by the European Union

nordic cluster)	manufacturing sector, is affiliated to. Members of CO-industri are some big unions like the United Federation of Danish Workers (3F), the Danish Metalworkers' Union (Dansk Metal) and the private branch of Union of Commercial and Clerical Employees in Denmark (HK Privat). **One main employers' association in the manufacturing sector** (DI). **Union density (not specifically in the manufacturing sector): 68%. Employers' association density in the private sector: 53%.**	a framework for collective bargaining with legislation on labour market issues, but as far as the social partners delivers responsible results, the state does not interfere. **However, tripartite cooperation and regulation plays an important role** in Danish industrial relations, especially when major welfare state issues are at stake (i.e. pension, paternity leave, vocational training). Quite often, the state, employers' organisation and trade unions work out solutions that divide the responsibility between collective agreements and legislation.	**sectoral, sectoral and company level. Collective bargaining coverage in the private sector: 74%.**	committees are the main information and consultation bodies at workplace level, and they are composed of trade union representatives and managers.
France ('state-centred' model in the south cluster)	**Union pluralism**, with different confederations (CGT, CFDT, FO, CFTC and CFE-CGC). **One main employers' association in the manufacturing sector**, UIMM, which is affiliated to MEDEF. **Union density (not specifically in the manufacturing sector): 11%.**	**Strong role of the state in French industrial relations and collective bargaining.**	**Two-tier structure, with collective bargaining taking place at sectoral** (either territorial or national) **and company level.** Articulation recently shifted from a hierarchical principle (with company-level which could only improve sectoral standards) to a distribution of topics (with topics on which the sector prevails and others, many more, on which the company prevails). **Collective bargaining coverage in the private sector: 96%.**	**Workplace labour representation is ensured via trade unions and structures elected by the whole workforce.** In the private sector, these structures merged into one following a 2017 reform.

Co-funded by the European Union

Germany ('social partnership' model in the centre-west cluster)	**One main trade union federation in the manufacturing sector, IG Metall,** which is affiliated to DGB. **One main employers' association in the manufacturing sector, Gesamtmetall**, which is affiliated to BDA. **Union density in the metal sector: 58%** (well above union density in the whole economy which is less than 17%). **Employers' association density in the metal sector: 47%.**	**The collective bargaining and codetermination system is regulated by law.** However, rules of articulation between different levels of industrial relations are also set out in collective agreements. Social partners are strongly integrated in public policy making.	**Traditionally, dual system of industrial relations, with collective bargaining** (by trade unions) **taking place at sectoral level and codetermination** (by works councils) **occurring at company level. More recently, there has been a decentralisation trend** towards, on the one hand, more regulatory responsibilities for works councils and on the other hand, derogatory opportunities for collective bargaining (by trade unions) at company level. **Collective bargaining coverage in the manufacturing sector: 46%.**	**Workplace labour representation is ensured via works councils,** which are endowed with information, consultation and codetermination rights.
Hungary ('transition economies' model in the centre-east cluster)	**Fragmentation of the trade union scene. Union density in industry: 7.1%.**	**Tripartite advisory bodies at national level merely have a symbolic character**.	**Only company-level collective bargaining or, at best, multi-company collective bargaining. Collective bargaining coverage in industry: 18.5%.**	**Dual channel of workplace labour representation: either via representative trade unions or works councils.**
Ireland ('liberal pluralism' model in the west cluster)	**One trade union confederation, to which both SIPTU and Connect (operating in the manufacturing sector) are affiliated to.** In addition to them, the British organisation Unite the Union may also operate in Irish companies. **One major cross-sectoral employers' associations (IBEC)**.	**Very voluntaristic and autonomous collective bargaining system**. During the national social partnership period (1987-2009), national tripartite agreements set out minimum social and labour conditions. Such social partnership model does not exist today, although **there are advisory tripartite forums at national level**.	**One-tier collective bargaining structure, centred on company-level.** Some sort of coordination on wage regulation is ensured via pattern bargaining, according to which the pay deals reached in pharmaceutical and chemical companies progressively set the trend in other companies and industries.	**Workplace labour representation is ensured via shop stewards**, that are workers delegated by sectoral trade unions and strongly connected with them.

Co-funded by the European Union

	Union density in the manufacturing sector: around 19%. **Employers' association density in the private sector (in terms of workers covered): 70%.**		**Sectoral Employment Orders (SEOs)**, made by the Ministry of Labour following recommendations of the Labour Court (upon request of social partners), set some minimum terms and conditions of employment (e.g., sick, pensions, etc.) in the manufacturing sector. **Collective bargaining coverage (not specifically related to manufacturing sector): 34%.**	
Italy ('state-centred' model in the south cluster)	**Union and employers' association pluralism** with various associations on both sides. **Union density in the manufacturing sector: 31,4%.** **Employers' association density in the manufacturing sector (in terms of companies covered): 50%.**	**High degree of autonomy of industrial relations from the national legislation** (no legal extension mechanism of collective agreements). However, in the 1990s, tripartite cross-sectoral agreements outlined the general features of the collective bargaining system. During the last 40 years, **Italian legislators have progressively delegated some of their specific functions in labour regulation to social partners and collective bargaining**.	**Two-tier collective bargaining structure** (with 1. national sectoral and 2. company-level collective agreements). **Articulation between levels follows (at least formally) the principles of delegation and derogation, controlled by the national level**. Art. 8 of Law 148/2011 allows territorial and company-level agreements to deviate, under certain limits and conditions, from national contractual and legislative provisions. A single-employer collective bargaining structure only applies to Fiat (now Stellantis) after its exit from the main employers' association in the metal sector and its withdrawal from the main national sectoral agreement.	**RSU is the main workplace labour representation** body and it can be set up in productive units with more than 15 employees. Its members are elected by the workforce on the basis of a list of candidates proposed by the trade unions. **RLSs are workers' representatives for safety** that must operate in each workplace, according to law.

Co-funded by the European Union

			Sectoral collective bargaining coverage is often esteemed above 90%. Decentralised collective bargaining coverage in the manufacturing sector is about 30/40%.	
Luxembourg ('social partnership' model in the centre-west cluster)	**Union pluralism**, with three main trade union confederations with affiliates operating also in the manufacturing sector. **Union density (not specifically in the manufacturing sector): around 32%.**	**Unions hold seats in the Chamber of Employees (CSL), which has an important role in influencing economic and social public policy**, along with the employers' chamber. Traditionally, employment legislation is adopted via tripartite consensus between the government and employees' and employers' representatives.	**Three-tier structure, with collective bargaining taking place at cross-sectoral** (also with the government for major economic and social issues)**, sectoral and company level. The relative importance of sectoral and company-level collective bargaining varies across sectors.** Some sectors are covered by sectoral agreements (whose efficacy is extended to all employees by government); other sectors are only covered by company-level agreements. **Overall, there are no functional links between sectoral and company-level provisions.** **Collective bargaining coverage in the private sector: 55%**	**Workplace labour representation is ensured via an employee delegation,** composed of representatives (most of them are union members) elected by all employees.
Malta ('liberal pluralism' model in the west cluster)	**Three main trade unions** operating in the manufacturing sector: GWU, UHM and FOR.U.M. **Two main employers' associations**: Malta Chamber of SMEs and Malta Employers' Association (MEA). **Union density (not specifically in the**	**There are a few tripartite social dialogue bodies at national level**: the Malta Council of Economic and Social Development (MCESD) and the Employment Relations Board (ERB), which makes recommendations on	**One-tier collective bargaining structure, centred on company level.** **Collective bargaining coverage (not specifically related to manufacturing sector): around 50/60%.** For workers not covered by collective bargaining,	**Workplace labour representation is essentially ensured via shop stewards** (trade union delegates), although it is legally possible for non-unionised workers to elect a non-unionised representative.

Co-funded by the European Union

	manufacturing sector): 40%.	national standards of employment.	government-issued **Wage Regulation Orders** (covering e.g., minimum pay rates, overtime pay, annual leave rights) and/or **National Regulation Orders** (covering e.g., pay indexation) apply.	
The netherlands ('social partnership' model in the centre-west cluster)	**Union pluralism** with different organisations operating in the manufacturing sector (belonging to FNV, CNV and De Unie). **Union density (not specifically in the manufacturing sector): 18%.**	**There is a tripartite body, the Social and Economic Council, composed of social partners' representatives**, which is a major economic advisory council to the government.	**Collective bargaining mainly occurs at industry level, although many large firms in the manufacturing sector have their own company-level agreement and do not apply any sectoral agreement (single-employer bargaining).** In the other cases, company agreements with works councils can improve standards set at industry level. Derogations are also possible in some cases. **Collective bargaining coverage (not specifically in the manufacturing sector): 91%.**	**Workplace labour representation is ensured via works councils.**
Portugal ('state-centred' model in the south cluster)	**Two main trade union confederations** (CGPT and UGT), with federations also operating in the manufacturing sector. **One employers' organisation**: Confederation of Portuguese Business. **Union density (in the private sector): around 8%.**	**Different channels for tripartite dialogue**: e.g., the Standing Committee for Social Concertation, composed of representatives from trade unions, employers' associations and public administration, which issues opinions and evaluates legislative proposals; the Consultative Council for the Promotion of Health and Safety, composed	**Three-tier structure, with collective bargaining taking place at sectoral, multi-company** (between companies with relatable conditions) **and company level. Usually there are no functional links between sectoral and company agreement.** When there are competing agreements, lower-level agreements take	**Dual channel of workplace labour representation via works councils** (though low in number and essentially provided with information rights) **and trade union delegates** (who can sign agreements with the employers). There are also health and safety representatives.

Co-funded by the European Union

		of trade unions and employers' representatives and dedicated to health and safety related issues.	precedence over higher-level ones. Industry-level agreements are more important in terms of covered employees. **Collective bargaining coverage (not specifically in the manufacturing sector): 92%.**	
Slovakia ('transition economies' model in the centre-east cluster)	**One main trade union confederation (**KOZ SR), with OZ KOVO federation representing workers in the manufacturing sector. **Union density (not specifically in the manufacturing sector): 13%. Employers' association density (not specifically in the manufacturing sector): above 30%.**	**There is a tripartite Economic and Social Council**, which discusses government policies and proposes legislation on economic and social issues. However, its influence is declining.	**Sectoral-level collective bargaining is important** (also in the manufacturing sector), **but company-level collective bargaining is increasing. Collective bargaining coverage in the private sector is falling: 47%.**	**Dual channel of workplace labour representation: either via representative trade unions or works councils.** However, it is much more usual to have a union than a works council.
Spain ('state-centred' model in the south cluster)	**Union pluralism** with two main federations in the manufacturing sector (UGT-FICA and CCOO Industria). **Two main employers' confederations representing respectively large and small and medium companies** (CEOE and CEPYME). **Union density (not specifically in the manufacturing sector) 13%.**	**Participation of social partners in public policy is limited, depending on the governmental attitude.** At the local level, though, there are a number of tripartite industrial dialogue forums.	**Three-tier structure, with collective bargaining taking place at cross-sectoral** (national), **sectoral** (national and territorial), **company and workplace level. Sectoral agreements take precedence over company agreements.** Deviations from sectoral standards are however possible at company level. **Collective bargaining coverage in industry: 87%.**	**Workplace labour representation is ensured via either employee delegates** (in companies with less than 50 employees) **or company committees** (in companies with at least 50 employees). Health and safety representatives as well as equality delegates may be constituted too.
Turkey	**Three main trade union confederations** (Türk-İş, DISK and Hak-İş) **and further independent trade unions.** In the	**Industrial relations and collective bargaining are highly governed by law.** There is a tripartite Economic and Social	**One-tier collective bargaining structure, centred on company or establishment level.**	**Workplace labour representation is ensured via shop stewards** (trade union delegates), **or, in their absence, voluntary**

Co-funded by the European Union

	metal sector, important associations are Turk Metal (on the labour side) and MESS (on the employers' side). **Union density in the private sector: less than 5%.**	Council, aimed at integrating social partners in policy making. There is also a tripartite Minimum Wage Setting Commission.	**Collective bargaining coverage in the private sector: 10/15%.**	**boards or commissions composed of managers and workers' representatives.**

3. National trade union organizations approach towards workers' data protection and processing

As was stated in the previous section, the GDPR provides for powerful means to monitor the processing of workers' personal data. First of all, the reasons for the processing of personal data are limited. This means the processing takes place with the consent of the data subject(s) concerned. Lacking consent, the processing of personal data can be allowed if there is a contractual or legal obligation, if it is done in the public interest or to protect the vital interests of an individual or if there is a legitimate interest (cf. Recital 40 and Article 6 (*Lawfulness of processing*) GDPR). However, these grounds all need to be interpreted restrictively and need to meet specific conditions, depending on the processing they are put forward to motivate.
For instance, the GDPR is extremely suspicious of consent as a legal ground for the processing of personal data. To be in accordance with the GDPR, consent will be valid only if it can be proven, is freely given, informed, specific and unambiguous and obtained by a clear affirmative action. When consenting to the processing of personal data is part of a document containing other clauses, it must be clearly distinguishable, easily intelligible, and easily accessible (cf. Articles 4(11) (*Definitions*), 7 (*Conditions for consent*) and Recitals 32 and 42 GDPR).
Of particular interest for the processing of workers' personal data are the principles set out in Recital 43: "In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller […]. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the

Co-funded by the European Union

provision of a service, is dependent on the consent despite such consent not being necessary for such performance".

It is clear in the vast majority of cases workers' consent will not be a sufficient legal ground for the processing of their personal data[70]. In its Opinion 2/2017, the European Article 29 Working Party, dealing with the subject of employers' legitimate or legal grounds to process employees' personal data expressed reservations regarding workers' consent as a sound legal ground: "According to the Working Party, employees are rarely in a position to freely give, refuse or withdraw their consent, given their dependency in the employment relationship. It is therefore considered that employers should rely on other legal grounds"[71]. To conclude this brief discussion

[70] Nevertheless, the new German Data Processing Act does mention employees' consent as a legal ground: "If the processing of personal data of employees is based on consent, the assessment of the voluntariness of the consent shall in particular take into account the dependency of the employee in the employment relationship as well as the circumstances under which the consent was given. Voluntariness may exist in particular if a legal or economic advantage is achieved for the person employed or if the employer and the person employed pursue similar interests. Consent must be given in writing, unless another form is appropriate due to special circumstances. The employer shall inform the data subject in text form about the purpose of the data processing and about his or her right of withdrawal in accordance with Article 7(3) of Regulation (EU) 2016/679" (GDPiR National Report on Germany, cit., p. 23), which, after all, is not contrary to what is stated in Recital 155 GDPR, which surprisingly *does* mention consent… Unfortunately, it falls outside the scope of this report to identify the source and reasoning behind said Recital mentioning consent as a potential legal ground for the processing of workers' personal data or which amendments from which MEPs might have been in play. Suffice it to say the original Recital in the Proposal is significantly different from the final one. Compare Recital 124 of the Proposal of the GDPR ("The general principles on the protection of individuals with regard to the processing of personal data should also be applicable to the employment context. Therefore, in order to regulate the processing of employees' personal data in the employment context, Member States should be able, *within the limits of this Regulation*, to adopt by law specific rules for the processing of personal data in the employment sector"; emphasis added) to the final version (Recital 155 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, 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, 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").

[71] GDPiR National Report on Belgium, p. 24. *Contra*, the advice of the Council of the Order of Barristers of the Luxembourg Bar to the *Projet de loi 7184, Projet de loi portant organisation de la Commission nationale pour la protection des données et mise en oeuvre du règlement (UE) 2016/679 du Parlement*

on the matter of consent as a legal ground for the processing of personal data, it should be recalled data subjects have the right to withdraw consent at any time[72]. In 2020, the European Data Protection Board (EDPB) reiterated said reservations: "An imbalance of power also occurs in the employment context. Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent. Therefore, the EDPB deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee" (EDPB, 2020, § 21, p. 9)[73].

---

européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat: see the Dossier consolidé. Projet de loi 7184, 12 September 2017, p. 409. The Council of the Order of Barristers of the Luxembourg Bar was of the opinion said consent is possible under the GDPR. The Council referred to the part of the 2017 WP29 advice which, according to the Council states that the consent of the employee may be taken into account in certain specific cases and as such, the "outright exclusion of employee consent as a basis for legitimacy of employee monitoring is therefore in contradiction with the clear position of the Article 29 Working Party" (GDPiR National Report on Luxembourg, p. 25, footnote 93).

[72] Cf. Article 7(3) GDPR.

[73] Also see the references there cited. The EDPB does leave room for exceptional situations in which an employer could rely on employees' consent: "There may be situations when it is possible for the employer to demonstrate that consent actually is freely given. Given the imbalance of power between an employer and its staff members, employees can only give free consent in *exceptional circumstances, when it will have no adverse consequences at all* whether or not they give consent" (EDPB, 2020, § 22, p. 9, emphasis added). The example the EDPB gives, is indicative for how exceptional such situations are: "A film crew is going to be filming in a certain part of an office. The employer asks all the employees who sit in that area for their consent to be filmed, as they may appear in the background of the video. Those who do not want to be filmed are not penalised in any way but instead are given equivalent desks elsewhere in the building for the duration of the filming" (*ibidem*, 23, p. 9).

Co-funded by the European Union

It is clear some contractual obligations can allow or oblige the processing of workers' personal data, for instance for the payment of wages, etc. As there are many legal obligations to do so, for instance for the correct payment of social security contributions, taxes, etc. However, one of the core principles of the GDPR states data can only be lawfully collected "for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" (Article 5(1) GDPR: the so-called principle of 'purpose limitation').

The most problematic motivation for the processing of workers' personal data by employers is that of 'legitimate interest', a discussion so vast and depending on so many factors, it falls outside the scope of this report. Nevertheless, it is clear workers' personal data must be processed at all times with respect for and in accordance to the core principles of the GDPR, set out in, inter alia, in Chapter II, *Principles* (Articles 5-11 GDPR). Moreover, specifically for the processing of personal data in the context of employment, Article 88 provides "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, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place" (Article 88(2) GDPR). As mentioned before, the advisability of specific rules at the national level, leaves room for a debate which falls outside the scope of this report.

But what means do trade unions and workers' representatives have for monitoring workers' personal data is being processed and whether said processing is compliant with the GDPR?

To answer this question, we must look at the different levels trade unions can be active: the national, the sector and the company level.

At the national level, trade unions will lobby in order to influence new legislation. In many cases, such lobbying is, as is most lobbying, of an informal nature. In some Member States, lobbying can be part of a formal structure. In Luxembourg, for instance, all employees are mandatory members of the Chambre des salariés (CSL)[74] which has a voice in the legislative process and in the socio-economic institutions of the country through inter alia issuing opinions on draft laws[75]. Another example of where opinions of social partners are formally taken into account in the legislative process, is the National Labour Council in Belgium[76]. Of course, lobbying and advising

[74] See www.csl.lu.

[75] See the section *Missions and activities*, in www.csl.lu.

[76] Cf. GDPiR National Report on Belgium, cit., p. 30.

Co-funded by the European Union

at the national level are of importance when, for instance, legislation implementing art. 88 GDPR is either up for draft or amendment.
Apart from lobbying, there are also forms of social dialogue at the national level[77]. Again, the National Labour Council in Belgium can serve as an example since CLA's on the processing of workers' personal data were concluded in its bosom[78].
Also at the sector level, social dialogue can also lead to the conclusion of CLA's. However, those seem to be rare or non-exist in the Member-States research.
On the company level, whenever possible, trade unions and workers' representatives will try to rely on the social dialogue and 'talking things through' with the employer. However, it was reported in many if not the majority of cases, social dialogue fails in the field of data processing. In many cases, the employer refuses to supply information, supplies insufficient or incomplete information or stalls. Some employers downright refuse talking about the processing of workers' personal data or try to turn the tables stating the GDPR does not allow them to discuss the subject. A good practice identified are German trade unions who will engage external consultants, both legal and ICT-experts, to assist workers' representatives assimilate and evaluate information provided by the employer, for instance in the framework of works council meetings[79]. Seeking advice from ICT-experts is a particular good practice, since the processing of personal data and the monitoring of the lawfulness of said processing is not only a serious legal matter, but said monitoring must also take place at the technical level, or else one can only 'take the other's word for it'… And as the now infamous saying goes: 'Trust but verify!'. Let's not forget, and such was reported in both interviews and surveys, that there is a lack of knowledge[80] – or data literacy – also (and according to some, mostly) on the employers' side[81]. After all, the good practice identified in Germany referred to above is limited to (very) large companies, where Mitbestimmung actually works, and trade unions and employees' representatives stand strong. As was reported in interviews, said practices are much rarer to totally absent in SMEs, where trade unions are smaller, employees' representatives are weaker and the support budgets for ICT are also much smaller, if not absent, than in large companies. But, to the extent there is proper social dialogue, also on the subject of the processing of workers' personal data, jointly looking into both the legal and technical aspects of said processing is a best

[77] See, for instance, the GDPiR National Report on Turkey, pp. 27-28.
[78] Cf. GDPiR National Report on Belgium, cit., pp. 4-5 and 15 ff.
[79] Cf. GDPiR National Report on Germany, cit.
[80] See, for instance, the GDPiR National Report on Italy, pp. 26 and 30-31.
[81] And of data awareness (at both sides) but that is another matter.

Co-funded by the European Union

practice. Another good practice was identified in Italy where some employers conclude more than one CLA regarding the processing of workers' personal[82].

In Luxembourg, prior to the entry into force of the GDPR, the processing of workers' personal data was subject to an *ex ante* control mechanism by the Luxembourg National Data Protection Commission. In their opinion regarding the proposal for a new Act regarding data protection pursuant to the entry into force of the GDPR, the Council of Barristers, stating the GDPR also provides *ex ante* measures made reference to Article 35 GDPR[83] which imposes an obligation to carry out a Data Protection Impact Assessment where "a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1) GDPR). A DPIA is an "assessment of the impact of the envisaged processing operations on the protection of personal data" and must be carried "out prior to the processing" (Article 35 (1) GDPR). Furthermore, the Council of Barristers' advice also refers to the Article 29 Working Party *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. In said guidelines, the WP29 clarifies that "the reference to 'the rights and freedoms' of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience, and religion" (*ibidem*, p. 6). More importantly, the said WP29 guidelines point out that "The mere fact that the conditions triggering the obligation to carry out DPIA have not been met does not, however, diminish controllers' general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects. In practice, this means that controllers must continuously assess the risks created by their processing activities in order to identify when a type of processing is 'likely to result in a high risk to the rights and freedoms of natural persons'" (*idem*).

In Germany also, the DPIA is considered an important tool. In 2018, the Datenschutzkonferenz (DSK) published a (non-exhaustive) 'DPIA blacklist' (DSK, 2018) for the private sector (Article 35(4) GDPR)[84]. This list contains 17 types of data processing operations which require a DPIA (DSK, 2018). The DSK has also issued

[82] GDPiR National Report on Italy, cit., p. 24.
[83] Cf. GDPiR National Report on Luxembourg, cit., p. 22.
[84] Cf. Mueller (2018).

practical guidance on how to carry out a DPIA (DSK, 2017)[85]. Controllers are required to consult the Federal Commissioner for Data Protection and Freedom of Information (BfDI)[86] prior to processing which will form part of a new filing system if a DPIA indicates that the processing would result in a substantial risk to the legally protected interests of data subjects in the absence of measures taken by the controller to mitigate the risk; o the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a substantial risk to the legally protected interests of data subjects. If the BfDI believes that the planned processing could violate the law, in particular, because the controller has not sufficiently identified the risk or has not taken sufficient measures to mitigate the risk, the BfDI may provide the data controller and/or processor with written advice as to measures which should be taken within a period of six weeks of receipt of the request for consultation (Nebel, 2023)[87].

Last but not least, workers can exercise the rights bestowed upon them by the GDPR (cf. *supra*) of which the right of access is one of the most important. Furthermore, workers can mandate a lawyer or a worker representative or in some cases, unions will provide workers with a lawyer to lodge a complaint in cases where he deems the processing of his personal data by his employer is not compliant with the GDPR (Article 80(1)). Whether or not trade unions can initiate legal action in such cases absent a mandate *expressis verbis* from the workers concerned seems to remain a point of discussion[88] as was reported by a trade unionist in Belgium, whose trade union frequently uses Article 80(2) GDPR during social dialogue or social conflicts regarding the processing of workers' personal data. However, as mentioned before, the judgement of the Court of Justice of the European Union in the cited case *Meta Platforms Ireland* in our opinion leaves little doubt as to the applicability of said reading and the extension of said jurisprudence to trade union organisations[89].

[85] "Some regional supervisory authorities have published guidelines relevant to DPIAs, for instance: – the Lower Saxony data protection authority ('LfD Niedersachsen') issued guidance; […] – the Bremen data protection authority ('the Bremen Commissioner')" issued a list of processing operations subject to DPIAs; "– the Data Protection Authority of Bavaria for the Private Sector ('BayLDA') issued guidance" (Nebel, 2023).

[86] See www.bfdi.bund.de.

[87] Also see § 69(1) and (3) BDSG).

[88] Cf. GDPiR National Report on Belgium, cit.

[89] Or at least to such trade unions recognised as such by the Member State concerned.

Co-funded by the European Union

4. Main topics and trends in social dialogue practices in selected countries

By far the most important topic in social dialogue regarding the processing of workers' personal data is the monitoring of workers and, by extension, surveillance of workers. This is not surprising, since monitoring and surveillance – often by the means of 'foremen'[90] have always been a part of the manufacturing industry ever since the First Industrial Revolution or at least it has been since the end of the 19th Century. One only needs to read *Pieter Daens*, the famous book by Louis Paul Boon (1971)[91], or look into phenomena like Taylorism (Taylor, 1911), and other production styles involving 'human resources management' practices (Wickström & Bendix, 2000).

After WW2, as a result of ongoing industrial and technological evolutions and the rise of mass-production of consumer goods, monitoring and surveillance of workers started to make use of video cameras, later also known as closed circuit television-systems (CCTV)[92]. As such, it should not come as a surprise that many CLA's in the field of data-protection and court cases[93] are on or mention the practice of video-surveillance[94].

However, the evolution of technological devices allowing for the monitoring and surveillance of workers resulted in such devices being abundantly present and used. Personal computers, tablets, smartphones and software installed on said devices while Internet connectivity allows for the remote access of information in both ways,

[90] In many cases, work supervisors are now called 'quality managers'.

[91] Or watch the movie *Daens*, directed by Stijn Coninx.

[92] 'Television literally' means 'looking from afar' (cf. the German 'Fernsehen'). CCTV-systems are typically monitored and controlled in a 'control room'. As mentioned above, manufacturing or production supervisors are not a new thing and where formerly known as 'foremen' (cf. *supra*). See also Hotek (2003), p. 10.

[93] See the GDPiR National Report on Belgium, cit., p. 21 ff., for a number of (in)famous court cases (from criminal to civil law cases) in Belgium involving workers and video-surveillance in which the rules on data-protection fixed in a CLA were not observed but the images obtained where allowed as evidence, nonetheless. Said cases clearly show the issue of the processing of workers' data-protection is not confined to the data protection legislative framework nor to the social dialogue on that topic, or rather, proves the concept of the 'legislative framework on data protection' must be interpreted extremely broad.

[94] Or legislation: cf. also Article 4 of Act No. 300/1970 (and its 2015 update) in Italy and the GDPiR National Report on Italy, cit., p. 7 ff.

Co-funded by the European Union

where only the operating system and the software used mediate which data are accessible by whom, often unknown to the user of the device and software[95].
GPS-enabled devices, such as car navigation systems, smartphones and wearables not only allow for location tracking but will often allow for the monitoring of motion, and thus driving style. Wearables or handheld tools will often allow for in-house location tracking and monitoring of movement, allowing for the monitoring of worker performance and productivity, frequency of the use of restrooms and even the proximity of other workers. Although such modern tools can be used for noble purposes such as safety and health and the prevention of occupational accidents and diseases, one should not forget any means of monitoring and surveillance in the field of OSH can allow for monitoring and surveillance for other purposes. It is on this point, for instance, the principle of purpose limitation is of utmost importance. However, if the workers' personal data for monitoring and surveillance is not being processed in a transparent way, which most often is not, workers will not only not be aware, but it will be difficult if not impossible to monitor if said processing is compliant with the legislative framework on data processing. Even if it turns out not to be compliant, data can still be allowed in a court of law, as we have just learned from the Belgian jurisprudence on that point[96]. All the more reason to prevent the unlawful processing of workers' personal data before it takes place or to stop it as soon as it is discovered.
At this point, however, it seems the sense of urgency of trade unions and workers' representatives is insufficiently present if not totally absent. In Portugal, for instance, "data protection in the manufacturing sector in Portugal is articulated in a very reactive (ex post) instead of proactive (*ex ante*) and trade union action happens after the fact, leaving little space for action and prevention. For the most part, privacy issues are not developed to their fullest extent through collective bargaining. As a result, collective agreements are limited to what is mandatory by data protection laws (GDPR and Labour code). Therefore, clauses regarding data

[95] For instance, many documents, e.g. generated by a word processor, contains metadata showing the time the document was created, the time the document was last saved, the devices used. Sometimes, even the time the document was worked on, the users and the different versions can be easily retrieved. Popular office software tools more and more allow (third party) plugins that will, for instance, transcribe video meetings, include which participant said what, summarise not only the meeting duration but also the time different participants were speaking and even generate a resume, summarising all the above points. Handy for the participants, but of course, also for participants supervisors.
[96] Cf. *supra*.

Co-funded by the European Union

protection only concern to digital rights and nothing related to participation or supervision – if present at all"[97]. It was even reported in Spain the "GDPR has had little effectiveness and applicability in labour matters"[98].

As regards the main reasons behind the limited development of company-level collective bargaining on workers' data processing, respondents in Ireland "refer either to managerial unilateralism or to the fact that digital technologies are rarely introduced in their companies. Among the main obstacles faced by workers' representatives when negotiating with managers over these issues: the difficulty to get timely, full and complete information from management, the lack of knowledge from one side or both, and the absence of data management professionals in bargaining tables. [While] data protection policies are generally drafted by management, at best after consulting workers' representatives"[99].

Where there is a sense of urgency, means allocated are most often insufficient or, again, absent. All the more striking in the manufacturing sector, one of the sectors where technological innovations have always been implemented first, Industry 4.0 being a recent illustration thereof (Armaroli & Dagnino, 2019, pp. 173-175 and the references there cited). As such, it seems trade unions are not aware of the importance of data and hence of data-protection nor prepared for the evolutions that have been taking place during the past decade. The use of Big Data and algorithms, the use of Algorithmic Management and phenomena such as 'platformisation' of work, be it through online digital platforms providing platform work or similar platforms used to allocate tasks in-house, allowing not only for the monitoring and surveillance of workers, but also openly or covertly turning workers more and more into competitors, where the cynical endpoint is workers ending up competing with themselves. Where historically, piece work has always been just that, at least workers could monitor their own production and thus, monitor the correct payment of wages according to their own productivity. Such is no longer the case today where workers are not aware what data is being processed and for which purposes nor to what ends. As is often propagated by digital online platforms providing for platform work as an alibi and a reason for refusing transparency about which data are being processed and how, it is a fact the processing of personal data is effectively a black box for the workers concerned. Totally unacceptable, considering said data processing can have consequences on workers' wages,

[97] GDPiR National Report on Portugal, p. 19.
[98] GDPiR National Report on Spain, p. 22.
[99] GDPiR National Report on Ireland, p. 20.

Co-funded by the European Union

careers and can even be used for disciplinary reasons. Ironically, 'The Sword of Damocles' was "the name for an early virtual reality (VR) head-mounted display and tracking system, widely considered to be the first augmented reality HMD system"[100].

5. The role of European Works Councils in Multinational Companies

In addition to the questionnaire directed at workers' representatives, whose results have been described in §§ 4.3 and 4.4 above, a different questionnaire was administered to European Works Council members, especially those operating in MNCs active the manufacturing sector and dealing with collective bargaining or social dialogue procedures at company-level, in order to investigate their opinions and experiences concerning the topic of workers' data processing by employers.
Due to the termination of UvA from the Consortium, and the evident impossibility to administer the questionnaire in Turkey, the questionnaire was administered in 11 countries (Belgium, Czech Republic, Germany, Hungary, Italy, Ireland, Luxembourg, Malta, Portugal, Spain, Slovakia). Unfortunately, however, answers were retrieved only from EWC members based in Belgium, Germany, Italy and Slovakia.
The situation reported by respondents that have a seat in European Works Councils seems to be better compared to what reported by workers' representatives, especially for what concerns the provision of information by the company on the processing of employees' personal data. For example, several German, Slovakian, Belgian and Italian respondents reported that their EWC is both informed and consulted by the company about its data management processes even outside its plenary meetings. Despite this, negotiations and/or joint initiatives with management on the matter remain scarce in all countries surveyed.
The lack of data protection experts from the side of the union is often reported as one of the main reasons behind the scant development of collective agreements or the development of a proper dialogue with management over workers' data processing, together with the EWC members' lack of proper knowledge and skills. On this last matter, coherently with what was reported by workers' representatives, it is to be noted how the training which is rarely provided to EWC members appears to be

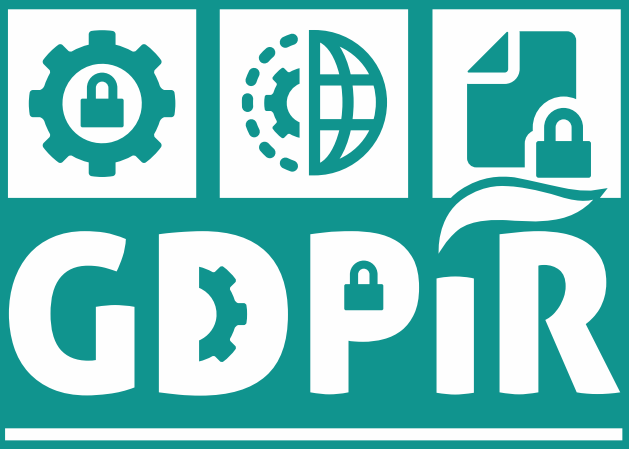
[100] *The Sword of Damocles (virtual reality)*, in *en.wikipedia.org*.

Co-funded by the European Union

quite general and theoretic, mainly covering the key elements of the European and national privacy and data protection law and leaving behind industrial relations actors' prerogatives or negotiation strategies. However, some of the Slovakian respondents highlighted that the trainings also focused on emerging technologies like artificial intelligence and algorithmic management.

Lastly, another data that emerged from the questionnaire is that workers' data processing is usually addressed as part of the activities of an EWC working group dealing with more wide-ranging topics (e.g., digitisation at work). This might be linked to the circumstance according to which many respondents reported that the issue is not considered a priority at the transnational level, given the absence of any rights or prerogatives for EWCs in this field according to the European and national legislation, but also to the same EWCs founding agreements.

Co-funded by the European Union



MANAGING DATA PROCESSING
IN THE WORKPLACE THROUGH
INDUSTRIAL RELATIONS

CONCLUSIONS

The research activities carried out in the context of the GDPiR project resulted in a comprehensive overview of European manufacturing sector trade unions' general approach to data processing in the workplace – also in light of the prerogatives foreseen by European and national legislation, the role acquired by Data Protection Authorities (DPAs) and judicial organs on the matter, and the institutional features of national industrial relations systems across the selected countries.

Firstly, while the processing of workers' data is exponentially increasing, in light of the steady progression of the digitalisation and datafication processes (see § 2) the issue appears not to be a priority in trade unions' bargaining agendas in the majority of the Member states we researched. Trade unionists indeed report to be mostly concentrated on what are perceived as more pressing and concrete issues, such as wage protection, occupational health and safety and so on. This approach strongly contrasts with that of the European-level manufacturing union, i.e., IndustriAll Europe, which recently promoted several initiatives aimed at increasing unionists' awareness on the challenges brought by digitalization, among which employers' processing of workers' data plays a pivotal role. However, IndustriAll's efforts to provide national-level unions with adequate tools to have a real voice on the matter is again often hindered by the difficulty of engaging them on topics perceived as too far from workers' day-to-day reality (§ 4.1).

With regard to national legislation on data processing, it is to be noted how, when the prerogatives of Article 88 GDPR have been exercised, the employment-specific provisions on the issue often deal only with specific topics, such as workers' monitoring and surveillance, the use of consent as a legal basis for data processing and the limitation of the use of workers' health, generic, or biometric data for employment-related purposes – with case law reflecting the same trends[101]. Only a few Member states among those researched appear to be more forward-thinking, with legislations directly addressing the new challenges for data protection in the workplace brought by last-generation technologies (Artificial Intelligence, algorithmic management) and National Data Protection Authorities issuing guidelines on the same topics directed both to employers and employees.

National legislations are instead more explicit in terms of prerogatives awarded to trade unionists and workers' representatives on data protection matters, with information rights being the most common, followed by consultation rights; the role

[101] As mentioned before, the compliance of national legislation, CLA's or other measures and practices implemented pursuant to Article 88 GDPR is oftentimes questionable to say the least.

Co-funded by the European Union

of collective bargaining appears instead to be more limited in most legislations, though not all of them (§ 3.2). On the contrary, members of European Works Councils reported that the issue of workers' data processing is rarely dealt with at the transnational level, mostly because of the absence of any rights or prerogatives for EWCs in this field according to European and national legislation (§ 4.5).

The results of the above-mentioned research activities now spur the question: is the legislative framework on the processing of personal data in Europe up to the task? Clearly, the GDPR is a strong legal instrument, providing for strong principles and rights data subjects can rely on, and for tools and means to take action in case the processing of personal data is deemed to be non-compliant with said principles and rights. Nevertheless, some reservations need to be made. *First*, effective enforcement is not always easily achieved. The disparity of DPA's, of their organisation and functioning leaves room for improvement, to say the least. Also, In the context of employment, enforcement can and should play an important role in cases where workers' personal data is processed in a way that is not compliant with the GDPR. However, social partners have little and mostly no active voice within the DPA's. In some cases, an appeal to the ruling of the DPA must be brought before a commercial court[102]. Second, specifically with regard to the processing of workers' personal data, both Article 80 and Article 88 give rise to discussion, as was mentioned before, said ambiguities hampering the social dialogue on the topic of the processing of workers' personal data in times where such processing is of paramount and still increasing importance. Future research looking into the compliance of national legislation, CLA's and practices with the (core principles and rights enshrined in) the GDPR is called for[103], not in the least when it comes to the principle of transparency, and, as mentioned before, the role and functioning of DPA's when issuing opinions or judging cases and the effectiveness of enforcement in the context of employment.

---

[102] In Belgium, for instance, appeals to rulings of the DPA must be brought before the Market Court (cf. *Market Court*, in *www.rechtbanken-tribunaux.be*), which, in case in the context of employment is in stark contrast with the Belgian tradition where (civil) cases in the context of employment are brought before Labour Courts where magistrates are assisted by 'lay-judges': one from employers' and one from employees' side. Even criminal cases in the context of employment, are treated by so-called 'social chambers', specialised in 'criminal social law'.

[103] Cf. for instance the discussions on the 'protection of employers' property' as a legal ground for surveillance of workers that took place in Luxembourg (cf. GDPiR National Report on Luxembourg, cit., pp. 19 and 28. Also see the GDPiR National Report on Belgium, cit., p. 18, and Article 88(1) GDPR).

Co-funded by the European Union

In conclusion, generally speaking, the results of the research phase of the GDPiR project appear in line with the main hypothesis underlying the project itself, i.e., the presence of diffused lack of data literacy and awareness concerning the challenges posed by data processing among European workers representatives and trade unionists of the manufacturing sector, which needs to be tackled through dedicated initiatives. The training modules foreseen in the next phase of the GDPiR project (M17-M19) aim to constitute an integral part of those activities, complementing IndustriAll Europe's initiatives concerning bargaining strategies on digitalization and GDPR awareness.

In more detail, it is clear training needs to be directed at educating trade union members and employees not only on how to use strategic litigation strategies and exploiting the legal prerogatives which most national legislations endow them with to participate actively in workers' data processing, but, since data processing is becoming more pervasive and at the same time opaquer, also increase the level of data awareness and data literacy. The expected long-term impact should be that of training 'data protection experts' among trade union members, inspired by international best practices and lessons learned with the aim of allowing for the implementation of virtuous social dialogue practices in their territorial or company-level context.

Co-funded by the European Union

MANAGING DATA PROCESSING
IN THE WORKPLACE THROUGH
INDUSTRIAL RELATIONS

REFERENCES

Abraha, H. H. (2022). A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace. *International Data Privacy Law, 12(4)*, pp. 276-296

Armaroli, I., & Dagnino, E. (2019). A Seat at the Table: Negotiating Data Processing in the Workplace: A National Case Study and Comparative Insights. *Comparative Labor Law & Policy Journal, 41(1)*, pp. 173-196

Article 29 Data Protection Working Party (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 4 April

Boon L. P. (1971). *Pieter Daens*. Amsterdam: De Arbeiderspers

Caprile, M., Sanz, P., Riobóo, I., Welz, C., & Rodríguez, R. (2018). *Mapping varieties of industrial relations: Eurofound's analytical framework applied*, Eurofound Research Report

Christenko, A., Jankauskaitė, V., Paliokaitė, A., Reinhold, K., & Järvis, M. (2022). *Artificial intelligence for worker management: risks and opportunities*, EU-OSHA Policy Brief

De Coninck, M., Gillis, D., & Jorens, Y. (2013). *The Belgian social criminal code: an English translation by IRIS | International research institute on social fraud*. Brugge: die Keure

DSK (2018). *List of processing activities for which a DPIA is to be carried out*

DSK (2017). *Kurzpapier Nr. 5. Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO*

Dukes, R., & Kirk, E. (2023). Legal Change and Legal Mobilisation: What Does Strategic Litigation Mean for Workers and Trade Unions? *Social & Legal Studies (on-line)*, pp. 1-22

EDPB (2020). *Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1*, 4 May

European Court of Human Rights (1992). *Judgment in the case of Niemietz v. Germany*, Press Release, 16 December

European Court of Human Rights (2022). *Personal Data Protection*, Thematic Factsheet, September

European Court of Human Rights (2023). *Personal data protection*, Factsheet, July

European Union Agency for Fundamental Rights (2010). *Data Protection in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II*

Fainmesser, I. P., Galeotti, A., & Momot, R. (2019). *Digital Privacy*, HEC Paris Research Paper No. MOSI-2019-1351, in *www.ssrn.com*, 6 October

Flink, M. (2021). *Beschäftigtendatenschutz als Aufgabe des Betriebsrats. Kompetenzen und Verantwortung des Betriebsrats für den Datenschutz*. Berlin: Duncker & Humblot

Co-funded by the European Union

Hendrickx, F., Mangan, D., & Gramano, E. (eds.) (2023). *Privacy@work. A European and Comparative Perspective*. Alphen aan den Rijn: Wolters Kluwer

Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F. (2019). The European Union General Data Protection Regulation: What It Is and What It Means. *Information & Communications Technology Law, 28(1)*, pp. 65-98

Hotek, D. R. (2003). 21st Century Manufacturing Supervisors and Their Historical Roots. *The Journal of Technological Studies, 29(1)*, pp. 10-18

Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data. A Revolution that Will Transform How We Live, Work, and Think*. Boston: Houghton Mifflin Harcourt

Monton, A. L. (2022). Difference and Similarities: Digitization, Digitalization, and Digital Transformation. *GlobalSign Blog*, 22 March

Mueller, S. (2018). *German DPA Publishes Blacklist Of Processing Operations Subject To A "DPIA"*, in *www.jdsupra.com*, 30 August

Naimi, A. I., & Westreich, D. J. (2014). Book Review. Big Data: A Revolution That Will Transform How We Live, Work, and Think. By Viktor Mayer-Schönberger and Kenneth Cukier. *American Journal of Epidemiology, 179(9)*, pp. 1143-1144

Nebel, M. (2023). *Germany – Data Protection Overview*, in *www.dataguidance.com*, September

Nevens, K. (2008). Van werkboekje tot Dimona. *Sociaalrecht Blog*, 17 September

Oracle (2022). *The Evolution of Big Data and the Future of the Data Platform. How organizations use data platforms to get more value from data*

Stephens-Davidowitz, S. (2018). *Everybody Lies. Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are*. New York: Arper Collins

Stewart, G. A., & Hegner, B. (2018). Time to adapt for big data. *CERN Courier*, 23 March

Taylor, F. W. (1911). *The principles of scientific management*. New York, London: Harper & Brothers

Waeyaert, W., Hauben, H., Lenaerts, K., & Gillis, D. (2022). *Italy: a national and local answer to the challenges of the platform economy*, EU-OSHA Policy Case Study

Wickström, G., & Bendix, T. (2000). The "Hawthorne effect" – what did the original Hawthorne studies actually show? *Scandinavian Journal of Work, Environment & Health, 26(4)*, pp. 363-367

Wong, B. (2019). Delimiting the concept of personal data after the GDPR. *Legal Studies, 39(3)*, pp. 517-532