Chapter 6
Data Processing in Employment Relations; Impacts of the European General Data Protection Regulation Focusing on the Data Protection Officer at the Worksite

Clara Fritsch

Abstract From the 1990s European Unions are increasingly confronted with ignored employees' privacy or misused employees' personal data. There has been a vivid European discourse about this issue in the early 2000s. The European GDPR brings the topic back to the European agenda. The article points out who is involved in employee data protection from side of the employees' interest organizations. The contribution further describes which are the employees' interests stressing some crucial points of the GDPR such as the data protection officer at company site and the article on data protection in employment relations. The author tries to figure out how the GDPR matches the employees interests – or otherwise. Therefore she compares the European Commission's approach with that of the LIBE-committee to see which one would serve more the employees' fundamental right to privacy.

This article gives an insight on how the European Data Protection Regulation (EDPR) will effect labour relations and looks for consideration of employees' interests within the EDPR. According to Harding,[1] Haraway,[2] and other representatives of the "standpoint theory", it is important to openly state the position of the author. I am a sociologist, working with the Austrian Union of Private Sector Employees, Graphical Workers and Journalists (GPA-djp). My main field of work is consultation of works councils who are responsible for privacy issues at the

[1]Hirsh Elizabeth and Garry A. Olson, "Starting from Marginalized Lives: A Conversation with Sandra Harding", JAC, journal of Rhetoric, Culture, & Politics (1995).

[2]Haraway Donna, "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective" Feminist Studies (1988, Vol 14, No. 3).

C. Fritsch (✉)
Union of Private Sector Employees, Graphical Workers and Journalists, Alfred Dallinger Platz 1, A- 1034 Vienna, Austria
e-mail: clara.fritsch@gpa-djp.at

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_6

workplace, employees' data protection and monitoring systems. Dealing daily with privacy issues at workplaces – whether it is a newly installed surveillance camera, an international mother-company's request to receive all employees' performance data, a whistle-blowing hotline necessary according to the US-American Sarbanes-Oxley Act or a new navigation device placed in all company cars without the approval of employees or workplace representatives – is the very practical background of this text. Workplace experience shaped this article on one hand. On the other hand, I was involved in law amendments that deal with workers privacy – both in Austria and Brussels. My task was to promote the employees' view and interests in discussions with politicians at the European Trade Union Confederation (ETUC), with members of the European Parliament and with Representatives of the European Commission. These discussions are another background shaping this text.

Employees' interests nowadays are losing weight all over Europe (Busch et al. 2012).[3] Their rights are cut and social exclusion is on the rise. Thus, they are marginalised – especially since the economic crisis. The standpoint methodology postulates that research should initially concentrate on marginalised groups. The perspective of the "marginalised lives" is inevitable for science, as Sandra Harding[4] says.

The epistemological approach of this text is Karin Knorr-Cetinas[5] *Manufacture of Knowledge* where she shows that scientific work always depends on social (and technical) means and interaction. New scientific texts are always shaped by several different players. I tried to demonstrate – following the conventions of Knorr-Cetina – how different players shape a new European law.

Empirically the article mainly uses diverse writings by Austrian and international unions and other organisations focusing on the impact the EDPR will have on employees' interests.

The aim of the contribution is to link practical experience with the academic sphere by expressing the standpoint of marginalised employees' interests in the field of privacy politics at workplaces.

6.1 An Outline of Employee Data Protection

All over Europe the use of personal data of employees is business. Personnel administration by personal information systems, personal data created by the use of email and the internet, data of working time records, attendance and sickness records, data from video cameras, and many more information and communication

[3]Busch Klaus et al., "Eurokrise, Austeritätspolitik und das Europäische Sozialmodell, Wie die Krisenpolitik in Südeuropa die soziale Dimension der EU bedroht" (2012).

[4]Harding Sandra, "Standpoint methodologies and epistemologies: a logic of scientific inquiry for people", in UNESCO and International Social Science Council (2010).

[5]Knorr-Cetina Karin, *Manufacture of Knowledge* (Oxford 1981).

technologies (ICT) are implemented on company levels generating and administrating personnel data. Employers all over Europe and beyond precede much more data than is effectively needed to fulfill legal or contractual requirements.

Sure, data protection is a topic concerning everyone but employees as data subjects often are double victims once as citizens and consumers and secondly as dependent workers. Sometimes being an employee and a private person concerned is so closely connected (for example, when working at a hospital and having personal medical records stored at the same place or when working at a banking institution and being forced to have a banking account there as well) it leads to misuse of personal data. Looking at dynamic data, connection data or just log files, one can easily recognize that personal data is sometimes created automatically, without consent or even knowledge of the data subject, indicating that employees' access and the right to information is difficult to achieve. The information imbalance is evident. Employers might use this data without informing the employee – the result may be a surprising end of the employment relation.

Throughout history working conditions changed with tools and instruments of work. The biggest change until now was the industrial revolution turning hand work in machines' work. Currently we are facing a digital revolution shaping nearly every workplace.[6] ICT has changed working conditions in terms of reaction time, multitasking, availability of knowledge and – foremost important in matters of fundamental rights – monitoring possibilities. Systems are much more interdependent and linked to each other than they were in the twentieth century. Unified communication systems, shared documents and cloud services transform employees into anywhere- and anytime-workers, who at the same time can be easily traced and tracked. Acquisition and retention of employees' personal data by ICT is happening at high speed nowadays. The large and further increasing number of data leads to the use of information without caring about the data processing principles set by the European Commission in the European Data Protection Directive regarding finality, proportionality, transparency – just to mention the most important ones.

6.2 European Scientific Research on Employee Data Protection

EU-wide comparisons concerning individual awareness on data protection at the workplace among employees in general and among employees responsible for ICT are evidence of highly differing consciousness within the EU countries. An average of every third employee in the EU feels well informed about his/her data protection rights and just half of the employees trust their employers.[7] Just 13 % of the 4.800

[6]European Commission, *The European e-Business Report, A portrait of e-business in 10 sectors of the EU economy, 5th Synthesis Report of the e-Business W@tch* (Brussels, 2006).

[7]European Commission, *Special Eurobarometer Data Protection* (Brussels, 2003).

data controllers interviewed in 27 EU member states are familiar with the national data protection law and the same amount frequently contacts the national data protection authority.[8] These few figures reveal the necessity of a data protection officer at the worksite (DPO) in order to fulfil the legal requirements and to protect the employees' fundamental right to privacy. DPOs can strengthen employees' privacy at the workplace since they make sure that the company's data proceedings correspond with data protection law and other law applicable to the line of business. According to the Austrian Private Sector Union DPOs should be the information link between employer, employees, clients, customers and business partners. Currently Germany is the only country within the European Union that has implemented a mandatory DPO at company level for companies with more than nine employees dealing with data proceedings.

Following the European Data Protection Directive each member state shall implement the directive into national law, hence should have an equivalent data protection level. But this is not the case in the employment context, as some few studies have shown dealing with national legal frameworks as well as industrial relations. Available studies on an international level are missing some crucial points. Some authors deal with an international scope, but do not focus on labour law,[9] other findings are limited to the comparison of legal standards regarding the use of email and the internet at the workplace, but do not include other data processing.[10] The European Article 29 Data Protection Working Party conducted a summary of the national legislation on surveillance and monitoring of electronic communication in the workplace in 2002, describing that the then member states were missing other data processing as well.[11] None of these studies combines the legal situation with technical innovation at workplaces and the only one that does[12] has no neutral approach to technology. None of these studies includes the member states that joined the European Union after 2004. It seems as if the discourse had its peak in the early years of the 2nd millennium. A more recent study was published in 2011, but it is limited to the Australian law and to the use of Email and internet.[13]

This might be caused by the fact, that there are diverse legal backgrounds as well as diverse cultures in data protection in general. The "Eurobarometer" 2008 detected

[8]European Commission, *Flash Eurobarometer Data Protection in the European Union Citizens' perceptions* (Brussels, 2008).

[9]Lilian Mitrou and Maria Karyda, *Employees' privacy vs. employers' security, Can they be balanced?* (Elsevire Ltd. 2005).

[10]Catherine Delbar et al., "New technology and respect for privacy at the workplace," *European Industrial Relations Observatory* (2003).

[11]Article 29 – Data Protection Working Party, *Working document on the surveillance of electronic communications in the workplace* (Brussels, 2002).

[12]Catherine Delbar et al., "New technology and respect for privacy at the workplace", *European Industrial Relations Observatory* (2003).

[13]Anne O'Rourke, Julian Teicher and Amanda Pyman, "Internet and Email Monitoring in the Workplace: Time for an Alternate Approach", *Journal of Industrial Relations* (2011 vol. 53).

that 72 % of the EU citizens do not even know about their national data protection authority, whose purpose is – amongst others – to protect individuals against data misuse. In 2010, the European Union Agency for Fundamental Rights realised a study dealing with the role of national data protection authorities. Findings are that these authorities are organised quite differently regarding their independency, resources, assertiveness and sanction possibilities.

6.3 Legal Situation

In the last 15 years there have been several attempts to regulate privacy at workplaces constraining the use of monitoring and surveillance within employment relationships respectively. Some European countries have specific legislation in this area. In 2004, Finland amended the "Act on the Protection of Privacy in Working Life" based on an act first passed in 2001. This is the most elaborated act on this topic in the European Union specifically dealing with employee data proceeding and including applicants data as well. Of course, jurisdiction and single clauses within labour or constitutional law deal with workplace monitoring, workplace privacy and workers representatives' participation, but single acts of legislation on this very topic are a rare good.

Intersectoral collective agreements in Norway, for example, state that privacy at workplaces is to be retained. The Belgian national collective agreement No. 81 from 2002, the "agreement on the protection of the private lives of employees with respect to controls on electronic on-line communications data", is another European "early bird" regulating data protection within industrial relations. However, it only applies to private employment relations. The agreement states the goals allowing for the online monitoring of employees' behavior at the workplace, e.g. technical functioning of the ICT as well as controlling of inner company internet compliance.[14]

The problem with compliance guidelines is that employees or workplace representatives are never involved when such compliance regulations, behavior guidelines, codes of conduct Binding Corporate Rules (BCR) – or however the documents are called – are established. Putting surveillance measures in force in order to control employees' behavior according to employer-driven compliance always puts the employee on the weaker part. Compared to the set of possibilities within the GDPR enabling an employer to process employees' personnel data, an increasing importance of Binding Corporate Rules (BCR) can be indicated.

Back to the Belgian national agreement, we can see an advantage for Belgian employees. Individual controlling measures must always be preceded by generic controlling measures. Hence, employees are better protected against false suspicions and probably consequently caused dismissal. Furthermore, Belgian employers must

[14]Catherine Delbar et al., "New technology and respect for privacy at the workplace", *European Industrial Relations Observatory* (2003).

inform employees and their representatives prior to any monitoring measures. The approach of generic before individual monitoring also follows the Portuguese data protection authority that published guidance on employees' internet and email use.

Many national data protection authorities elaborate guidelines and similar documents as well (for example the United Kingdom, Ireland, Italy, Austria or France) in order to deal with the data protection responsibilities within employment relations. Some national data protection authorities expressed opinions dealing especially with electronic communication at workplaces, for example, Denmark, Germany, Ireland, Italy, France or Belgium.[15] But these documents are of rather weak legal binding. Obviously, authorities all over Europe have – more or less successfully – tried to fill a legal gap.

Information duties before conducting individual surveillance measures within employment relations can be found in France, the Netherlands, Spain, Sweden or Austria. Consent of employees is explicitly needed in some national labour laws such as labour legislation in the Netherlands, France, Germany or Austria. Workplace related regulation of video surveillance exists in Belgium and Denmark.

Delbar et al. say: "Despite a lack of specific legislation, the general legal framework and principles are interpreted as having implications for employees' internet and e-mail use in some countries." The German way of getting along with employee data protection is constitutional law stipulating the right to "informational self-determination". Much adjudication are operationalizing the constitution and therefore giving guidance for workers' data protection as well. But jurisdiction differs a lot all over Europe as, for example, in Italy the employer got the right to see an employees' private email sent to the companies address anytime, while Dutch and French courts deny this recurring due to the fundamental right of keeping correspondence secret. Moreover, national jurisdiction is a weak instrument when European wide legal security shall be the outcome.

"Given the general absence of specific legislation on employees' privacy at the workplace, the introduction of such provisions has been discussed or proposed in a number of countries, sometimes with direct relevance to internet/e-mail use." state Delbar et al.[16] Finland, Germany, Norway and Sweden have tried to change this status quo and worked on specific legal acts – some of them still struggling for a better legislation on employee data protection.

[15]Hendrickx Frank, *Protection of workers' personal data in the European Union* (Leuven/Tilburg, 2002).

[16]Catherine Delbar et al., "New technology and respect for privacy at the workplace," European Industrial Relations Observatory (2003).

6.3.1 The Austrian Example

Austria is a typical example for the international legal situation. No special rules on workplace privacy, only little evidence of jurisdiction and an only slowly rising awareness of the importance of the topic shape the field of Austrian employee data protection.

Doubtless there is an economic dependency of employees on their employers. Since no employee wants to accuse his/her employer of data abuse during an existing employment contract, court rulings on the right of data protection of employees are rare. Even more so, since evidence is sometimes hard to proof. The result is no jurisdiction in Austria regarding data protection legislation. This is also driven by the fact that data protection law belongs to individual right, which means employees have to lodge an appeal before a court of first instance and pay a lawyer on their own. Workers representatives have no right to be party in the proceeding. Rulings concerning employee data protection after an employee has been dismissed refer to labour law, where more jurisdictions exist that judges can rely on. The result is a prevailing lack of data protection jurisdiction in employment relations causing legal insecurity.

A recently concluded study by an employees' interest organization (the Chamber of Labour Vienna) found, that only one out of four ICT systems that would need compulsory regulation by a works agreement, concluded between the workforce representative and the employer, is actually regulated.[17] One reason is that ICT is difficult to understand for workplace representatives as well as employers. To regulate ICT, negotiators must have at least some technical understanding and know how personnel data is proceeded. Due to the fast advance of ICT, weekly updates and new implemented systems every year, it is difficult to make up leeway. The increasing quantity of systems, some of which are corresponding with each other, neither makes things easier. Therefore, even interested employees and works councils lose track. Data protection officers (DPO) at company level could remediate this obstacle. Representative figures in Austria show that the employees are better informed and more works agreements are concluded in companies, in which DPOs have been established voluntarily.[18]

Some legislation parties in Austria are engaged in developing a legal regulation on employee data protection since 2010, but did not succeed yet. In the last 5 years, there have been several efforts to strengthen workplace privacy by legally implementing a DPO at the company level. The first attempt in summer 2010 should have brought about an obligatory DPO with dismissal protection, a 4-year working period, technical resources and knowledge as well as permanent further education.

[17] Riesenecker-Caba, Thomas and Alfons Bauernfeind, *Verwendung personenbezogener Daten und Grenzen betrieblicher Mitbestimmung: Datenschutz in der Arbeitswelt* (Arbeiterkammer Wien, 2011), 73–78.

[18] Fritsch, Clara, "Vogelstraußpolitik, der Tenor von Umfragen zum innerbetrieblichen Datenschutz in Österreich," *Arbeit und Wirtschaft* (2008): 17.

He/she should not have been bounded by employer's instructions. The position of a company DPO as the Austrian Trade Union Federation ("Österreichischer Gewerkschaftsbund", ÖGB) wanted it, should have even more weight, as he/she would only be put in place with the approval of workplace representatives and should be responsible not only for company and customer data, but also for employee personal data. The employer's interest organizations', the Chamber of Business, argument is that this would be too expensive and that there would be no necessity of such a position due to a well-functioning Austrian data protection law.

After another unsuccessful attempt to implement an obligatory DPO to the Austrian data protection law in summer 2011, the third attempt followed in 2012. This amendment was stipulating that a voluntary DPO should be implemented at company level. Again, the Chamber of Commerce did not agree and the government dropped the plan again.

6.4 Employee Data Protection by Relevant European Players

6.4.1 The European Commission

In August 2001, the European Commission started a first round of formal consultation with social partner raising the question, whether protection of employees' data requires special guidelines and if yes, how these guidelines should be expressed – by a directive, a recommendation or just a code of conduct? Employer organisations mostly found the existing legal framework sufficient and warned about excessive regulations and burdens for small- and middle-sized companies. (These concerns were expressed repeatedly when it came to consultations in 2010 as described in Sect. 6.5.2.). Unions all over Europe painted a controversial picture, stating that the existing directive is helpful but not sufficient and demanded a specific directive on workplace data protection.

In October 2002, the European Commission launched a second consultation of European social partners. In the end, the Commission elaborated a framework proposal for employee data protection including, among other details, obligatory employees' representatives' consultation before implementing new ICT, monitoring only if national data protection authorities controlled the ICT in advance and the interdiction of secret monitoring if there is no concrete suspect of a grave criminal misbehaviour.[19] (Reading the proposals made by the European Parliament's Committee on Employment and Social Affairs (EMPL) in 2013,[20] one can find some of these points again.)

[19]European Commission, *Second stage consultation of social partners on the protection of workers' personal data* (Brussels, 2002).

[20]Committee on Employment and Social Affairs, *Opinion for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for General Data Protection Regulation* (Brussels, 2013).

There followed no further action from the Commission's side for a long period and the social partners did not take up the matter themselves. It was the year 2010 when the Commission started a new consultation; this time open to the public and dealing with data protection in general not specifically with employees' data protection. 288 contributions were counted when the public consultation closed. Replies were manifold as the list of contributors shows.[21]

Big players in the field of ICT (such as eBay, Alcatel, Yahoo, Vodafone or Microsoft) sent their contributions as well as public authorities and interest organisation. The latter comprising much more employer organisations from the finance, medical and ICT sector than employees' interest organisations. Papers raising awareness on the employees' special interests in data protection just came from Germany and Austria. The ETUC and UNI Global Union, the international federation of the service sector unions, also responded to the Commission's consultation.[22] National unions in the EU and their umbrella organisations seemed not to be interested in the matter at that time, while those branches whose vital interest are affected by data processing were much aware of the imminent "dangers" of a new European data protection regime.

6.4.2 The European Article 29 Data Protection Group

The Article 29 Data Protection Working Party, an assembly of all national data protection authorities including representatives of the European Data Protection Supervisor and of the European Council with the aim to interpret the Data Protection Directive from 1995 according to specific problems raising all over Europe (for example, the proceeding of geo-data, cloud computing or face recognition), published the "Opinion on the Processing of Personal Data in the Employment Context" in 2001 aiming for: "further guidance on the issues where the application of general principles of data protection raises particular problems relevant to the employment context, such as the surveillance and monitoring at the working place, employee evaluation data and others."[23] This opinion was a landmark for advocates of an individual employee data protection act. Although some efforts have been taken to come to such an international legal norm, it has not yet been concluded.

The opinion of the Article 29 Data Protection Working Party are in general very helpful for unions, as they very often outline concrete suggestions on how to deal

[21] European Commission, *Summary to the Replies to the Public Consultation About the Future Legal Framework for Protecting Personal Data* (Brussels, 2010).

[22] European Trade Union Confederation, *ETUC response to the Communication from the Commission 'A comprehensive approach on personal data protection in the European Union'* (Brussels, 2011) and Uni global union, *Submission to the European Commission communication A comprehensive approach on personal data protection in the European Union* (Brussels, 2011).

[23] Article 29 Working Party, *Opinion on the Processing of Personal Data in the employment (Brussels, 2014).*

with actual problems occurring in the working area – for example, if employees' data is transferred to non-European Union member states for reasons of bonus compensation, if external workers are located, if video surveillance is installed, and so on. Although the opinions do not have the power of legislation or jurisdiction, they give a perception on how the European Directive is to be handled and thus have an impact on employees' privacy.

6.4.3 International Trade Unions

The International Labour Organization (ILO) was the first organisation addressing the issue of workers' privacy. In 1997, the first work on this topic by a union confederation was published: "Protection of Workers' Personal Data".[24] After that, it became rather silent around workers' privacy at the ILO. When the European Commission's consultation on the future legal framework of Data Protection Regulation was running in 2010, just a few European unions sent their statements – namely the Austrian and German union federations.[25]

The Union Network International (UNI Europa), a union federation in the service sector, concluded at an executive assembly in June 2010 that: "several reasons plead in favor of establishing a particular framework of employment specific rules: legal clarity and certainty, a more consistent and homogenous application of the rules governing the protection of individuals' fundamental rights and freedoms in this regard, the specificity of the employment relationship and the weaker position of workers, recent technological advances and their application in the workplace, the growing number of transnational mergers, take-overs and acquisitions and an increasing number of employees working for companies or organizations that have establishments or subsidiaries in more than one country, the growing tendency of multinational companies to concentrate personal data of all employees in one country and therefore undermine national participation rights of employees in the field of data storage, handling and processing."[26] UNI Europa already had basic experience in workplace privacy as it has been dealing with the issue since 1998, when the campaign "online rights @ work" was launched, which concluded in a code of practice in 2000.[27] The code, for example, includes that employees and their representatives must have the right to use ICT for union purposes and that hidden surveillance at workplace shall be forbidden. (This point showed up again when the EMPL committee voted on the GDPR in 2013.)

[24] International Labour Organization, *Protection of Workers' Personal Data* (Geneva, 1997).

[25] Österreichischer Gewerkschaftsbund, *Stellungnahme zum Gesamtkonzept für den Datenschutz der Europäischen Union* (Wien, 2011).

[26] Uni global union, *Data protection and employment in the European Union* (Madrid, 2010): 2.

[27] Uni global union, *online rights at work* (Nyon, 2000).

The European Trade Union Confederation (ETUC) followed with a document adopted in October 2012,[28] proposing that proceeding of workers' data needs distinct legislative framework: "In order to respect different labour market models and industrial relations system in Europe, the issue of data protection for workers should be regulated in a specific directive stipulating minimum standards that considers both the need for protection of workers' personal data and the role of trade unions when they act as a part of the collective bargaining process". This ongoing demand for specific legislation is not fulfilled within the GDPR, but another point – important to unions as well – was: the DPO. The ETUC appealed for "making the appointment of an independent DPO mandatory and harmonizing the rules related to their tasks and competences. In addition it would be advantageous to provide at European level adequate training standards for such officers."[29] DPOs are part of the GDPR-proposal of the European Commission, while the DPOs' training standards were added by the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE).

6.4.4 The European Economic and Social Committee (ESSC)

The opinion of the European Economic and Social Committee (ESSC) is close to that of the ETUC concerning workplace regulation although not claiming for an individual legal framework on the topic.

The first draft by the European Commission (Art. 82) said: "Within the limits of this regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context".[30] The ESSC expresses: "The words: 'Within the limits of this Regulation . . . ' should be replaced with: ' . . . On the basis of this Regulation . . . '".[31] It can be reviewed as an success of the ESSC that this claim together with the amendments of the EMPL committee proposing the same are now part of the parliament's draft of the GDPR (see also Sect. 6.5.7).

Concerning the DPO, the ESSC defines a set of rules: "The conditions related to the role of DPOs should be set out in more detail, particularly in relation to protection against dismissal, which should be clearly defined and extend beyond the

[28] European Trade Union Confederation, *ETUC position in the General Data Protection Regulation – improving the protection of workers' data* (Brussels, 2012).

[29] European Trade Union Confederation, *ETUC response to the Communication from the Commission 'A comprehensive approach on personal data protection in the European Union* (Brussels, 2011).

[30] European Commission, *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* (Brussels, 2012).

[31] European Economic and Social Committee, *Opinion of the European Economic and Social Committee on the General Data Protection Regulation* (Brussels, 2012).

period during which the individual concerned holds the post; basic conditions and clear requirements for performing this activity; exemption of DPOs from liability where they have reported irregularities to their employer or to the national data protection authority; the right for employee representatives to be directly involved in the appointment of the DPO and to be regularly informed about problems that arise and how they are resolved. The issue of the resources allocated to the function must also be clarified."[32] This detailed list is a clear indication for the importance the ESSC sees in this position. Some of the demands – such as the dismissal protection for the DPOs – can also be found in the LIBE proposal; however, only until the end of the officer's period. Still, the question of legal accountability of the DPO remained unsolved and employee representatives' participation rights are not strengthened at all. This consolidated version of the ESSC – consisting of employers' and employees' representatives – is considerable since it makes a commitment that workers' representatives have to be asked when a DPO is established.

6.4.5 The European Council

The European Council is just mentioned for the sake of completeness – to add the third party of legislation of the European Union. But since the European Council prefers closed-door negotiations, not much is known about its opinion – except for one communication in May 2013.[33] The German newspaper "Spiegel Online" reported on 2nd of December 2013 that the trialogue-negotiations could fail at all due to the German "waiting game" at the European Council.[34]

Summing up the employees' interest organizations and engagement of trade union in employee data protection over the last two decades, it can be depicted that there has been quite a lot of bargaining at company and branch level. Collective agreements concerning privacy at workplaces are drawn up by the social partners in several EU member states, some even on the branch level (Denmark, Italy and the Netherlands), and some actually on the national collective bargaining level (Belgian, Denmark, Norway). But just one member state has a specific legislation act on data protection regarding employment relations passed by parliament (Finland).

At the same time, there is not much further action from national unions when it comes to an international level. Here, we can depict that the torch is passed on to international union organizations such as UNI Europa or the ETUC. The higher the bargaining level gets, the less legal agreements by the social partners can be found.

---

[32]European Economic and Social Committee, *Opinion of the European Economic and Social Committee on the General Data Protection Regulation* (Brussels, 2012).

[33]Council of the European Union, *Interinstitutional File 2012/0011* (Brussels, 2012).

[34]http://www.spiegel.de/netzwelt/netzpolitik/deutsche-beamte-bremsen-europas-datenschutz-aus-a-936704.html

6.5 How the GDPR Affects Workplace Privacy

The European Commission drafted a new Data Protection Regulation, officially presented – after a leaked version in November 2011 – on 25th of January 2012. The following text only refers to those GDPR articles particularly relevant to the employment context. The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), responsible for the concluding amendments on the GPDP in October 2013 voted on it's GPDP-version after having dealt with almost 4000 amendments submitted by the members of parliament. In the following chapters I will point out which of the European Councils and which of the LIBE-committee's amendments underline the trade unions' position and strengthen workplace-privacy, and which contrast union's standpoints.

6.5.1 Harmonization

Interdependent corporate structures all over Europe and beyond require equal data protection standards. The European Data Protection Directive from 1995 tried to fulfill this task, but was not very successful as has been argued in Sect. 6.3. Data protection authorities, jurisdiction and sanction practice offered a wide range of data protection practice.

Currently, it is difficult to get access to employees' personal data in another country than that of data origin; not only being a matter of language. The possibilities of controlling data processing subsequent the data left its "home country" are more or less inexistent as we learn by consultation processes. These troubles of cross border data access are present not only for employees, but also for the management of multinational groups. Facing the complaints multinationals express concerning difficulties in transferring transnational data, one can easily conclude that there are not the same legal standards on data protection within the EU at that time. Thus, harmonization would support the needs of all parties concerned.

On the other hand, regarding differing labour law regimes and participation rights of workers' representatives across Europe, harmonization is fairly unrealistic. Common minimum standards (for example, how DPOs or official data protection authorities shall fulfill their duties) would give employees a more stable basis. Hence, it is an advantage to have data proceedings in the employment context equipped with further national possibilities (also see Sect. 6.5.7).

6.5.2 The Threshold

Since most of the European data protection laws do not know specific labour regulations, i.e. no specific regulation on DPOs at work or other specifications in

the employment context, there was no need of thresholds excluding one or the other company. For some new responsibilities are transferred to undertakings, the European Commission set a threshold to some of them. The European Commission's version of GDPR fixed a threshold of 250 employees a company would need in order to be concerned. The "High Level Group of Independent Stakeholders on Administrative Burdens" established in 2007 by the European Commission might have been one of the drivers of the Commissions' GDPR proposal. Although, in Austria this threshold would lay the "burden" of a DPO at the company level on only 2 % of the companies, nevertheless employers' interest organizations strongly opposed. This again shows the unwillingness of employers to seriously deal with the topic. Just 16 % of Austrian companies voluntarily installed a DPO at the company level and this officer is not responsible for employees' personal data.[35]

The threshold designed by the European Commission comes into force, if data controllers not established in the European Union have to entitle a representative in Europe (Art. 25), if they designate a DPO at the company level (Art. 35), if they document data proceedings (Art. 28) and if it comes to sanctions (Art. 79).

The LIBE committee proposed another threshold in article 25: "a controller processing personal data which relates to less than 5000 data subjects during any consecutive 12-months period and not processing special categories of data [...] or data on children or employees in large-scale filing systems."[36] According to the LIBE committee's plans, a risk analysis should be implemented for companies below the threshold as well, but documentation duties should apply to all companies. The LIBE definition posts a more technical approach. It lays the emphasis not on company size, but on the companies' products, no difference whether these products are materials or services. The LIBE approach has a look on what the company does and not how big it is. Seen from an employee's interest perspective this facilitates law enforcement by the fact that employee data is declared valid, if it comes to obligatory establishing representatives of controllers, since this representative would be responsible for fulfilling the data subject's rights. Documentation duties for all companies and a newly defined threshold are a return to the employees' interest.

6.5.3 Consent

The LIBE proposal does no longer distinguish between consents given by a data subject under circumstances of equal power or under circumstances of unequal power, while the European Commission's draft did so. In recital 34, the Commission explicitly defined the employment relation as a relationship with imbalanced power,

[35] Clara Fritsch. "Vogelstraußpolitik, der Tenor von Umfragen zum innerbetrieblichen Datenschutz in Österreich." *Arbeit und Wirtschaft* (2008).

[36] Jan Albrecht, *Inofficial Consolidated Version after LIBE Committee Vote Provided by the Rapporteur* (Brussels 2013).

in which consent should not be a legitimate ground for data proceedings. This gave hope to employees and their representatives and interest organizations that the bad practice of blank consents would diminish. This optimism reduced after the LIBE voting.

6.5.4 Documentation

Until now, it was up to national legislation how to handle the transparency principle. Austria decided to implement a register open to the public, in which each data proceeding is to be recorded by the data controller – the employer in employment relations. The register, handled by the Austrian Data Protection Authority, helped works councils as well as employees to enforce their right on information, to force the employer to comply with the law. When it comes to data transfer to third countries or proceedings including sensible data, the Austrian authority actually had to approve proceedings, hence becoming an ally of employees and works councils, who do not want employees' data to leave the company in order not to lose access and controlling rights.

Documentation duties now are shifted to the company level by the GDPR (Art. 28). Although, the national authorities have the right to control these documentations (Art. 29), the anticipated practice – at least in Austria – is of only little usage concerning this right. Particularly, since it is evident that the Austrian authority holds the 23rd position out of 24 European member states when it comes to personnel resources.[37] The closure of the official documentation register in Austria will certainly weaken the employees' position.

6.5.5 Responsibility on the Company Level

A new pile of employer's responsibilities and legal data proceeding possibilities will find their way into employment relations: Data protection by design and by default (Art. 23), documentation at the company level (Art. 28), data protection impact assessment (Art. 33), data protection compliance review (Art. 33a), codes of conduct developed or at least proofed by the data protection authority (Art. 38), data protection certification (Art. 39) and binding corporate rules approved by the national data protection authority (Art. 43) shall now be available for employers to proof their data processing to be legal. Experience – at least in Austria – shows that self-made, self-controlled inner-company rules are likely to be weak, not to be followed and not to be sanctioned. Especially, if there is little participation and

[37] Hans Zeger, "Datenschutz International, Unterschiede, Gleichwertigkeit, Vereinbarkeit" (Vienna, 2007).

controlling power of employees' representatives and unions or at least of public bodies, one cannot really trust the self-regulation of companies. It seems as if the GDPR follows the already existing practice in some European countries where employer organizations wrote codes of conduct regulating employees' internet behavior on workplaces, e.g. in Ireland, Italy or Norway.[38]

The LIBE vote added just one of the new accountability tools to the co-determination rights of employees' representatives: When proceeding data by means of binding corporate rules, employers have to design these rules together with the employees' representatives or at least inform them about their existence (Art. 43/1a).

6.5.6 The Data Protection Officer

A compulsory DPO at the worksite, who performs his/her tasks independently and represents a gateway for employees, their representatives, employers and the data protection authority, was one of the most important demands expressed by the Austrian Trade Union Federation. Experts from Germany postulate this as well. Peter Schaar, the former German Federal Commissioner for Data Protection and Freedom of Information, states that the DPO is an essential addition to the European Data protection law. But Schaar adds that the DPO needs more protection from arbitrary actions by employers and needs to cooperate closely with employees' representatives.[39] The demand for a compulsory DPO at the worksite with dismissal protection is in coherence with the Europeans Commission's and the LIBE Committee's draft of the GDPR. The European Commission's proposal created the DPO not bound to employer's instructions, but without employees' representatives' participation or even information (Art. 35 ff). Only 2 % of Austrian companies would have had to install this position, since the Commission set a 250-employee-threshold (see Sect. 6.5.2).

Some amendments during parliamentary discussions of the Committee on Employment and Social Affairs (EMPL) also found their way into the LIBE proposal, such as the ban of secret surveillance or blacklisting. Other amendments of the EMPL were brought in on part of parliamentarians standing close to unions, advocating for more employees' representatives' participation rights, but did not survive the EMPL vote in February 2013.

LIBE amended a 4-year working period (Art. 35/7) instead of the 2 years proposed by the Commission, dismissal protection (Rec. 75), "the ability to work with employee representation [...], advanced training measures to maintain the specialized knowledge required to perform his or her duties" (Rec. 75a) as well as

[38]Catherine Delbar et al., "New technology and respect for privacy at the workplace," European Industrial Relations Observatory (2003).

[39]Peter Schaar, "Die geplante EU-Datenschutz-Grundverordnung, Auch beim Beschäftigtendatenschutz ist ein Nachbessern erforderlich", Computer und Arbeit (2013/3).

the task to inform employee representatives on data processing of the employees (Art. 35/1j). Hence, at least the recitals explain that DPOs also have to deal with employees' personnel data and serve as contact person for their concerns. This could strengthen employees' enforcement of the fundamental right to privacy.

6.5.7 The Article on Employment Relation (Art. 82)

From a union's perspective, the article on special data proceeding within an employment relation is one of the crucial parts of the GDPR. It was reworked by the EMPL and sets standards in employee data protection all around Europe for the first time. Although the GDPR now sets one standard for all European member states, it will be hard to match it with labour law regimes (compare Sect. 6.5.1). Having European minimum standards on dealing with employee data is a proper means to also take into account special national labour rights. It would have been of no use, if according to the GDPR – like the European Commission stated in its first draft – member states would have had to apply all the same level of workplace related data protection regardless of their national labour legislation. Especially participation rights of workplace representatives concerning collective agreements – whether on company, branch or regional level – would have been impaired by the GDPR.

What strengthens employee data protection within this article is the ban of blacklisting employees, who e.g. took part in union actions making it impossible for them to find work again and the ban of any hidden surveillance measures. Employers need to offer clear information and are allowed to precede personal data only if: "The purpose of processing such data must be linked to the reason it was collected for and stay within the context of employment. Profiling or use for secondary purposes shall not be allowed" (Art. 82/1a). What we still miss are workers' representatives' participation rights.

6.5.8 The One-Stop-Shop

Although a harmonized law concerning data protection at the workplace is a welcomed step further, the now installed principle of one-stop-shop will be a practical obstacle to protect employees' privacy rights. The "one-stop-shop", meaning that establishing one main company within the European Union providing one DPO for all other establishments, facilitates data transfer for companies. In principle, this could also make it easier for employees to enforce their data protection rights. They would not have to pass several authorities, would have a well-defined authority or other responsible person to address and could rely on being treated as all other European employees.

As consultant practice shows these advantages might be overridden by disadvantages such as: data subjects must first find out, who is responsible for their

data protection requests – the bigger the multinational, the more complicated this is; especially within "matrix-organisations", a currently favoured organisation structure throughout multinationals. In matrix-structured companies the superior is no longer responsible for disciplinarian and professional tasks. The authorities are separated from each other and from their local connections. An employee may have his/her disciplinary superior two floors above and the professional superior some 2.000 km away at the mother company. Such company structures cause rising exchange of personnel data within the personnel management via ICT systems. Since labour law and therein inscribed participation rights of workplace representatives on the company level differ all over Europe – and beyond – it seems likely that multinationals will locate their main establishment in a country, where participation rights are rather week. Such regime shopping – quite common in matters of tax regulations – might then also occur in terms of data protection. This is already happening, for example, in Ireland, where there are low taxes and low data protection interests united and where big players in the worldwide web already have headquarters as the Financial Times reported on September 25th, 2013 (eBay, Facebook, Google, LinkedIn, Twitter, Yahoo, Accenture, . . .). While Ireland's data protection commissioner welcomes the one-stop-shop (according to the Financial Times on July 15, 2013), the experience users make when claiming for their right on information is that Irish data protection authorities are not supportive.[40]

6.5.9 Sanctions

The newly adopted sanction regime differs from the current one. Sanctions are no longer imposed according to a fixed amount but also according to a percentage share of the annual worldwide turnover (Art. 78 and 79) – similar to European competition legislation. The European Commission's draft included a maximum of 2 % of the worldwide turnover, while the LIBE voted for a maximum penalty of even 5 %. This, of course, alarmed enterprises and is definitely one explanation for the extraordinary high number of amendments to the GDPR.

When visiting Austrian companies for consulting reasons, one observes that multinationals start being concerned about high sanctions they might face according to the GDPR. Until now, it was regarded to be a trivial offense not to fulfill the requirements of the data protection law in Austria – in particular because there were no legal consequences. But due to the new European data protection regime and its future sanction fees, "these times will pass away" as a works council put it during recent consultation talks.

[40]For example the experiences of the NGO "Europe versus Facebook" (http://www.europe-v-facebook.org/DE/de.html).

6.6 Summary

General recognition of employees' data protection as a special form of data protection is a step forward. It is more than many EU member states currently offer their employees. An equal law across Europe – a DPO in many companies, specific regulations for the employment relation and higher sanctions – will add more value to employees' privacy.

Mutual efforts of employees' interest organizations (such as ETUC, UNI or the ÖGB) and the European social partners in the ESSC made some advantages possible for employees' data protection (such as the DPO, the ban of blacklisting, or the higher sanctions).

The current directives' proposal fulfils the employers' will of easier data transfers but it lacks the employees' right to easily access his or her personal data. Hence there is still an imbalance between employers' possibilities and employees' rights. The GDPR clearly fails regarding participation rights of workplace representatives for example, when it comes to establishing a DPO at the company level. Obviously, employee representatives' participation rights are shifted to the national level, but some minimum standards may improve employees privacy.

Bibliography

Albrecht, Jan, "Inofficial Consolidated Version after LIBE Committee Vote Provided by the Rapporteur" (published 22nd of October 2013, accessed February 12, 2014, http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf)

Article 29 – Data Protection Working Party, "Opinion on the Processing of Personal Data in the Employment Context, Executive Summary", published 2001, accessed February 1, 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48sum_en.pdf

Article 29 – Data Protection Working Party, "Working document on the Surveillance of Electronic Communications in the Workplace", published 2002, accessed February 1, 2014, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf

Busch, Klaus, Hermann, Christoph, Hinrichs, Karl und Thorsten Schulten, "Eurokrise, Austeritätspolitik und das Europäische Sozialmodell, Wie die Krisenpolitik in Südeuropa die soziale Dimension der EU bedroht.", Friedrich-Ebert-Stiftung, November 2012, accessed May 4 2014, http://library.fes.de/pdf-files/id/ipa/09444.pdf

Committee on Employment and Social Affairs, "Opinion for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for General Data Protection Regulation", published March 4, 2013, accessed February 2, 2014 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN#title3

Council of the European Union, "Interinstitutional File 2012/0011", published 2012, accessed February 3, 2014, http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2010227%202013%20INIT

Delbar, Catherine, Mormont, Marinette and Marie Schots, "New technology and respect for privacy at the workplace." *European Industrial Relations Observatory* (2003), accessed February 4, 2014, http://www.eurofound.europa.eu/eiro/2003/07/study/tn0307101s.htm

European Commission, "Second stage consultation of social partners on the protection of workers' personal data", Brussels, 2002, accessed February 11, 2014, http://ec.europa.eu/social/main.jsp?catId=708

European Commission Directorate General Internal Market Unit E Media and data protection, "Special Eurobarometer, Data Protection", Brussels, 2003, accessed February 4, 2014, http://ec.europa.eu/public_opinion/archives/ebs/ebs_196_en.pdf

European Commission, "The European e-Business Report, A portrait of e-business in 10 sectors of the EU economy, 5th Synthesis Report of the e-Business W@tch", Brussels 2006, accessed February 4, 2014, http://ec.europa.eu/enterprise/archives/e-business-watch/key_reports/documents/EBR06.pdf

European Commission Direction General Justice Freedom and Security, "Flash Eurobarometer, Data Protection in the European Union, Citizens' perceptions, Analytical Report", Brussels 2008, accessed February 4, 2014, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf

European Commission Direction General Justice Directorate C Fundamental rights and Union citizenship Unit C.3 Data protection, "Summary of Replies to the Public Consultation about the Future Legal Framework for Protecting Personal Data", Brussels, November 4, 2010, accessed February 4, 2014, http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf

European Commission "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)", Brussels 2012, accessed February 4, 2014, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF

European Economic and Social Committee, "Opinion of the European Economic and Social Committee on the 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)'", *Official Journal of the European Union C 229/90*, Brussels 31.7.2012, accessed February 1, 2014, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:229:0090:0097:EN:PDF

European Trade Union Confederation, "ETUC response to the Communication from the Commission 'A comprehensive approach on personal data protection in the European Union'", Brussels, 2011, accessed February 4, 2014, http://www.oegb-eu.at/servlet/BlobServer?blobcol=urldokument&blobheadername1=content-type&blobheadername2=content-disposition&blobheadervalue1=application%2Fpdf&blobheadervalue2=inline%3B+filename%3D%22EGB-Position_zur_Datenschutz-Richtlinie_%2528in_englischer_Sprache%2529.pdf%22&blobkey=id&root=S05&blobnocache=false&blobtable=Dokument&blobwhere=1294824487171

European Trade Union Confederation, "ETUC position on the General Data Protection Regulation – improving the protection of workers' data", Brussels, 2012, accessed February 4, 2014, http://www.oegb-eu.at/servlet/BlobServer?blobcol=urldokument&blobheadername1=content-type&blobheadername2=content-disposition&blobheadervalue1=application%2Fpdf&blobheadervalue2=inline%3B+filename%3D%22ETUC_Datenschutz.pdf%22&blobkey=id&root=S05&blobnocache=false&blobtable=Dokument&blobwhere=1353945635532

Fritsch, Clara. "Vogelstraußpolitik, der Tenor von Umfragen zum innerbetrieblichen Datenschutz in Österreich", *Arbeit und Wirtschaft 04/2008*, Wien, 2008, accessed February 4, 2014, http://www.arbeit-wirtschaft.at/servlet/ContentServer?pagename=X03/Page/Index&n=X03_1.a_2008_04.a&cid=1208204202221

Haraway Donna, "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective", Feminist Studies, Vol. 14 No. 3, 1988

Harding Sandra, "Standpoint methodologies and epistemologies: a logic of scientific inquiry for people", in UNESCO and International Social Science Council, 2010, pages 173–175. World Social Science Report: Knowledge Divides. Paris: UNESCO, accessed May 4 2014, http://knowledge4empowerment.files.wordpress.com/2011/06/harding_standpoint_-2010.pdf

Hendrickx, Frank. *Protection of workers' personal data in the European Union, Two Studies.* University of Leuven/Tilburg, 2002, accessed February 4, 2014, http://collection.europarchive.org/dnb/20070702132253/. http://ec.europa.eu/employment_social/labour_law/docs/dataprotection_hendrickx_combinedstudies_en.pdf

Hirsh, Elizabeth and Garry A. Olson, "Starting from Marginalized Lives: A Conversation with Sandra Harding", JAC, journal of Rhetoric, Culture, & Politics, 1995, accessed May 4 2014, http://www.jaconlinejournal.com/archives/vol15.2/hirsch-starting.pdf

International Labour Organization, "Protection of Workers' Personal Data", Geneva 1997, accessed 2nd of February 2014 http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf

Knorr-Cetina, Karin, *Manufacture of Knowledge* (Oxford 1981)

Mitrou, Lilian and Maria Karyda, "Employees' privacy vs. employers' security, Can they be balanced?", Elsevire Ltd. 2005, accessed February 4, 2014, http://www.icsd.aegean.gr/website_files/metaptyxiako/82038633.pdf

O'Rourke, Anne, Teicher Julian and Amanda Pyman, "Internet and Email Monitoring in the Workplace: Time for an Alternate Approach", *Journal of Industrial Relations* (2011 vol. 53)

Österreichischer Gewerkschaftsbund, "Stellungnahme zum Gesamtkonzept für den Datenschutz der Europäischen Union", Vienna, 2011, accessed February 4, 2014, http://www.oegb-eu.at/servlet/BlobServer?blobcol=urldokument&blobheadername1=content-type&blobheadername2=content-disposition&blobheadervalue1=application%2Fpdf&blobheadervalue2=inline%3B+filename%3D%22%25D6GB-Stellungnahme_zur_Datenschutz-Richtlinie.pdf%22&blobkey=id&root=S05&blobnocache=false&blobtable=Dokument&blobwhere=1294824487158

Riesenecker-Caba, Thomas and Alfons Bauernfeind. *Verwendung personenbezogener Daten und Grenzen betrieblicher Mitbestimmung: Datenschutz in der Arbeitswelt*. Arbeiterkammer Wien, 2011.

Schaar, Peter, "Die geplante EU-Datenschutz-Grundverordnung, Auch beim Beschäftigtendatenschutz ist ein Nachbessern erforderlich", *Computer und Arbeit* (Bund Verlag 2013/3)

Uni global union, "online rights at work", Nyon 2000, accessed February 3, 2014, http://www.uniglobalunion.org/sites/default/files/attachments/pdf/OnlineRightsAtWork_EN-print.pdf

Uni global union, "Executive Committee, Item 9, Data protection and employment in the European Union" (paper presented at the executive meeting in Madrid, June 2–3, 2010).

Uni global union "Submission to the European Commission communication A comprehensive approach on personal data protection in the European Union", Brussels, 2011, accessed February 7, 2014, http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/uni_en.pdf

Zeger, Hans, "Datenschutz International, Unterschiede, Gleichwertigkeit, Vereinbarkeit" (paper presented at a seminar, Austria, Vienna, October 16–18, 2007).