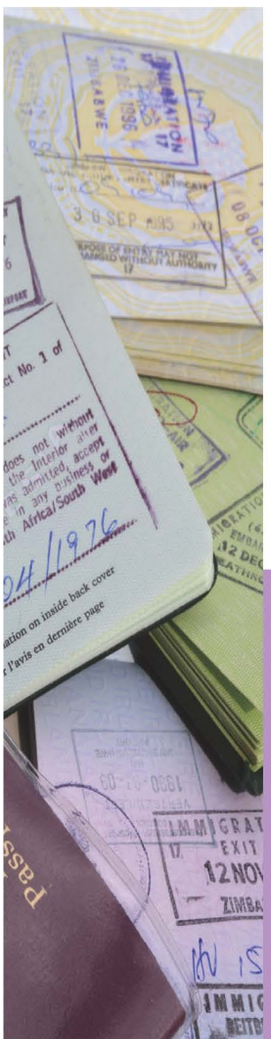
EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS



Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

Protection of Personal Data in Work-related Relations

STUDY

EN

2013

EUROPEAN PARLIAMENT

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

Protection of Personal Data in Work-related Relations

STUDY

Abstract

This study looks at the possibilities to complement the general data protection framework with specific rules for employment relations. Data protection in employment relations clearly touches on labour law. The specific actors involved, the social partners, and the strategies used in the past to harmonise labour law, are taken into account. The study evaluates the application of the existing general data protection framework in employment relations and considers possible options to improve it.

PE 474.440 EN

This document was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs.

AUTHOR(S)

Paul De Hert
Hans Lammerant

Under the coordination of the Centre d'Etudes sur les Conflits, Liberté et Sécurité (CCLS) and the Justice and Home Affairs section of the Centre for European Policy Studies (CEPS).

The authors would like to express their gratitude to Prof. Elspeth Guild and Dr. Sergio Carrera (CEPS) for their comments on an earlier version of this study.

RESPONSIBLE ADMINISTRATOR

Alessandro DAVOLI
Policy Department C - Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: poldep-citizens@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

To contact the Policy Department or to subscribe to its newsletter please write to:
poldep-citizens@europarl.europa.eu

Manuscript completed in April 2013

This document is available on the Internet at:
http://www.europarl.europa.eu/studies

DISCLAIMER

CONTENT

LIST OF ABBREVIATIONS

BDSG	Bundesdatenschutzgesetz
CBP	College Bescherming Persoonsgegevens
CNIL	Commission nationale de l'informatique et des libertés
CoE	Council of Europe
DPA	Data Protection Authority
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EESC	European Economic and Social Committee
ETUC	European Trade Union Confederation
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
ILO	International Labour Organisation
RFID	Radio-frequency identification

EXECUTIVE SUMMARY

The main goal of this study is to provide the LIBE Committee with background information and useful recommendations for possible future activities on data protection in employment relations.

The European Commission is currently reviewing the general framework on the protection of personal data and has proposed a General Data Protection Regulation.

This paper starts with the observation that a number of attempts have been made to provide for data protection legislation in employment relations – complementary to the general framework – but without results. This study is thus not limited to a legal study of the application of data protection in employment relations, but also looks at the political process linked to developing such legislation.

Data protection in employment relations also touches upon labour law. The labour law context has its specific political process and involves the social partners as actors. For this reason the study takes the perspective of strategies used to harmonise labour law in the past to evaluate the application of data protection in employment relations today, and looks at the options available for future activities. Four strategies can be identified: a) developing detailed rules with directives and regulations, b) European-level social dialogue, c) soft law methods to achieve policy coordination, but avoiding binding legislation, d) using general principles enshrined in fundamental rights, which are adaptable to very diverse contexts.

In the first chapter we present the data protection framework at the international, EU and national level. The general data protection framework, provided in Directive 95/46/EC or in the newly proposed GDPR, is analysed as a framework of general principles. These general principles can be used directly, translated into more specific legislation or through social dialogue, or given as guidance through soft law instruments. Several examples of the application of data protection in employment relations are then analysed, reflecting the use of the different strategies.

To guide the assessment of the need for complementary rules, we look at the application of data protection in specific issues in employment relations in the second chapter. The choice of these issues is based on the second stage of the consultation of social partners in preparation of the 2004 draft Directive on the protection of workers' personal data.[1] We consider the application in several Member States of the general framework of Directive 95/46/EC to see if the general principles-based approach is problematic. We conclude that a general principles-based approach leads to a patchwork of diverging national solutions.

In the third chapter we revisit the four strategies and the policy options they offer. We look at the positions of the social partners and those reflected in the discussions in the European Parliament. To conclude we evaluate the policy options and formulate some recommendations.

[1] European Commission, *Second stage consultation of social partners on the protection of workers' personal data*, 2004.

GENERAL INFORMATION

KEY FINDINGS

- When observing the stated need of several governments (i.e. Germany, Sweden, Finland) and international bodies (European Commission, CoE, ILO) to complement the general data protection framework with specific rules for employment situations, there is a notable gap between intentions and outcomes.
- Employers' organisations and unions do not share a common definition of the issue, yet both perspectives do point to the EU level as the appropriate level to deal with such matters.
- The gap observed reflects the difficulties inherent in harmonising labour law. These difficulties are not of a legal nature, but more a question of building trust. The data protection authorities lack legitimacy in the workplace. Effective enforcement of data protection in employment relations must involve the social partners.
- Harmonising data protection in employment relations will need to fit in with the strategies used to harmonise labour law. Four strategies can be identified: a) developing detailed rules with directives and regulations, b) European-level social dialogue, c) soft law methods to achieve policy coordination, but not binding legislation, d) using general principles enshrined in fundamental rights, which are adaptable to very diverse contexts.
- The right to protection of personal data evolved out of the right to privacy and became an autonomous fundamental right. From an ‘opacity tool’, limiting interference in the private sphere, it became a transparency tool, regulating and organising the legitimate processing of personal data and subjecting this processing to control by the data subject.
- The data protection framework contains a set of principles that are applied to every act of processing personal data: legitimacy, finality, proportionality, relevance, accuracy, transparency, data security, participation and control by the data subject. These principles provide a flexible framework that can be applied in diverse situations.
- We recognise the four strategies in the implementation of data protection in employment relations at different levels. Detailed regulations were devised by the ILO, the CoE, DG Employment and Social Affairs and in Member States. Social dialogue was used in the implementation at national level. The Opinions of Art. 29 WP and other guidance provide an example of soft law instruments. The general principles-based approach is used in the European institutions and in several Member States.
- In general, we conclude that the application of general principles leads to a patchwork of divergent national applications. This is often due to differences in other laws, leading to different contexts in which the general principles are applied. But we also see considerable variation in the application of the general principles as such. One such area is new technologies, where there is still much to learn regarding how to deal with them and the impact they have on social behaviour. Another area is long-standing customs and cultural traditions, such as giving information about criminal convictions.

- This study first concludes that the legal harmonisation of data protection legislation is important for the employment context. Both employers and workers have an interest in the harmonisation of data protection laws.
- A second conclusion is that the application of data protection in the employment context based on general principles leads to a patchwork of different solutions, especially when new technologies are involved.
- A third conclusion is that to develop data protection rules in employment matters, the specificity of the political process in labour issues has to be taken into account. The data protection authorities lack legitimacy in the employment context. The social partners, as legitimate actors in employment matters, have to be involved and given ownership in the process to develop rules concerning data protection in employment matters.
- An effective approach needs to present a mix of hard and soft law. Hard law can create legal certainty, while soft law allows for learning processes and trust-building.
- Article 82 GDPR, including the proposed amendments, reflects the different tensions present in the debate on data protection in employment matters. The underlying tensions can only be resolved properly through a trust-building process, a political process that takes all interests into account. Such a process must involve the social partners more directly.
- The proposed amendments to Article 82 GDPR, which include minimum standards for data protection in employment relations, reflect a wish to develop at least a minimal framework for data protection in employment relations. Although they lack coherence, they can be used as leverage to task the European Commission and the social partners to develop a more coherent framework. A review of Article 82 GDPR is recommended. The Commission should be asked to substitute the minimum standards included in Article 82 with a coherent Directive on data protection in employment relations.
- An effective application of data protection on new technologies needs to be developed. This justifies consultation on a regular basis between the social partners and the DPAs at national and European level. Such a consultation should create awareness of the impact of new technologies and create the necessary trust to develop common solutions.

INTRODUCTION

KEY FINDINGS

- When observing the stated need of several governments (i.e. Germany, Sweden, Finland) and international bodies (European Commission, CoE, ILO) to complement the general data protection framework with specific rules for employment situations, there is a notable gap between intentions and outcomes.
- Employers' organisations and unions do not share a common definition of the issue, yet both perspectives do point to the EU level as the appropriate level to deal with such matters.
- Data protection in employment relations interferes with other areas of law, especially labour law. A multi-layered approach is needed. Harmonisation efforts have to take into account the specific nature of the other areas of law involved.
- The gap observed reflects the difficulties connected to harmonising labour law. These difficulties are not of a legal nature, but a question of building trust.
- Data protection authorities lack legitimacy in the workplace. Effective enforcement of data protection in the workplace will have to involve the social partners.
- Harmonising data protection in employment relations will need to fit in with the strategies used to harmonise labour law. We note four strategies: a) developing detailed rules with directives and regulations, b) European-level social dialogue, c) soft law methods to achieve policy coordination, but avoiding binding legislation, d) using general principles enshrined in fundamental rights, which are adaptable to very diverse contexts.

In recent years several scandals have put the spotlight on data protection in employment relations.

The firm *Lidl* was fined twice for violations of the German Data Protection Act. The first investigation began in 2008 after press reports about covert filming by *Lidl* of its employees, even in private areas such as toilets, and keeping personnel files with private details.[2] A year later it transpired that *Lidl* kept files on the health of employees.[3] *Deutsche Bahn* was fined in 2009 for a massive screening of the e-mails and computer files of its 173,000 employees, without grounds for suspicion.[4] And *Telekom* checked if managers, members of the board of directors and leading worker representatives had had telephone contact with journalists.[5]
Such practices – in clear violation of the laws on data protection – show that data protection is far from being a given in employment situations. These controversies

[2] Stern, 26 March 2008, http://www.stern.de/presse/vorab/ueberwachungsskandal-lidl-liess-beschaeftigte-systematisch-bespitzeln-615032.html.

Stern, 11 September 2008, http://www.stern.de/wirtschaft/news/unternehmen/ueberwachungsskandal-lidl-muss-millionen-strafe-zahlen-638756.html.

[3] Der Spiegel, 4 April 2009, http://www.spiegel.de/wirtschaft/mitarbeiterkontrolle-lidl-fuehrte-geheime-krankenakten-ueber-mitarbeiter-a-617347.html.

Der Spiegel, 5 April 2009, http://www.spiegel.de/wirtschaft/lidl-datenskandal-brisante-papiere-in-der-muelltonne-a-617348.html.

[4] Zeit, 23 October 2009, http://www.zeit.de/wirtschaft/unternehmen/2009-10/bahn-bussgeld.

[5] http://www.datenschutzbeauftragter-info.de/telekom-bespitzelungsaffaere-bgh-bestaetigt-haftstrafe-fuer-ehemaligen-abteilungsleiter/.

strengthened the call for specific rules for the protection of employees' personal data to complement general data protection rules.

Such calls are not new, however. The Council of Europe indicated in 1989 in its recommendation on 'Protection of personal data used for employment purposes'[6] the desirability of adapting the general rules, given in Convention n° 108 from 1981, to the particular requirements of the employment sector. The International Labour Organisation (ILO) adopted in 1996 a Code of Practice on the Protection of Workers' Personal Data.[7] After establishing the general data protection framework with the adoption of Directive 95/46/EC, the Commission committed itself to take initiative to complement this general framework for employment situations. From 2001 till 2003 the European Commission did consult with the social partners on a European directive on the protection of workers' personal data.[8] But this attempt did not lead to results. Also in the Member States several initiatives were taken, but with limited results. The Finnish Act of May 2001, supplemented in 2004, on protection of privacy in working life[9] was the first national legislation in the EU dealing specifically and quite comprehensively with data protection in the workplace. In several countries some specific rules on employment-related data protection were included in data protection laws, labour laws or specific regulations or in collective bargaining agreements (CBA). But on the whole the results were limited, and attempts in Sweden and Germany to make specific data protection laws for employment situations were not successful (yet). We can on one hand observe several governments (Germany, Sweden, Finland) and international bodies (European Commission, CoE, ILO) stating the need or intention to complement the general data protection framework with specific rules for employment situations. On the other hand we observe very few results. This gap between the widely stated intention and the rule making that did result is remarkable. What are the reasons behind this gap between needs and deeds? Is there indeed a need for specific rules? What are the options available?

Looking at the needs expressed at non-governmental level, we notice that there is no common definition of the problem. Employers' organisations do express a need for harmonisation. It is difficult for companies which are active across the EU to define common policies towards their employees while having to respect a diverse patchwork of national data protection laws. Unions on the other hand do signal problems with the protection of personal data at the workplace. When such personal data gets transferred to another country inside or outside the EU, questions arise on how the protection of this data can be guaranteed or enforced. More generally, the existing EU data protection framework seems to be lacking in addressing privacy issues at the workplace or in its enforcement. These different perspectives on data protection problems do not guarantee a common vision on how to address these issues. But both perspectives do point to the EU level as the appropriate level to deal with these issues. Data protection was originally addressed at European level to avoid that national data protection legislation would be a barrier for the internal market. For this reason the new General Data Protection Regulation (GDPR) introduces even further harmonisation. Leaving too much space for widely different

---

6 Council of Europe, *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.

7 ILO, *Code of practice on the protection of workers' personal data*, Geneva, International Labour Office, 1997

8 European Commission, *Communication from the Commission, First stage consultation of social partners on the protection of workers' personal data*, 2003, http://ec.europa.eu/social/main.jsp?catId=708&langId=en; European Commission, *Second stage consultation of social partners on the protection of workers' personal data,* 2004, http://ec.europa.eu/social/BlobServlet?docId=2504&langId=en.

9 Ministry of Justice Finland, *Act on the Protection of Privacy in Working Life (759/2004)*, 2004, English translation on http://www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf.

approaches concerning data protection in employment relations, would run counter to this objective.

Data protection in employment relations cannot be considered in isolation. In practice data protection interferes with individual and collective labour law, while also health law, non discrimination law, criminal and evidence law can come into play. The legal framework of data protection is based on several international and EU legal instruments, while labour law, social security law, criminal and evidence law is mostly national law and differs widely across the EU. Therefore a multi-layered approach has to be taken. Harmonisation efforts have to take into account the specific nature of each of these areas.

The difficulties associated with harmonisation do differ in each of these areas and are not just of a technical nature. Harmonisation of labour law has been difficult and contentious, and several strategies have been taken in the past. The gap signalled above between intention and outcome concerning data protection in employment relations is not just the reflection of technical difficulties linked to the application of data protection. In the first place it reflects the difficulties connected to harmonising labour law. This is not just a question of legal technique, but of building trust. Together with harmonising laws, also interests have to be harmonised through social dialogue.

Rule-making in labour law and social policy has historically involved quite different political processes compared to other policy areas. Through social dialogue between employers' organisations and workers' organisations very different political players came to the foreground. A first consequence of this is that the data protection authorities, being in other circumstances the most prominent actors representing collective interests, have a legitimacy problem. Effective enforcement of data protection in the workplace will have to come to terms with the role of the social partners. The shape industrial relations have taken at national level will determine how this is done at national level. Similarly, it is important to take into account how at the European level the social dialogue functions and the strategies taken to harmonise labour law. This leads to the second consequence that, when it comes to formulating options and recommendations, we have to look how the options to deal with data protection in the employment context fit with the strategies to harmonise labour law.

Four legal strategies can be discerned through the development of European social policy and labour law, which also left their traces in the EU institutional framework.[10]

a) The first is harmonisation through EU hard law instruments. This is the strategy traditionally used to develop the internal market. With directives and regulations the European institutions develop a relative detailed legal framework, with little space for national differences.
b) The second is European-level social dialogue, foreseen in article 155 TFEU. The social partners can negotiate agreements at EU-level, which can be given legal force by the Council, if the issue is within the remits of article 153 TFEU, or by the Member States.
c) The third method is the open method of coordination. This is a soft law approach to achieve policy coordination, but avoiding binding legislation. The continuous dialogue and influencing through research, exchange of best practices, establishment of guidelines, periodic monitoring and evaluation, ... should achieve a mutual learning and harmonising effect.

[10] Bercusson, B., *European Labour Law*, Cambridge University Press, 2009.

d) The fourth strategy uses general principles, which are applicable in and adaptable to very diverse contexts. Labour law scholars have called it the strategy of fundamental rights or the constitutionalisation of labour law.[11] Such a 'fundamental rights approach' is another way to avoid narrow and detailed harmonisation. But, as human rights scholars will object to calling a reduction to general principles in opposition to more developed legislation a fundamentals rights approach, I will call it general principles-based.

This specificity of the political process on labour issues also has consequences for the role of the European Parliament. Depending on the strategy chosen, the role of the European Parliament will differ. In the first and fourth strategy the European Parliament can play its full role of co-deciding on the legal framework. In the first strategy that is on a new specific instrument, while the fourth strategy limits itself to the general framework or the GDPR now under discussion. The 2 other strategies provide a much more limited role for the European Parliament. It has the right to be informed on the results of the social dialogue on European level, but has no decision making role. Still, the European Parliament has means to push the other actors into action.

We use these strategies to approach the question on how to complement the general data protection framework with rules or instruments to guide its application in employment relations.

In the first chapter we present the data protection framework on international, EU and national level. The general data protection framework, provided in directive 95/46/EC or in the newly proposed GDPR, fits well with the general principles-based approach. In this approach we do not need extra instruments, as the general framework is sufficient for its application in employment relations. Therefore, after an introductory overview, we present this framework of general principles. We continue with presenting attempts to complement this general framework with extra rules concerning the application in employment relations. First on international level (ILO, CoE), then at EU level an unsuccessful attempt to make a directive on data protection and privacy in employment matters. All these efforts can be seen as examples of the first strategy of translating the general principles in detailed legislation. In section 1.5 we look at how these different strategies are also present in the implementation in the Member States. The application of data protection in the EU institutions, presented in section 1.6, is another example of the general principles-based approach.

To guide the assessment of the need for complementary rules, we look in the second chapter at the application of data protection at specific issues in employment relations. The choice of these issues is based on the second stage of the consultation of social partners in preparation of the 2004 draft directive on the protection of workers' personal data.[12] We look at the application in several Member States of the general framework of directive 95/46/EC to see if the general principles-based approach leads to problems.

In the third chapter we look again at the four strategies and which policy options they provide. We look at the positions of the social partners and those reflected in the discussions in the European Parliament. To conclude we evaluate the policy options and formulate some recommendations.

[11] Bercusson, B., *European Labour Law*, 2009 ; Hendrickx, F., The Future of Collective Labour Law in Europe, *European Labour Law Journal*, Vol 1 (2010), n°1, p. 72.

[12] European Commission, *Second stage consultation of social partners on the protection of workers' personal data*, 2004.

1. THE LEGAL FRAMEWORK OF DATA PROTECTION

KEY FINDINGS

- The right to protection of personal data evolved out of the right to privacy and became an autonomous fundamental right. From an opacity tool, limiting the interference in the private sphere, it became a transparency tool, regulating and organising the legitimate processing of personal data and subjecting this processing to control by the data subject.
- The data protection framework contains a set of principles that are applied to every act of processing personal data: legitimacy, finality, proportionality, relevance, accuracy, transparency, participation and control by the data subject, data security. These principles provide a flexible framework that can be applied in diverse situations.
- The ILO and the CoE developed soft law instruments to provide guidance on the application of these principles in employment relations.
- After consultations with the social partners, in 2004 DG Employment and Social Affairs drafted a Directive concerning the processing of workers' personal data and the protection of privacy in the employment context. This draft was never presented to the Commission, but shows that more detailed data protection legislation for employment relations is feasible from a technical point of view.
- The implementation of data protection in the Member States shows the same variety of techniques in the employment context: although the application of the general principles as such is prominent, translating the general principles into specific legislation or through social dialogue can also be found, as can the provision of soft law guidance by the DPAs.
- The application of data protection in the European institutions can be seen as an effective application of the general principles-based approach.

This chapter presents the legal framework of data protection. The first section presents the evolution of this framework out of the fundamental right of privacy into an autonomous fundamental right and legal framework. This legal framework has inherited the general principle-structure from its origin in fundamental rights and as such it is very well adapted for use in the general principles-based strategy in the employment context. Section 1.2 develops the general principles in the data protection framework.

The next sections deal with applications of the data protection framework. Section 1.3 presents the efforts of the ILO and the CoE to provide complementary rules for employment relations. Their soft law instruments are currently the only complementary instrument available. Section 1.4 presents the EU effort to make a directive on privacy and data protection in employment matters. This effort is an example of the first strategy, trying to translate the general principles into detailed legislation. But it did not lead to results. It covered similar matters as the ILO and CoE guidance.

In section 1.5 we present some examples of how Member States have dealt with data protection in employment matters. We end with the application of data protection in the European institutions, which is an example of the general principles-based approach.

1.1. Overview of the international and European framework

Protection of personal data is based on the fundamental right to privacy, but has evolved into a framework of rights and duties that exceeds the right to privacy and has acquired the status of an autonomous fundamental right in itself. Both rights do partially overlap, but function with a different logic.

Gutwirth and De Hert point to two distinct constitutional or legal tools to limit and control power.[13] One set of constitutional tools are opacity tools, which set limits to the interference of power in individual matters. These tools shield certain areas and prohibit the interference of power. The other set are transparency tools, which guarantee transparency and accountability of the powerful. These tools regulate and organise the exercise of power, in order for it to be legitimate.

The right to privacy can be seen as an opacity tool, while the right to protection of personal data is a transparency tool. In practice these distinctions are not absolute, because the data protection framework also contains opacity elements. But in general both rights function according to different logics, and the development of the data protection framework also meant the development of a right to protection of personal data distinct from the right to privacy.

The first legal foundations are formed by the international human rights framework, which includes the right to privacy. This right is codified in Article 8 of the European Convention on Human Rights (ECHR), which guarantees everyone “the right to respect for his private and family life, his home and his correspondence” (Art. 8 §1 ECHR), and in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which states that “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.” (Art. 17 §1 ICCPR).

When automated data processing became available in the sixties and seventies of the last century, also the awareness grew that this could lead to new infringements on privacy. This led to the development of a new framework for the protection of personal data. The first data protection laws were adopted in Sweden and Germany. As automated data processing also had international implications through increasing flow across frontiers of personal data, the Council of Europe and the OECD took the initiative to develop an international framework. The Council of Europe adopted in 1981 the first legally binding international instrument on data protection: the Convention for the Protection of Individuals with regard to Automatic Processing of Personal data (also known as Convention 108). The OECD adopted in 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
Both instruments created a new international framework for the protection of personal data, which exceeded the traditional right to privacy. They did not prohibit the processing of personal data as infringements to privacy, but were meant to regulate such processing. They had to make the transborder flow of personal data possible by creating the framework through which this could be done in a legitimate way. The data protection framework contained the means to make processing of personal data transparent and accountable through rights of information, access and rectification. These transparency tools cannot be derived from the older right to privacy.

[13] Gutwirth, S., De Hert, P., Regulating Profiling in a Democratic Constitutional State, in Hildebrandt, M. and Gutwirth, S. (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science + Business Media B.V. 2008, 271-293.

Convention 108 led to the adoption of data protection laws in several European countries. These laws were based on the principles enshrined in Convention 108, but differed widely in their implementation. The EC was confronted with the danger that these laws could block or hinder transborder flows of personal data and be an obstacle for the well functioning of the internal market. This impelled the EC to undertake a harmonisation effort, which resulted in Directive 95/46/EC 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. This directive provided the general framework for the processing of personal data. It included and further developed the general principles of Convention 108, while also providing a common approach to regulation and control by the data protection authorities.
This general framework applied as such also to work-related relations, as was confirmed by the European Court of Justice in the *Österreichischer Rundfunk* decision. The Court stated that the directive 95/46 applied to employment situations in general, also those who have no direct link with the exercise of freedoms of movement. The directive was intended to ensure the free movement of personal data between Member States through the harmonisation of national provisions on the protection of individuals with regard to the processing of such data. As such it applies to work-related relations, without presupposing the existence of an actual link with free movement between Member States in every situation.[14]

This general framework was not intended to be the final word on data protection. It could be supplemented by sectoral directives with more specific rules implementing the general principles from Directive 95/46/EC. This happened in the telecommunications sector with Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. This directive was later updated by Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (also known as the E-privacy directive). Both these directives provide the actual framework of data protection applying to work-related relations.

The European Commission did launch in 2001, in the framework of the Social Policy Agenda 2000-2005, a consultation with social partners on data protection in the employment context. Aim was to establish a specific directive on the protection of personal data in employment relations. A draft directive was made, but due to other priorities it was never presented before the Commission.[15]

These directives are only applying to first pillar matters. In the third pillar data protection was covered by Council framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. As it has no direct employment-related consequences we will not further consider this framework decision.
These directives are also not applying to the European institutions themselves. To guarantee the protection of personal data also on this level first the necessary legal base had to be created, which was provided through the insertion of Article 286 into the EC treaty by the Amsterdam treaty. This article gave the EC the competence to lay down data

[14] ECJ, Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk, Judgement of 20 May 2003, joined cases C-465/00, C-138/01 and C-139/01; De Hert, P. and Gutwirth, S., Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, in eds. Gutwirth S., Poullet, Y., De Hert, P., Nouwt, J., & De Terwangne, C., *Reinventing data protection?*,Springer, 2009, 29-31.

[15] Interview Dimitrios Dimitriou, DG Employment, 12 February 2013.

protection rules for the European institutions and to set up a supervisory body. Both are implemented by Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. The processing of employment-related personal data by the European institutions is covered by this regulation. Further consideration we leave for a later chapter.

The adoption of the Charter of Fundamental Rights of the European Union at the Nice Summit in 2000 confirmed the development of a distinct fundamental right to the protection of personal data. This Charter contains both the right to privacy in Article 7 and the right to the protection of personal data in Article 8.
The right to privacy is formulated in a similar manner as the earlier human rights treaties:

> Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 formulates the right to protection of personal data as:

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.

§2 contains the basic principles for legitimate processing of personal data and states the right to access and the right to rectification, §3 guarantees independent supervision. This formulation is a clear expression of the extra transparency tools developed in the data protection framework, which exceed the right to privacy.

In the following parts we will look into the more substantive details of the general data protection framework in Directive 95/46/EC.

1.2. The general principles of data protection

1.2.1. The protection of personal data as a fundamental right

The data protection framework inherited the basic fundamental rights approach from the right to privacy. It consists of general principles which can be applied in a variety of circumstances and contexts. The fact that the right to protection of personal data has become a fundamental right distinct from the right to privacy does not mean both rights do not share a lot.

First we will look to some important definitions in the data protection framework and the different scope of the right to privacy and the right to protection of personal data. Next we will look at the application of both rights and compare their use of general principles.

The directive 95/46 applies to the processing of personal data. Personal data is defined as any information relating to an identified or identifiable natural person (Article 2.a). Personal data only concerns natural persons, not legal persons. An identifiable person is a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic,

cultural or social identity (Article 2.a). The trigger to the applicability of the data protection framework is the identification of a person who is related to the data. This identification, or possible identification, makes the data into personal data subjected to the data protection framework. Identification means that a person can be distinguished from others or singled out.[16] If such potential identification exists, depends on "all the means likely reasonably to be used by the controller or any other person".[17]
The directive excludes some forms of processing out of its application. First when the processing happens manually and is not a part of a filing system or intended to become such (Article 3.1). Second when it is done by a natural person in the course of a purely personal or household activity (Article 3.2).
This scope is not the same as of the right to privacy. On the one hand the right to privacy protects also against interferences which have nothing to do with processing of personal data. The right to privacy enshrined in Article 8 ECHR also includes issues which have to do with autonomy and the development and fulfilment of personality, like the possibility to develop sexual relations.[18] On the other hand, most processing of personal data can be considered as an interference with privacy according to Article 8 ECHR, but not all. The ECtHR recognises certain processing of personal data as not interfering with privacy.[19]

In the ECHR the basic mechanism is first to state the protected right and secondly to state under which conditions interferences with this right are allowed. Article 8 §2 ECHR states when interference with the right to privacy is allowed: "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."
Three principles can be deduced from this formulation.

- The **legality principle**: interferences with the protected right have to be based on a legal norm. This legal norm does not have to be a written law passed by a legislative body. It can be based on customary law or case law, The European Court of Human Rights (ECtHR) uses a qualitative criterion: the law has to be adequately accessible and the law has to be sufficiently precise. The citizen should be able to have an indication on which legal rules are applicable and these legal rules should enable the citizen to foresee the consequences of his actions.[20]
- The **finality principle**: the interference must pursue one of the listed legitimate interests.
- The **necessity principle**: the interference has to be necessary in a democratic society, which implies a double criterion. First, the **relevancy principle**, meaning that the interference has to be able or to be useful to obtain the envisaged interest. Second, the **proportionality principle**, implies a balancing of interests. The envisaged interest by the interference has to outweigh the privacy interest and the least intrusive way of interfering has to be chosen.

These principles are also present in the data protection framework. Before we look at the data protection framework a last remark has to be made on the applicability of the ECHR in

[16] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 01248/07/EN, WP 136, 20.06.2007, 13-14.

[17] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 15-17.

[18] ECtHR, decision Brüggeman and Scheuten v. Germany, 12.7.1977.

[19] De Hert P., Gutwirth S., Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, 2009, 24-26.

[20] Hendrickx, F., *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 41-43.

private relations. The human rights framework originally developed as a guarantee for citizens against public authorities. The text of Article 8 §2 ECHR speaks about interferences of public authorities. But over time the applicability of the human rights framework in private relations has been accepted before courts across Europe.[21] Although only states are brought before the ECtHR, this court also accepted the applicability of these rights in private relations and the positive obligation of states to guarantee these rights.[22] The data protection framework clearly aims as well at private relations. It develops the general principles further and makes them more usable in private relations.

Data Protection Principles	
- Legitimacy principle - Finality principle - Proportionality principle - Relevance principle	- Accuracy - Transparency - Data subject participation and control - Data security

Directive 95/46 states in Article 7 the criteria for making data processing legitimate and in Article 6 principles which the actual processing has to meet. The legality principle is expressed in Article 6.1.a, stating that personal data has to be processed fairly and lawfully. This implies that every processing of personal data has to be based on a legal norm. According to which legal norms is further specified in Article 7.
The finality principle is expressed in Article 6.1.b, stating that personal data must "be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes". This limits the collection of personal data to what is relevant for the specific purpose, as well as the use of this data to the purpose for which it was originally collected. Any further use needs to be evaluated again against Article 6 and 7. These purposes have to be decided upon before collecting the data. Which purposes are legitimate is further specified in Article 7.
The proportionality and relevance principles are expressed in Article 6.1.c, stating that the personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed". Only personal data that is useful and only the minimal amount needed may be processed. Also Article 6.1.e is an expression of these principles. When the data is not needed anymore for the purpose for which it was collected or processed, it has to be erased or kept in a form which no longer allows identification.
Depending on the national implementation a slightly different categorisation can be given of these principles.

The first legitimation given for legitimate processing by Article 7 is when the data subject has unambiguously given his consent (Article 7.a). This ground shows that data protection clearly applies to private relations. The processing can be legitimated by the freedom to contract. The applicability of this legitimation to employment relations is questionable due to the subordinate position of the employee.[23] Consent will be discussed further.
Article gives 4 other specific criteria, of which the performance of a contract (Article 7.b) or compliance with a legal obligation (Article 7.c) are the most important in employment

[21] Hendrickx, F., *Privacy en arbeidsrecht*, 1999, 20-31.

[22] ECtHR. n° 30668/96, 30671/96, 30678/96, 2 July 2002 (Wilson et all./UK); Vanwijngaerden, J., De werking van grondrechten tussen particulieren, geïllustreerd met voorbeelden, *Jura Falconis*, jg 44, 2007-2008, nr 2, p. 217-248.

[23] Article 29 Data Protection Working Party, *Opinion 8/2001 on the processing of personal data in the employment context*, WP 48, 13.9.2001, 23.

relations.[24] Employment relations are often based on a contract, and to meet the obligations in the contract the employer has to process certain personal data of the employee. Employment and social security law often impose legal obligations on the employer to disclose personal data. Processing in order to protect the vital interests of the data subject (Article 7.d) can be a legitimation in issues of safety.
This is followed by one open criterion in Article 7.f, where a wide range of legitimate interests can be brought in as long as a proportionality check is made. In all these cases the legality principle has to be fulfilled. In order to be legitimate the interests have to be lawful. In employment relations the legal norms regulating these relations can provide the legal base for these interests.

In Article 8 these principles are adapted to specific categories of sensitive data. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life is prohibited, except in a more limited set of circumstances. More limited, as there is a larger interference with private life and the proportionality test will more often lead to a negative answer.
First if the data subject has given his explicit consent (Article 8.1.a). Where consent in the general case could be implicit as long as it was unambiguously, for the sensitive data the consent has to be explicit. Member States can specify the situations in which prohibition to process this sensitive data cannot be lifted using consent. This possibility is used by several Member States in the employment context.
Most relevant in employment context is the first exception, which allows the processing if necessary for a legal obligation, but only in the context of employment law and when authorised by law. The third exception gives so-called tendency companies or ideologically motivated employers the possibility to use convictions or beliefs as criterion.
More exceptions can be made by the member states.
A specific exception exists for medical purposes if the data are handled by a medical professional subject to professional secrecy or someone with an equivalent obligation.
Data concerning offences or criminal convictions may be carried out only under the control of official authority or under adequate safeguards provided by national law. Member States also have to regulate the processing of national identification numbers or other identifiers.

Further principles can be derived specific to the data protection framework. These principles turn the data protection framework into a transparency tool.
Data quality and data security principles. The data quality principle is expressed in Article 6.1.d. The personal data has to be accurate and kept up to date. This implies that inaccurate data has to be rectified or erased. The data security principle is a consequence of the finality and necessity principles. Any person acting under the data controller or processor has a confidentiality duty, implying that he may not process the data except under instructions from the controller or if required by law (Article 16). He may not make other uses of the data. The controller must also prevent accidental loss or disclosure (Article 17).
Transparency. What happens to his personal data has to be transparent to the data subject. This implies that the data subject has the right to get from the controller information on the identity of the controller, the purposes of the processing and who receives the data (Article 10 and 11)
Data subject participation and control. This implies that the data subject has the right to know if his personal data is processed and the logic behind this processing, as well as access to the data (Art 12). It also implies that the data subject has the right to object certain

[24] Article 29 Data Protection Working Party, *Opinion 8/2001 on the processing of personal data in the employment context*, WP 48, 15.

processing of personal data (Art 14) or to demand the rectification, erasure or blocking (Article 12.b). The data subject also has the right not to be subject of decisions based on automated decision making (Article 15).
The ECtHR has derived positive obligations from the right to privacy, like the right to access and rectification, but in a weaker form as provided by the data protection framework.[25]

1.2.2. Specific application mechanisms

The data protection framework in directive 95/46 is not limited to a fundamental rights framework, but also includes safeguards and accountability mechanisms to assure the practical application of the data protection framework. It establishes supervision by an independent authority on data controllers. Several mechanisms assure this supervision, like notification or prior checking obligations. It also grants the supervisory authorities powers of investigation and intervention, and to engage in legal proceedings against violations.
In the implementation of these enforcement mechanisms the Member States are given a relative freedom. Member States have also developed other control mechanisms, like the obligation to appoint data protection officers in larger data controllers.

A second specific issue is the transfer of personal data in third countries. In general such transfer is allowed to countries having an adequate level of protection. Such adequate level is assured in the EU by the directive, but not outside the EU. A first mechanism to enable the transfer of personal data is by the assessment of the Commission of the level of protection in a third country. If the Commission finds this level adequate, such transfer is allowed. Otherwise not, with some exceptions (Article 26.1). Member States can still allow the transfer in other cases, if the data controller can provide other safeguards, like contractual clauses offering adequate protection. The commission can also approve standard contractual clauses, allowing the transfer of personal data by controllers based on these standard contractual clauses.

Lastly the directive allows sectoral specification in how to apply the data protection principles through codes of conduct.
Another mechanism for sectoral specification not mentioned in this directive are the conclusion of other directives. In practice one such directive has been approved: the e-privacy-directive for the telecommunications sector.

1.3. International regulation of data protection in work-related relations

Other international actors have made efforts to complement the general data protection framework and have given attention to data protection in employment relations. Both the Council of Europe and the International Labour Organisation (ILO) drafted instruments to guide this implementation. Because the diversity in individual and collective labour law and the political sensitivity attached to international attempts to regulate it, both limited their action to soft law instruments.

The ILO Code of practice on the protection of workers' personal data was adopted in 1996 as non-binding guidance.[26] It applied to both private and public sector, and to both manual

[25] De Hert P., Gutwirth S., Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, 19-20 & 24-29.

and automated processing (Article 4). It applies not only workers, but also applicants for work. As such it not only applies to direct employers, but also to employment agencies.[27]

Article 5 lists the general principles and specifies their role in the employment context. The legitimacy or legality principle and the relevance principle are expressed in Article 5.1: "Personal data should be processed lawfully and fairly, and only for reasons directly relevant to the employment of the worker." This makes clear that processing of personal data can only be legitimated on reasons directly connected to the employment relation. A further specification of the legitimacy principle is that workers may not waive their privacy rights (Article 5.13). In other words, consent is not a ground for legitimate processing of personal data. Another application of these principles is that the processing of personal data may not lead to unlawful discrimination (Article 5.10).
Article 5.2 states that personal data should be used only for the purposes for which they were originally collected. This expression of the finality principle is immediately nuanced by stating that when personal data is processed for other purposes the employer has to ensure that they are not used in a manner incompatible with the original purpose and that misinterpretations avoided (Article 5.3). This nuance follows from the fact that employment relations are often long-term relations and that new needs for processing can show up later.[28] A further application of the finality principle is that personal data collected in connection with technical or organisational measures to ensure the security and proper operation of automated information systems should not be used to control the behaviour of workers (Article 5.4).
The proportionality principle is expressed in Article 5.7, stating that employers should regularly assess their data processing practices in order to reduce the amount and kind of personal data collected and to improve the privacy of the workers.
Data subject participation and control is included through the prohibition of decisions based solely on automated processing of personal data (article 5.5). By consequence, evaluating worker performance cannot be based solely on electronic monitoring (Article 5.6). Data subject participation and control also has a collective dimension through a role for worker representatives. Workers and their representatives should cooperate with employers in protecting personal data and in developing policies on workers' privacy (Article 5.11) and should be kept informed of any data collection process, the rules that govern that process, and their rights (Article 5.8). This is also an application of the transparency principle.
Data security implies a confidentiality duty for everyone with access to personal data (Article 5.12). Everyone processing personal data should receive training to understand their role in the application of this code (Article 5.9). Article 7 states more generally the duty for the employers to ensure security safeguards.

Article 6 implements the data protection principles for the collection of personal data. As such it addresses most controversial issues.
An important application of the principles of transparency and data subject participation is that all personal data should be obtained from the individual worker or, when it is necessary to obtain it from third parties, he should be informed and give explicit consent (Article 6.1-6.2). The code also gives more specifications on how to deal with consent (Article 6.3-6.4).
Article 6 further specifies how to deal with categories of sensitive data. In general these should not be collected, except if the data are directly relevant to an employment decision and in conformity with national legislation (sex life, political or religious beliefs, criminal

[26] ILO, *Code of practice on the protection of workers' personal data*, 1997.

[27] Commentary on the code of practice, in ILO, *Code of practice on the protection of workers' personal data*, 11.

[28] Commentary on the code of practice, in ILO, *Code of practice on the protection of workers' personal data*, 13.

convictions) or unless obliged or allowed to do so by law or a collective agreement (trade union membership or activities). Health data can only be obtained if needed to determine whether the worker is fit for a particular employment, to fulfil the requirements of occupational health and safety or to grant social benefits and if done in accordance with legislation, medical confidentiality and the general principles of occupational health and safety (Article 6.7). The data subject cannot be sanctioned for giving inaccurate or incomplete answers when questions concerning these sensitive data are not according to these rules (Article 6.8). In other words, in these circumstances he has a right to lie.
Polygraphs, truth-verification equipment or any other similar testing procedure should not be used (Article 6.10). Genetic screening should be prohibited or limited to cases explicitly authorised by national legislation (Article 6.12). Personality and other psychological tests are only allowed according to the principles in this Code, while the worker can object (Article 6.11). Drug testing has to be done according to national law or international standards (Article 6.13).
If workers are monitored they should be informed of the modalities and the employer has to minimise the intrusion on the workers' privacy. Continuous monitoring is only allowed for the purposes of health and safety or the protection of property. Secret monitoring is only allowed if there is suspicion on reasonable grounds of criminal activity or other serious wrongdoing (Article 6.14).

Article 10 deals with the communication of personal data. This is a form of further use, and needs a separate check of its legitimacy. Therefore communication to third parties needs the worker's explicit consent, unless the communication is

a) necessary to prevent serious and imminent threat to life or health;
b) required or authorised by law;
c) necessary for the conduct of the employment relationship;
d) required for the enforcement of criminal law. (Article 10.1)

Employers from the same group or public agencies are considered third parties (Article 10.3). The finality and proportionality principles also apply in internal communication. Only authorised users should have access to personal data and only to what is needed for their task. Interconnection of files is only allowed under strict application of this code. Employers should monitor the internal flow of personal data and ensure the application of these principles (Article 10.4-10.7, 10.11).
In case of medical examinations the employers should not receive medical information, but only conclusions relevant to the employment decision. They can indicate the fitness for the job, or the kind of jobs or work conditions which are medically contra-indicated. Also communication of personal data to workers' representatives should be limited to the personal data necessary to fulfil the representatives' specific functions (Article 10.8-10.10).
When employers use employment agencies they should request these agencies to process personal data according to this Code (Article 13).

The Code further deals with the security, the use and storage of data. Only data gathered according to this Code of Practice may be stored and only for as long as needed for the specific purpose for which it was obtained, apart from some exceptions.
The Code also deals in detail with the workers' right to access and rectification.

The Code also considers collective rights (Article 12). The workers' representatives should be informed and consulted:

a) concerning the introduction or modification of automated systems that process worker's personal data;

b) before the introduction of any electronic monitoring of workers' behaviour in the workplace;
c) about the purpose, contents and the manner of administering and interpreting any questionnaires and tests concerning the personal data of the workers.
d) Negotiations concerning the processing of workers' personal data should be guided and bound by the principles in this Code. In other words, the workers' representatives cannot trade the rights of the workers away or consent to processing contrary to this Code.

The ILO Code of practice gives an extensive application of the data protection framework in employment situations. It deals with most issues, which regularly are object of discussion or conflict.

The Council of Europe also followed up its general framework in Convention 108 with several recommendations on sectoral applications. One of these recommendations considers the protection of personal data used for employment purposes.[29] Its content is briefer but quite similar to the ILO Code of Practice. The Council of Europe is working on a modernisation of Convention N° 108, which includes a reconsideration of its recommendations as well. As part of this ongoing process a study was made on the recommendation concerning employment purposes. In this study the continuing usefulness and need for more specific rules on the application of data protection in employment, and by consequence for this specific recommendation, is recognised.[30]

1.4. The draft Directive concerning the processing of workers' personal data and the protection of privacy in the employment context

We mentioned already the intention of the Commission to develop a complementary directive specifying the application of the data protection principles in the employment context. This effort did not lead to a result. But a draft was made in 2004, which we will present here as an example of the shape such a EU effort could take. Important to note is that this preliminary draft was never approved nor even presented to the Commission. As such it cannot be considered as reflecting the position of the Commission.[31] We obtained this draft through an 'access to a document'-request.

The draft directive was based on Article 137(2) EC Treaty, now Article 153(2) TFEU. This article gives the European Parliament and the Council the competence to adopt, by means of directives, minimum requirements in areas like "(b) working conditions; (c) social security and social protection of workers; … (e) the information and consultation of workers".

This draft directive has a broader scope than directive 95/46, as it also applies to "the manual processing of personal data which are easily accessible and can be used as the basis

[29] CoE, *Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data used for Employment Purposes*.

[30] Buttarelli, G., *Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes and to suggest proposals for the revision of the above-mentioned Recommendation*, November 2010, http://www.coe.int/t/dghl/standardsetting/dataprotection/T-PD%20BUR%282010%2911%20EN%20FINAL.pdf.

[31] Letter 28 February 2013 of Muriel Guin, DG Employment, Social Affairs and Inclusion; interview D. Dimitriou, DG Employment, 12 February 2013.

of a decision that produces legal effects concerning the worker or significantly affects him." (Article 2).
The employment context includes aside of the employment also the recruitment and the termination of the employment relationship. The directive applies to processing of workers' data by data controllers in the employment context. This not just includes the employer, but also employment agencies, personnel selection consultants and even representatives of workers (recital 11). Worker includes trainees, apprentices, domestic servants, job applicants and former workers (Article 3).

Article 4 specifies the principles relating to data quality. The processing of workers' personal data is limited to "purposes directly relevant to and necessary for the employment of the worker concerned". The use of personal data has to be minimised and anonymous or pseudonymous data has to be used where possible. In principle workers' personal data is collected from the individual worker to whom they relate. This principle is strengthened by the explicit prohibition in Article 10 to require a worker to use the right of access to his records in order to supply those to the employer, unless the law foresees adequate safeguards. Data collection from third parties is possible if the worker has given "unambiguous consent" and either "in accordance with national legislation" or where "necessary and appropriate for the conclusion or the performance of an employment contract". No processing is possible for the purpose of discriminating, nor when the effect leads to discrimination or to violating other fundamental rights.

Article 5 narrows the legitimation grounds in the employment context. When other legitimacy criteria are provided by the data protection directives, data controllers may not rely on the consent of the worker as the sole legitimacy criterion. In other words, at least another legitimation ground aside of consent has to be available. When consent is one of the criteria relied upon, the refusal or withdrawal of consent by the worker may not justify adverse treatment by the controller. For the processing of sensitive data consent of the worker cannot be relied upon.

The processing of sensitive data is in principle prohibited, but with tailor-made exceptions given in Article 6. Compared to Article 8 in Directive 95/46, is the list of such data augmented with sexual orientation and data concerning offences. It is further specified that data concerning offences can only be processed where necessary and appropriate with regard to the particular nature of the job. Controllers have to specify which offences, criminal convictions or security measures are relevant, and the processing is subject to a prior check by the supervisory authority. Personal data on trade union membership can be processed by the trade unions when necessary and appropriate for the purposes of these organisations, or by others for purposes related to rights and obligations as trade union members within the limits of the legislation or CBAs and if those provide adequate safeguards. Personal data on racial and ethnic origin or on religious or philosophical beliefs can only be processed with the purpose of reviewing equality of treatment and with adequate safeguards. Personal data on political opinions can only be processed when it is in the context of organisations the ethos of which is based on a political opinion.

The processing of data concerning health is prohibited except when necessary and appropriate for certain purposes like complying with occupational health and safety requirements, determining whether the worker is fit with regards to the nature of the job, complying with the obligation to provide reasonable accommodation in case of disability, … Where the health data is obtained from medical examinations, the controller only is informed of the conclusions relevant to the employment decision. Health data subject to medical

confidentiality has to be processed by a medical professional or a person subject to an equivalent obligation of secrecy (Article 7).

The processing of drug and alcohol testing data is prohibited except when necessary and appropriate for certain purposes like determining the fitness of a worker for his job without posing a risk to his own safety or to the safety of others, a voluntary rehabilitation programme provided that the worker concerned has given explicit consent, protecting the vital interests of the worker or of another person where the worker is physically or legally incapable of giving his consent, or legal claims.
Individualised tests are only possible when there is a reasonable suspicion against the specific worker of drugs or alcohol use, which poses a serious safety risk. Data from random or routine generalised testing may not be processed for determining the fitness of workers, unless there is a reasonable suspicion of such use among workers carrying out a safety-sensitive job (Article 8).

The processing of genetic data is in principle prohibited. Genetic monitoring is possible where necessary and appropriate for protecting the health of the worker having regard to the particular nature of the job and if safeguards are provided, like the explicit consent of the worker. Other genetic data may be processed when necessary and appropriate for protecting the health and safety of the worker or of others, under more stringent safeguards and conditions, including the explicit consent of the worker and prior checking by the national supervisory authority. Employers only get informed of relevant conclusions and the data itself. Genetic data also has to be processed under professional secrecy (Article 9).

These special categories of health-related data have to be kept separate from all other personal data. The organisational structure of the data controller has to take the data protection requirements into account. The tasks of persons dealing with personal data have to be specified, and for sensitive data these persons have to be minimised (Article 14).

The draft directive also regulates monitoring. Article 11 contains some general provisions. Processing of workers' personal data through routine monitoring is prohibited, except where necessary and appropriate for protecting health, safety, security or property. Personal data collected while monitoring the security, the control or the proper operation of processing systems may not be further processed. Especially not to control the behaviour or performance of individual workers, except for the investigation of serious work-related criminal offences. Secret monitoring is also prohibited except when there is reasonable suspicion of a work-related criminal offence or serious misconduct and such monitoring is necessary, appropriate and no less intrusive means are available.
Personal data obtained through automated monitoring may not be the sole basis for evaluating the workers' behaviour or performance or for taking decisions with legal effects on the employment relation or significantly affecting the worker.
The communication between workers and workers representatives or health-care professionals has to be protected.

Article 12 regulates the monitoring of workers' e-mails or internet use. Routine monitoring for the purpose of detecting unauthorised use is prohibited, except on the conditions mentioned earlier for secret monitoring. Workers' private e-mails receive the same protection as private correspondence and this protection cannot be waived through general consent of the worker. Unless a reasonable suspicion of work-related criminal offence or serious misconduct an employer may not acquire knowledge of the content of private e-mails or private files. The fact that private use of work tools was not allowed does not impact on this protection.

A procedure safeguarding the workers' rights in case of monitoring to detect unauthorised use of e-mails or internet has to be determined in consultation with the workers' representatives. The employer has to inform the worker of his policy on e-mail and internet use, on monitoring and about the procedure in case of suspicion of unauthorised use.

Workers have a right of access to their personal data. They can supplement the employers' judgemental data on them with their comments. If such data is disclosed to third parties, then also these comments have to be notified to them (Article 13).

Information and consultation with workers' involvement is foreseen before the introduction, modification or evaluation of automated systems permitting the processing of workers' personal data, technical devices for monitoring of workers or questionnaires and tests used for recruitment or during employment (Article 16).

Depending on national traditions and practice, Member States shall promote dialogue between social partners, like through monitoring of workplace practices, collective agreements, codes of conduct or exchange of experiences and good practices, and encourage them to conclude agreements concerning the protection of workers' personal data (Article 18).

As a whole this draft directive dealt with the same issues as the ILO and CoE instruments. The draft directive shows that a more detailed regulation of data protection in employment relations is feasible from a technical point of view. The reason why this draft never made it into the decision making is twofold. The second stage consultation shows that the opinions of the social partners diverged. So the logical conclusion is that political differences presented a too large hurdle. But another reason mentioned was that data protection in employment relations was nowhere high on the priority list. Neither the Commission nor the unions made data protection in employment relations a priority.

1.5. Data protection in work-related relations in the Member States

Now we will look at how this framework has been applied by the Member States, and more specifically in work-related relations. It will outline with which instruments the Member States addressed data protection in work-related relations. We do not cover the whole EU, but present examples reflecting the use at national level of the legal techniques in the harmonisation strategies presented earlier. In other words, the legal context is provided by the general principles-based approach of directive 95/46. But we look if at the national level other techniques than this general principles-based approach have been used.

As discussed, the data protection framework is in the first place a fundamental rights framework. It provides general rules which have to be applied in a diversity of contexts. These general rules can be translated in specific legislation or through social dialogue into agreements between employers and workers' organisations. In the general principles-based approach they can be applied directly by the courts or by the DPAs.

We will not look in detail to the implementations of the general framework of directive 95/46. These laws will be substituted by the upcoming GDPR. What will remain are specific applications in the labour or other contexts, as *lex specialis*, as far as they are not in contradiction with the new GDPR. Article 82 §1 gives Member States the opportunity to complement the GDPR in employment relations.

Therefore we limit our attention to the ways how Member States have dealt with the employment context.

Some Member States have limited themselves to implementing the general data protection framework provided in Directive 95/46 and the telecommunication Directive 97/66/EC, updated by 2002/58/EC.
In the **UK** the general framework is provided by the Data Protection Act from 1998. The United Kingdom regulated separately the interception of electronic communications in the Regulation of Investigatory Powers Act 2000 (RIPA). Sections 4(2) and 78(5) of RIPA enable the Secretary of State to regulate legitimate business-related interception practices. On these grounds the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 were enacted. This also applies to workplace monitoring.
The Information Commissioner's Office, the UK supervisory authority for data protection, provided guidance for the application in work-related matters by issuing the Employment Practices Data Protection code,[32] together with supplementary guidance.[33] The Data Protection Act lists as one of the duties of the Information Commissioner the preparation of codes of practice, after consultation with trade associations and other relevant groups.[34] As such the UK limited itself mostly to the soft law method, foreseen in the code of conduct provisions in directive 95/46, to provide for more specific guidelines.

Other Member States have complemented this framework with specific, more legally binding implementations for the employment context.

In **France** the general data protection framework is found in the Act n°78-17 of 6 January 1978 concerning information technologies, files and freedoms (loi n°78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978), adapted in 2004 to Directive 95/46.
This is complemented by several provisions in the labour code applying the data protection principles in the employment context. Article L1121-1 Labour Code states that no limitation to individual or collective rights and freedoms may be made except when justified by the nature of the task and proportional to the envisaged aim. This expresses the necessity and proportionality principles and limits the employers' right of instruction and control. The transparency principle is also implemented in the labour code. No information concerning a (candidate) worker may be obtained without informing him beforehand.[35] The works council has to be informed of methods and techniques used in the recruitment of workers and of automated processing used in personnel management. It also has to be informed and consulted about all methods and techniques used to control workers.[36] Also specific rules concerning information gathering during recruitment are included in the Labour Code.
On the whole France uses also a general principles-based approach, but complemented it with specific provisions widening the scope of these principles to non-automated processing of personal data and to broaden the application of the transparency principle to the workers' representation.

[32] ICO, *Employment Practices Data Protection code*, November 2011.

[33] ICO, *Employment Practices Data Protection code- supplementary guidance*, June 2005.

[34] UK, *Data Protection Act*, section 5.

[35] France, *Labour Code (Code du Travail)*, L1221-9 and L1222-4.

[36] France, *Labour Code*, L2323-32.

Belgium transposed Directive 95/46 by adapting the Act of 8 December 1992 on the protection of the privacy in relation with the processing of personal data.
This was complemented by sectoral laws concerning telecommunication, social security and public administration. These have an impact on employment relations as well. But the most specific application of data protection in employment matters is given in collective bargaining agreements (CBA). These are negotiated in the National Labour Council between the unions and employer organisations. Some of these CBAs are given the status of a legal norm of general application by the government. These CBAs only apply to the private sector. As such Belgium presents a prominent example of the social dialogue strategy.
Main CBAs related to privacy and data protection are:

- CBA n° 38 of 6 December 1983 with regard to recruitment and selection.
- CBA n° 68 of 16 June 1998 relating to the protection of the privacy of employees in relation with camera surveillance on the work floor.
- CBA n° 81 of 26 April 2002 on the protection of privacy of the employees in relation with control of electronic on-line communication.
- CBA n° 89 of 30 January 2007 on the prevention of theft by employees and exit-control: this agreement imposes specific rules to the employer relating to the control of employees when leaving the workplace. This CBA regulates important privacy issues, but has no impact on the protection of personal data as such.
- CBA n° 100 of 1 April 2009 relating to a preventive alcohol and drug policy in the company

The other end of the spectrum is given by **Finland**, where a specific act regulates data protection in employment matters. Finland implemented directive 95/45/EC and the CoE Convention 108 with the Personal Data Act of 1.6.1999. The Act on the Protection of Privacy and Data Security in Telecommunications (516/2004) implements the e-privacy directive 2002/58 EC. In employment matters the general data protection framework has been complemented by the Act on Protection of Privacy in Working Life (477/2001). This act was later substituted by the Act on Data Protection in Working Life (759/2004), which entered into force on 1st October 2004. This act applies to the private sector and comparable employment relationships under public law. The Act lays down provisions on the processing of personal data about employees, the performance of tests and examinations on employees and the related requirements, technical surveillance in the workplace, and retrieving and opening electronic mail messages addressed to the employer.
It is remarkable that, despite the widespread expressed need for specific data protection regulations in employment matters, the Finnish law is still the only in existence. As such, Finland is the only example of a successful application on national level of the first strategy of developing detailed legislation.

In other countries similar attempts have failed till now. In **Sweden** two proposals were discussed in 2002 and in 2009, but these proposals never became law. The commission set up in 2009 to look into the need for specific legislation on privacy in working life concluded that the Personal Data Act provided in general good protection, but that this protection could be strengthened by the inclusion of some provisions. It proposed the strengthening of purpose limitation. The sole use of consent as ground for processing had to be excluded. Instead other grounds are necessary as well to allow the processing. It also noted the growing practice of employers asking job applicants to deliver extracts from criminal records or social security documents. Such practices had to be prohibited and sanctioned when the employers had no right to access that information directly. On the other hand, the commission saw no problem in employers obtaining credit information from credit rating agencies, as these information was already in the public domain. It also advised to make specific legislation on medical tests. Concerning surveillance by the employer the

general Personal Data Act was considered sufficient. But a general prohibition on privacy invading measures targeting excessive surveillance, background checks or questions during recruitment was proposed. The employer would also be forced to negotiate with workers' organisations according to the Co-Determination at Work Act, before introducing surveillance and backgrounds checks.[37]

The **German** general data protection framework is formulated in the Bundesdatenschutzgesetz (BDSG). The first version was adopted in 1977, substituted by a new version in 1990 and has been regularly changed since then. This general framework is complemented by regional data protection laws regulating the protection of personal data by the regional authorities and by other specific laws, like for churches.

In Germany the need for specific rules on data protection in employment matters has been recognised since the seventies and the adoption of such rules has been repeatedly the intention of the government.[38] In 2009 a separate section on data protection in employment relations was included. Article 32 BDSG provides a separate legal ground for processing of personal data in employment matters. It allows such processing for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract. Processing for the purpose of detecting crime is also possible where there is a documented reason to believe the data subject has committed a crime while employed; the processing is necessary for the investigation and is not outweighed by the data subject's legitimate interest. This legal ground is the sole legal ground for processing of personal data for employment related purposes and cannot be substituted by the legal ground for processing for business-related purposes or others.
More controversial is if consent still can constitute a legal ground in employment matters. Article 4 BDSG allows consent as a general legitimation aside of specific legal grounds like Article 32.[39] Article 4a defines the conditions such consent has to fulfil and states that consent has to be based on the data subject's free decision. This possibility of a free decision is doubtful in unequal relationships like employment relations.[40] On the other hand, Article 32 does not exclude the possibility to legitimate processing of personal data on consent.[41]
Article 32(2) BDSG enlarges the material scope of the protection of personal data to non-automated systems.[42] The personal scope includes aside of employees a wide range of employment-like relations, such as people participating in measures to integrate them into the labour market, people comparable to employees due to their economic dependence but working without an employment contract, people employed at certified workshops for persons with a disability or doing specific voluntary engagements.[43] Also employment in the public sector is included.[44] Article 32(3) BDSG leaves the participation rights of workers'

[37] Riksdag, *Integritetsskydd i arbetslivet* (english summary), SOU 2009:44, Stockholm 2009, http://www.riksdagen.se/sv/Dokument-Lagar/Utredningar/Statens-offentliga-utredningar/Integritetsskydd-i-arbetslivet_GXB344/.

[38] Simitis, S., et al, *Bundesdatenschutzgesetz*, Baden-Baden, Nomos, 2011, 1347.

[39] Simitis, S. et al., *Bundesdatenschutzgesetz*, 416-417, 434.

[40] Simitis, S. et al., *Bundesdatenschutzgesetz*, 416-417, 440.

[41] Bundestag, *Beschlussempfehlung und Bericht zu dem Gesetzentwurf der Bundesregierung – Drucksache 16/12011 – Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften ...,* 16/13657, 01.07.2009, 20.

[42] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1352.

[43] Germany, *Federal Data Protection Act (Bundesdatenschutzgesetz BDSG)* §3(11).

[44] Germany, *Federal Data Protection Act,* §12(4).

representatives unchanged. Seen the wide personal scope this means that the collective dimension of participation varies depending on the specific status of the worker.[45]

Article 32 BDSG was seen as an interim solution towards a more in-depth regulation.[46] The German government has drafted a proposal to include in the BDSG a more developed treatment of the protection of workers' personal data.[47] This motivation given for this proposal is to create more legal certainty, as the lack of specific rules creates doubt on the practical application of data protection. This proposal has not been adopted and this will probably not happen before the elections in September 2013. Still, it is worth looking at how the German government proposed to deal with data protection in employment matters.

The government proposes a new Article 32 BDSG, which contains a detailed regulation of the collection and processing of personal data in employment relations and in the recruitment phase before an employment relation. Contrary to the existing Article 32 it sets the general legitimation by consent from Article 4 BDSG aside. In the recruitment phase it provides the legal ground for data collection and processing if needed and proportional for the purpose of determining the suitability of a candidate. During the employment relation the collection and processing of personal data is allowed if needed and proportional for the purposes of fulfilling statutory obligations, fulfilling obligations towards the worker and the use of employer's right of control. In all these cases the data has to be gathered with knowledge of the worker. More intrusive data collection is foreseen for the investigation of crimes or heavy breaches of obligations, like covert collection or automated screening of employee data. The new article also contains rules concerning medical and other aptitude tests, video-surveillance, geographic monitoring systems, biometrics and the monitoring of the use of telecommunication. We discuss the details of this proposal further.

Alternative proposals for a separate law on the protection of personal data in employment matters have been tabled by the social-democrat party SPD[48] and the Greens.[49]
The Greens point to the fact that due to the lack of specific rules the protection of personal data in employment matters is lacking. Although court decisions gives indications on practical issues, often legal uncertainty remains and the protection is lacking more where there are no unions or works councils. The proposal contains the legal grounds and principles for data collection and processing and specific rules to implement the rights of data subjects. The use of consent is limited to specific cases provided by the law and no general ground for legitimation any more. It provides for the liability of employers for violations and an obligation to inform about it. The proposal clarifies the role of data protection officers in companies. The role of the works council is enlarged and unions can represent workers before the courts. The proposal regulates health and aptitude tests, the transfer of data within a group of enterprises, specific control measures as video-surveillance, data screening, control of telecommunication, geographic monitoring systems and biometrics.
The SPD also mentions the problem of legal certainty and the growing disrespect for the protection of personal data from employees. It refers to some specific problems, like the

[45] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1352.

[46] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1347.

[47] Bundestag, *Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes*, 17/4230, 15.12.2010

[48] Bundestag, Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz – BDatG), 17/69, 25.11.2009.

[49] Bundestag, Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen, 17/4853, 22.02.2011.

forced 'consent' with data processing, especially with health data, the uncertainty about video-surveillance, problems with covert monitoring, the inadequate obligation of data minimisation and the lack of effective sanctions. The proposal has a similar content as the Green proposal. We will discuss the details of the proposals with the thematic issues.
When one of the proposals in the German political debate becomes law, then it will be the most extensive legal framework for protection of personal data in employment matters.

On the whole we can say that the general principles-based approach, combined with advice by the DPAs, is prominent in the EU. Several attempts have been made or are still pending to develop more specific legislation on data protection in employment relations. The national traditions concerning social dialogue determine the shape and involvement of social partners.

1.6. Data protection in work-related relations in the EU institutions

In this section we look into the application of data protection in work-related relations in the EU institutions. It provides an example of effective application of the general principles-based approach.

Directive 95/46 did not apply to the EU institutions. Before data protection by the EU institutions could be addressed the legal competence had to be introduced in the EC treaty, which was done by the Amsterdam treaty. Article 286 EC treaty provided that from 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data would apply to the EU institutions and that an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies had to be established. This legal ground has now been substituted by Article 16 TFEU and Article 39 EU Treaty.

Based on this legal ground Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data was adopted. This regulation is not a specific implementation of directive 95/46, but provides a general data protection framework in its own right for the EU institutions and bodies. It provides similar principles according to which data processing is possible and similar rights to the data subject. The regulation also contains provisions concerning the protection of personal data in the context of internal telecommunications networks. Also, the European Data Protection Supervisor (EDPS) is established as an independent supervisory body.

The EDPS has three roles. First, the supervision and enforcement of compliance with the data protection regulation by the EU institutions. The EDPS has several compliance tools at his disposal, ranging from raising awareness by providing advice, guidance and training, consultations, inspections, monitoring and reporting exercises to prior checks of processing operations likely to present specific risks to the rights and freedoms of data subjects and the handling of complaints. The EDPS also has a range of enforcement powers, going from advice to the ban of processing operations.

A new element compared to Directive 95/46 is the establishment of data protection officers (DPO) at each of the EU institutions and bodies. The DPOs ensure in an independent manner the internal application of the data protection regulation at their institution of body and keeps a register of the processing operations notified to him. They are the primary interlocutors with the EDPS by responding to his requests and subjecting the operations likely to present risks for prior checking.

The other tasks of the EDPS are giving advice on the data protection risks of proposals of new legislation or communications and cooperation with other data protection actors, mainly within the Article 29 WP.

The persons protected by this regulation are those whose personal data are processed by Community institutions or bodies in any context, including those that are employed by these institutions or bodies.

Persons employed by EU institutions or bodies are in general not governed by the labour law of the country where they work, but by the Staff Regulations of officials and the conditions of employment of other servants of the European Communities. The applicability of national law is limited by the privileges and immunity enjoyed by the Institutions pursuant to Article 291 EC Treaty and Protocol (No 36) on the privileges and immunities of the European Communities (1965). The application of data protection in employment matters in the EU institutions boils down to the application of Regulation 45/2001 in the context of the Staff Regulations. The data protection practice at the EU institutions can be treated as another separate application, aside from the member states.

The EDPS has developed a large body of thematic guidelines, prior check opinions and consultations, administrative measures, … which are published on www.edps.europa.eu.

We discuss some guidelines as illustration of this practice. The guidelines are non-binding but are also an authoritative interpretation of the law by the EDPS. They are developed after some practice is developed through the prior checking procedures and are meant to reflect best practice.[50]

The EDPS published guidelines for the processing of health data in the workplace by Community institutions and bodies.[51] In practice health data mainly concerns medical files at a doctor's practice or at the medical service of an EU institution and administrative documents that include personal data relating to the health status of a person.
The guidelines look at the practical application of the data protection principles, contained in Regulation (EC) No 45/2001. The guidelines treat health-related data, which fall under the general regime of processing personal data, and health data in the strict sense, which are treated as sensitive data. In both cases data the provisions in Regulation 45/2001 are almost identical to those in Directive 95/46. The legal basis for processing will mainly be found in the Staff regulations, or in the Conditions of Employment of Other Servants, (hereinafter "CEOS"), the Rules on the Secondment of National Experts to the Commission and the Rules governing the Official Traineeship Scheme or exceptionally in national law. The necessity of the processing of health-related data has to be evaluated against this purpose for each concrete case.[52]
Some concrete cases provided in the Staff Regulations are:

- pre-recruitment medical examination. The purpose is to check the fitness of the candidate but also to determine whether death or invalidity benefits should be limited during the first 5 years of service due to a pre-existing medical condition.

The EDPS warns against collecting data solely for the purpose of prevention. Based on the proportionality principle, he also calls into question the use of an HIV-test.

- Annual medical check-up. The EDPS notes lack of specification of the purpose, but accept this to be for the purpose of setting up a joint sickness insurance scheme and for preventive medicine. The EDPS also advices an evaluation of the data in

[50] Interview Peter Hustinx (EDPS), 6 February 2013.

[51] EDPS, *Guidelines concerning the processing of health data in the workplace by Community institutions and bodies*, September 2009.

[52] EDPS, *Guidelines concerning the processing of health data in the workplace by Community institutions and bodies*, September 2009, 3.

each questionnaire on medical relevance. Given the purpose of prevention, there is also, when the check-up is done by a medical practitioner of own choice, no need to communicate more than a confirmation to the institutions that the examination took place. The communication of medical results should be based on freely given and informed consent.

- Further processing. The EDPS states his opinion that further processing can only be lawful if based on an informed and freely given consent of the data subject or if the processing is necessary to protect the vital interests of the data subject.
- Medical check to verify absence because of sickness/accident. The EDPS sees no legal base for any further processing of the data collected in the medical report. He also recommends that no medical data in the strict sense is contained in the medical examination report.

The EDPS also provides recommendations on retention periods of data, internal and external transfers of data, rights of access, rectification and information.

Another important example is the **EDPS Video-surveillance Guidelines**.[53] These guidelines were developed after a broad consultation. The **Follow-up Report to the 2010 EDPS Video-Surveillance Guidelines**[54] contains a systematic analysis of the status reports from EU bodies and takes stock of the implementation of the guidelines one year after its publication. This makes it the most extensive effort in reviewing the practical application of data protection in the EU institutions.

The Guidelines focus mainly to video-surveillance for security purposes, like access control. But they also apply to video-surveillance used during internal investigations or for other purposes. What is excluded from these Guidelines (but not from the application of the data protection regulation) is video-conferencing, broadcasting and recording meetings and events, … Not only CCTV is included but any electronic equipment capable of recording images, like web-cams, infra-red cameras, … The Guidelines apply also when no recording takes place but only live monitoring.

Personal data means in the first instance here recognisable facial images. But also less visible images of people can constitute personal data as long as persons are identifiable in relation with the circumstances, other data, … Also images of objects connected to persons, like number plates, constitute personal data.

The Guidelines give advice on how to implement privacy by design when introducing video-surveillance. Data protection and privacy safeguards should be built into the design specifications of the technology as well as into the organisational practices. The Guidelines also advise carrying out an impact assessment before installing and implementing video-surveillance systems. It is also advised to plan ahead for ad hoc surveillance, if the institution contemplates using during hosting events, internal investigations, etc. Consultation with stakeholders, like the data protection officer, staff and the EDPS, and competent authorities is essential in order to identify all relevant data protection concerns. Most video-surveillance systems are subjected to prior checking by the EDPS. Sometimes consultation with local authorities and the national DPA is advisable, even when national law does not apply. The decision to use video-surveillance has to be well-documented and requires a careful assessment of needs and benefits and the impact on fundamental rights. The purpose and lawful grounds have to be made explicit. Also an assessment has to be made if less intrusive

[53] EDPS, *EDPS Video-surveillance Guidelines*, 17 March 2010.

[54] EDPS, *Follow-up Report to the 2010 EDPS Video-Surveillance Guidelines*, 13 February 2012.

methods are available. Benefits and detrimental effects have to be weighed against each other. The Guidelines deal with several purpose like security, investigative purposes and employee monitoring. Employee monitoring by video-surveillance has to be avoided, apart from exceptional cases where an overriding interest can be demonstrated. The use of web-cams, broadcasting images over internet or intranet, in most cases also pose too many risks to be justified.

The Guidelines deal with a range of aspects in order to minimise the negative impact to fundamental rights, like camera locations and viewing angles, the number of cameras, times of monitoring, resolution and image quality, monitoring on Member State territory or in third countries, dealing with images revealing special categories of data. Areas under heightened expectations of privacy should not be monitored, like individual offices, leisure areas and toilet facilities. More intrusive high-tech or intelligent video-surveillance, like linked to databases for facial recognition, or the interconnection of video-surveillance systems require an impact assessment and prior checking by the EDPS. Covert surveillance will only receive a positive opinion of the EDPS under strict conditions, like to investigate serious crime and properly authorised in accordance with the law.

The Guidelines also deal with retention periods, access to and security of the images, transfers and disclosures, information to the public on the spot and by posting the video-surveillance policy online, and the right to access by data subjects. Accountability of the institutions implies transparency and demonstration of compliance. This gets shape through the video-surveillance policy and data protection audit. Such audit should document that the video-surveillance policy complies with the Regulation and the guidelines, and that the organisation is operating in accordance with its video-surveillance policy.

The Follow-up Report is based on these policies and data protection audits and follows the structure of the Guidelines. While serious efforts were done by the participating bodies, compliance with the Guidelines was disappointing at several issues. Only 2 bodies did meet all the requirements of the on-the-spot notice. 18 of the 42 bodies did claim to have published a video-surveillance policy, but only 4 could be found online of which 3 did provide relevant information. Only 5 bodies did announce an ongoing or planned impact assessment. Data protection training was taking place in only 11 bodies.
Of the 16 bodies which provided clearly defined purposes of their video-surveillance systems, 8 did state investigative purposes. One of these foresees the temporary set-up of cameras for internal investigations, while another intends to use the footage in disciplinary proceedings in extraordinary cases. Several bodies use or intend to use for a certain extent video-surveillance for employee monitoring. 2 bodies did provide the EDPS with an impact assessment in this context. 10 bodies did explicitly exclude covert surveillance. One body has implemented covert surveillance without prior checking by the EDPS. Another body foresees the possibility of covert surveillance without prior checking with the EDPS, to avoid that investigations are compromised. Several bodies do monitor areas under heightened expectations of privacy.

Although this Follow-up report may sound disappointing at certain points, it is important to note that this is a policy in full development and the Follow-up report is part of the learning and evaluation cycle.

The thematic guidelines and other published practice show the application of the data protection framework in an employment context, without further hard law-specifications. It shows that such framework, based on general principles, does not need further hard law specifications in order to function. Mr. Hustinx also doubted the need for such hard-law

specifications in the employment context.[55] The EU institutions, with more than 40000 employees spread over the EU, can be compared to a large transnational company functioning with a harmonised data protection framework (like the upcoming GDPR). On the other hand, the EU institutions also function under a single labour law, the Staff Regulations.

[55] Interview Peter Hustinx (EDPS), 6 February 2013.

2. SPECIFIC ISSUES CONCERNING PERSONAL DATA IN WORK-RELATED RELATIONS

KEY FINDINGS

- The use of consent as legitimation for the processing of employees' personal data is controversial, as it is doubtful that such consent can indeed be freely given. We observe differences among Member States in the permitted use of consent.
- The processing of medical data also varies, but mainly due to variations in social security law and health and safety regulations. In general the application of the data protection principles seems to pose few problems in this context. More problematic is the question of whether certain intrusive tests may be applied.
- Concerning the use of genetic tests in employment relations, we note two groups of practices. On the one hand, a total prohibition. On the other hand, the use of the general framework of dealing with health data, through which the use of genetic data is limited through the application of the proportionality principle.
- Member States apply the proportionality principle in diverse ways when it comes to drug testing. Some countries are restrictive and allow only testing when there is clear suspicion; others allow more systematic screening without suspicion.
- The processing of other sensitive data shows differences, but mostly due to differences in concrete situations, like customs concerning payment of union fees. These differences are generally unproblematic. For the processing of information about criminal convictions, Member States have different applications of the relevance and necessity principles. The range of jobs where questions concerning criminal convictions are allowed varies across Member States, as well as which convictions are considered relevant.
- The data protection principles are applied very differently on monitoring and surveillance. Member States differ in which purposes they allow for certain technologies. Concerning e-mail and internet surveillance we notice similar reasoning, but differences in the actual distinction between the private and professional. Also, court practice inside a country is not always consistent either. This shows the difficulties the courts have in coming to terms with new technologies.
- In general, we conclude that the application of general principles leads to a patchwork of divergent national applications. This is often due to differences in other laws, leading to different contexts in which the general principles are applied. But we also see considerable variation in the application of the general principles as such. One such area is new technologies, where there is still much to learn regarding how to deal with them and the impact they have on social behaviour. Another area is long-standing customs and cultural traditions, such as giving information about criminal convictions.

To guide the assessment of the need for complementary rules, we look at the application of data protection with specific issues in employment relations. These issues were considered as problematic in the second stage of the consultation of social partners in preparation of the 2004 draft Directive on the protection of workers' personal data.[56] We look at the

[56] European Commission, *Second stage consultation of social partners on the protection of workers' personal data*, 2004.

application in several Member States of the general framework of directive 95/46/EC to see if the general principles-based approach leads to problems or a diverse application. In practice this mostly concerns the legitimacy principle, the proportionality and the relevancy principle. Sometimes also the application of the transparency principle is under discussion, like concerning covert surveillance.

We do not cover the whole EU for each issue, but try to present the difficulties by contrasting the solutions adopted in some countries. Specific attention is also given to solutions provided by specific legislation adopted or proposed, like in Finland or Germany.

2.1. Processing personal data: consent and general requirements

Consent as grounds for legitimate processing of personal data is controversial, because the fear that workers, being in a dependent position, will feel under pressure to 'consent'.

Directive 95/46 includes consent as a ground for legitimate processing of personal data, for the processing of sensitive data and for the transfer of personal data to a third country that does not ensure an adequate level of protection. Consent is defined in Article 2 (h) of directive 95/46 as 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.'

Consent contains two fundamental elements: it has to be a 'freely given' or an unforced choice and it has to be based on relevant knowledge and understanding or 'informed'.[57] These elements ensure that the consent expresses an act of informational self-determination. The data subject has to know to what he consents and he has to do so voluntary and without external pressure. The consent has to express the will of the data subject.

The definition of consent and the qualifiers of consent in Directive 95/46 specify how such consent, being the indication of the wishes of the data subject, can be discerned in a valid way. Consent has to be a specific indication, leaving no doubt as to what the data subject consented to. Directive 95/46 demands that consent is unambiguous in order to be a ground for legitimate processing or for the transfer of personal data to a third country. Unambiguous means that the indication may not leave doubt concerning the wishes of the data subject, but it can be implied in another act. Silence or no expression of the will cannot be considered as consent. Some positive act expressing the will of the data subject is necessary.[58] Also the Article 29 Working Party states that it is questionable whether the absence of any behaviour could also be interpreted as an indication, even in very specific, unambiguous circumstances. The notion of indication seems to imply a need for action.[59]
For the processing of sensitive data explicit consent is needed, leaving even less space for misinterpretation of the will of the data subject. In this case consent cannot be implied in another act.

[57] Kosta, E., *Unravelling consent in European data protection legislation*, KU Leuven doctoral thesis, 2011, 134.

[58] Kosta, E., *Unravelling consent in European data protection legislation*, 147-148.

[59] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, WP 187, 13.7.2011, 12.

Consent is one of the main means for legitimising the processing of personal data. But the imbalance of power in the employment relation raises the question if consent to the processing of personal data can be freely given.

The Article 29 Working Party dealt with the question of consent in employment relations at several occasions. It uses as criterion for 'freely given' and thus valid consent, that the data subject must be able to refuse or withdraw consent without prejudice. The consent is not valid if there is a real or potential relevant prejudice linked to not consenting. It states that reliance on consent as ground for legitimate processing should be confined to cases where the worker has a genuine free choice and is able to withdraw consent without detriment.[60] This does limit but not totally exclude the use of consent in employment relations.[61]

The same reasoning applies in several other occasions outside employment relations, and for the use of consent as ground for legitimate processing of sensitive data[62] and the transfer of personal data to a third country that does not ensure an adequate level of protection.[63]

The notion of consent has been implemented in different ways in the Member States. The European Commission notes that consent is 'currently interpreted differently in Member States, ranging from a general requirement of written consent to the acceptance of implicit consent'.[64] The application in employment relations is by consequence also divergent.

The **Finnish** Act on the Protection of Privacy in Working Life leaves no space for using consent as a general ground for processing personal data in employment relations. It states that “No exceptions can be made to the necessity requirement, even with the employee’s consent”.[65] It provides consent as a ground for legitimate processing in specific cases, like in order to obtain personal data from a third party, medical tests on the employees demand, personality and aptitude tests, to another person opening his e-mails in his absence, … In all these cases consent is an extra condition, above the requirement that the processing is necessary for the employment relationship.

In some countries the use of consent as general ground for legitimate processing of personal data is not excluded. **Belgium** used the possibility to limit the use of consent as ground for processing of sensitive data, and excluded the use of consent in employment relations or when the data subject is in a dependent position of the data controller. This prohibition is lifted again when the purpose is to give the employee an advantage.[66]

---

60 Article 29 Data Protection Working Party, *Opinion 8/2001 on the processing of personal data in the employment context*, WP 48, 23 ; Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, WP 187 , 13-14.

61 Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, WP 187, 14.

62 Article 29 Data Protection Working Party, *Working document on the processing of personal data relating to health in electronic health records*, WP 131, 17.2.2007, 8-9.

63 Article 29 Data Protection Working Party, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, WP 114, 15.11.2005, 11.

64 European Commission, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on a comprehensive approach on personal data protection in the European Union*, COM(2010) 609, 4.11.2010, 8.

65 Finland, *Act on the Protection of Privacy in Working Life* (759/2004), section 3(2).

66 Belgium, Royal Decree of February 13, 2001 for the implementation of the law of December 8, 1992 on the protection of privacy with regard to the processing of personal data, art 27.

In other countries consent is available as ground for legitimate processing. **France** and the **Netherlands** have implemented quite literally the different uses of consent in directive 95/46.

In **Germany** Article 4 BDSG allows consent as a general legitimation aside of specific legal grounds like Article 32 for processing in employment relations.[67] This does not mean that in case of refusing to give consent, Article 32 can be used to legitimate the processing. Consent only plays a role when there are several possibilities to legitimate processing and the data processors are willing to respect the refusal of the data subject.[68]
On the contrary, all 3 new proposals concerning data protection in employment matters limit the use of consent. The government proposal,[69] introducing a new Article 32 regulating processing of personal data in employment relations into the BDSG, sets aside Article 4 and allows only consent when foreseen specifically in the new Article 32. Consent is needed to obtain personal data from third parties, for medical and other tests, for using data from job applicants after a decision has been made, etc. In other words, the use of consent does not disappear but is limited to a range of specific situations.
Also in the proposals from the SPD[70] and the Greens[71] the use of consent is limited to specific cases provided by the law, like for the transfer of data to third parties, and no general ground for legitimation any more.

Regulation (EC) No 45/2001, the data protection framework applying to the EU institutions and bodies, provides the use of consent in the 3 same cases as directive 95/46: as a ground for legitimate processing of personal data, for the processing of sensitive data and for the transfer of personal data to a third country that does not ensure an adequate level of protection. In his guidelines on the processing of health data the EDPS refers to the Article 29 WP and states that a possibility to refuse his/her consent has to be available in order to use consent as ground for legitimate processing.[72]

Data protection authorities and courts have also applied this reasoning to prohibit the use of personal data in employment relations based on consent. The **Dutch** DPA prohibited an enterprise controlling sick leave of employees for other employers to collect health data which could only be legitimated by consent.[73] The **Polish** Supreme Administrative Court doubted that due to the imbalance in the employment relation consent was freely given to collect biometric data (fingerprints) for access control and control of working hours. It considered this data collection disproportionate and refused to accept consent as legitimation.[74]

---

67 Simitis, S. et al., *Bundesdatenschutzgesetz*, 416-417, 434.

68 Simitis, S. et al., *Bundesdatenschutzgesetz*, 416.

69 Bundestag, *Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes*, 17/4230.

70 Bundestag, *Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz – BDatG)*, 17/69.

71 Bundestag, *Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen*, 17/4853.

72 EDPS, *Guidelines concerning the processing of health data in the workplace by Community institutions and bodies*, September 2009.

73 CBP, *Definitieve bevindingen in het ambtshalve onderzoek naar Verzuimreductie naar aanleiding van 'De Verzuimpolitie' van Zembla*, 3.7.2012, http://www.cbpweb.nl/downloads_pb/pb_20120711-verzuimreductie-medische-gegevens.pdf.

74 Supreme Administrative Court (Poland), I OSK 249/09, 1.12.2009.

To avoid the use of consent as ground for legitimate processing in case where it is in doubt that such consent is freely given, further limiting or specification of its use can be an option. The draft directive from 2004, excluded consent as legitimacy criterion for the processing of sensitive data and obliged for other data that consent could not be the sole legitimacy criterion.[75]

The proposed General Data Protection Regulation (GDPR) provides that 'Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller'.[76] Recital 34 mentions employment relations as an example of such imbalances. DG JUST points out that this does not exclude consent as a ground for legitimate processing in employment relations, but it is dependent on the individual case. The individual case has to be assessed to see if an imbalance is present which makes a free consent doubtful.[77]

Given the fact that the too wide use of consent is not only a problem in employment relations, a limitation or specification in the general framework is probably more preferable than a specific limitation for employment situations. DG JUST stressed that the provisions on consent of the GDPR are not more limiting or strict, but in continuity with the free consent of directive 95/84. It is only a clarification of the current system in line with the interpretation of the data protection supervising authorities.[78]

BUSINESSEUROPE and the German employers federation BDA do not agree with the reading of DG JUST. They read in the text of Article 7.4 and recital 34 of the GDPR a blanket exclusion of consent in imbalanced relations, not leaving a space for assessment of the individual case. This comes down to the exclusion of consent as ground for legitimate processing in employment relations.[79]

The EP Employment Committee tries to remedy the exclusion of consent by adding that in an employment context consent can still be used for data processing 'intended to have primarily legally or financially advantageous consequences for the employee'.[80]
BUSINESSEUROPE and BDA still have their doubts with this solution, because they consider that it does not provide sufficient legal certainty.[81] This can be illustrated with an example. A collective agreement can only differ from the law if it is in favour of the employee. But what if the agreement at company level allows the personal use of E-mail and internet and

---

[75] DG Justice, draft *Directive concerning the processing of workers' personal data and the protection of privacy in the employment context*, 2004, article 5.

[76] European Commission, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM/2012/011 final, 25.01.2012, article 7.4.

[77] Interview Marie-Helene Boulanger and Thomas Zerdick, DG JUST, 6 February 2013.

[78] Interview Marie-Helene Boulanger and Thomas Zerdick, DG JUST, 6 February 2013.

[79] European Parliament, *Opinion of the Committee on Employment and Social Affairs for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 4.3.2013, amendment 1 of recital 34 and amendment 24 of article 82 §1.f.

[80] BDA, *Appropriate modernisation of European data protection. Position on the draft European regulation 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")*, 15.5.2012, 3 ; BUSINESSEUROPE, letter of 20.2.2013 by M. BEYRER to members EMPL and LIBE Committee, http://www.businesseurope.eu/DocShareNoFrame/docs/2/HMPICOBDEHCHLONLHPPHHAIBPDW69DBYCN9LTE4Q/UNICE/docs/DLS/2013-00186-E.pdf.

[81] BUSINESSEUROPE, letter of 20.2.2013 by M. BEYRER to members EMPL and LIBE Committee ; interview Eva Barlage-Melber (BDA), Magdalena Bober, Cecilia Zappalà (BUSINESSEUROPE) 18.3.2013.

allows control of the employer on this use. Allowing personal use can be seen as in favour, but not more control.
We can conclude that the possibility to use consent as a ground for legitimate processing varies in the Member States. The solution proposed in the GDPR would effectively harmonise the use of consent.

2.2. Medical data

Medical data is one of the special categories of data, for which the grounds of legitimate processing are much more restricted. Processing of medical data is in principle prohibited due to the risks for privacy and discrimination. Also here exceptions exist, like if 'processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorised by national law providing for adequate safeguards',[82] which can be linked to legitimate concerns like fitness due to particular requirements for an employment, occupational health and safety or to determine entitlement for social benefits. Also is processing allowed when 'required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services'.[83] This relates to health care in general, but also to occupational health. Aside of expressing which purpose are legitimate, these articles also stress the necessity principle.

In employment relations the processing of medical data mostly happens during recruitment and to monitor workers' health and continuing fitness for the job. We have to distinguish between occupational health, which has a preventive task to assure that the worker's health does not get negatively affected by the work, and the evaluation of health aspects for selection purposes, which is mainly in the employer's interest. As such fitness has several aspects. First, is the worker capable in doing the job from a medical viewpoint. Secondly, to prevent occupational disease or injury. Thirdly, to protect others by ensuring that the worker does not constitute a hazard. This last aspect also concerns public health, for example in the food industry. Processing of health data also happens for social security reasons, like sick pay or advantages in case of disabilities.

Questions posed during job interviews do not always fall within the scope of data protection law, as they are not always processed by automated means or in a filing system, but are clearly related to privacy. Some countries have included specific rules in their labour laws (ex. France), made laws on the use of health information in employment context (Denmark[84]), have laws on medical examinations (ex. Netherlands,[85] Belgium) or enlarged the scope of data protection to the processing of personal data by non-automated means (Finland, Germany).
Questions concerning medical issues during job interviews have also been treated from the viewpoint of anti-discrimination law. Questions concerning pregnancy can lead to discrimination based on sex and are not allowed. In the case of Habermann the ECJ did not accept a dismissal based on the fact that the work was prohibited for pregnant women, given that pregnancy is only temporary and the employment contract was for an indefinite

[82] Directive 95/46/EC of the European Parliament and 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, article 8.2(b).

[83] Directive 95/46/EC of the European Parliament and 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, article 8.3.

[84] Denmark, Act No. 286 of 24 April 1996 on the Use of Health Information on the Labour Market.

[85] Belgium, Law on Medical Examinations (Wet van 5 juli 1997, houdende regels tot versterking van de rechtspositie van hen die een medische keuring ondergaan (Wet op de medische keuringen)).

period.[86] The case Webb concerned a replacement for someone on pregnancy leave, but who also got a contract for an indefinite period. Also in this case the ECJ considered the dismissal being a discrimination on grounds of sex.[87]

In **Belgium** the general data protection act provides the exceptional situations when it is not prohibited to process medical data.[88] The processing is allowed, among other reasons, when needed to fulfil specific obligations of the processor in the field of employment law, or needed for social security or public health, or for preventive health care. Written consent also lifts the prohibition, but the government can limit this possibility and has done so in employment matters, with the exception if the processing delivers an advantage to the worker.[89] In general the processing of medical data has to take place under supervision of a medical professional and have to be collected from the person himself, except when the data subject has given written consent or when needed to prevent an urgent danger or crime.

Medical examinations can take place for three purposes: monitoring of occupational health, control of sick leave and recruitment. During sick leave the employer has the right to send a physician to check the inability to work of the employee. This physician may only state his conclusion on the fitness to work of the employee and the possible duration of his inability. Other conclusions are subjected to his professional secrecy.[90]

The legal framework for monitoring of occupational health and selection in the private sector is given by the Act on the well-being of workers[91] and more specifically by the Royal Decree on health monitoring.[92] This Royal Decree foresees obligatory medical examinations for certain categories of workers and gives access to voluntary medical examinations for other workers, with the aim of preventing of risks. The employer is not allowed to ask medical examinations to (candidate) workers during the employment relation or for recruitment, other than for the purpose of examining a worker's fitness and those allowed in this Royal Decree.[93] The Act of 28 January 2003 on medical examinations performed in the framework of work relations[94] gives more specifications on the allowed medical examinations and tests, and applies to both private and public sector. It only allows biological tests, medical examinations and verbal information gathering concerning the health situation of a candidate worker at that moment for the purpose of examining the current fitness for a job. The use of genetic tests or AIDS-tests is prohibited, also for this examination of a worker's fitness. The government can indicate exceptional situations in

86 ECJ, Habermann-Beltermann/Arbeiterwohlfahrt (C-421/92), 5.5.1994.

87 ECJ, Webb/EMO Air Cargo (C-32/93), 14.7.1994.

88 Belgium, Act of December 8, 1992 for the protection of privacy with regard to the processing of personal data (Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens), article 7§2.

89 Belgium, Royal Decree of February 13, 2001 for the implementation of the law of December 8, 1992 on the protection of privacy with regard to the processing of personal data, article 27.

90 Belgium, Act on Employment Contracts (Arbeidsovereenkomstenwet), 3.7.1978, Article 31§2.

91 Belgium, Act of August 4, 1996 on the well-being of workers (Wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk).

92 Belgium, Royal Decree of 28 May 2003 on health monitoring (Koninklijk besluit van 28 mei 2003 betreffende het gezondheidstoezicht op de werknemers).

93 Belgium, Royal Decree of 28 May 2003 on health monitoring, article 14.

94 Belgium, Act of 28 January 2003 on medical examinations performed in the framework of work relations (Wet van 28 januari 2003 betreffende de medische onderzoeken die binnen het kader van de arbeidsverhoudingen worden uitgevoerd), *B.S.* 09-04-2003, 17757.

which these tests are allowed. It can also broaden this list of prohibited tests (but has not made use of this possibility yet).

Before a medical examination the worker has to be informed about which information is sought, which tests are done and why. The medical examination has to be done by an occupational health-specialist. He has to inform both the employer and employee of his conclusion on the medical fitness of the worker. This conclusion may not give any indication on the diagnosis or other information which could harm the privacy of the worker.[95] Apart from data minimisation, this also has an anti-discrimination purpose and avoids selection based on medical reason other than the fitness for the job. The employer also has to inform the worker of potential health risks connected with the job. The law on medical examinations in work relations also allows worker organisations to represent their members in legal procedures based on this law.[96]

The general data protection law gives everyone the right of access to his medical data directly or indirectly with the aid of a medical professional. The indirect access happens on demand of the data subject or the data controller.[97] The law concerning patient rights[98] provides a detailed implementation of this right of access and complements the general data protection law in important aspects like the transparency and data subject participation and control.

The Belgian courts have allowed candidate employees to lie when employers ask health information unrelated to the job or when such questions can lead to discrimination. This case law developed around cases concerning pregnancy. From the ECJ decisions on pregnancy, which concerned unlawful selection criteria, the Belgian courts deduced that also questions concerning pregnancy were unlawful.[99]

The **Finnish** Act on the Protection of Privacy in Working Life deals with health data in its section 5. It lists as legitimate purposes the payment of health-related benefits like sick pay, establishing if here is a justifiable reason for absence and the assessment of the employee's working capacity (if the employee expressly wishes this). Other laws can provide extra grounds for legitimate processing of health data. Such information has to be collected from the employee or elsewhere with his written consent.
Information on a worker's state of health may only be processed by persons who prepare, make or implement decisions concerning employment relationships on the basis of such information. The employer has to explicitly indicate the persons dealing with health data or specify the tasks that involve such processing. These persons are under a confidentiality duty. Health data needs to be stored separately from other personal data. The Act foresees one legitimate transfer of specific health data to the occupational health service, but the employee can object to such transfer.

In **Germany** the processing of medical data by the employer is based on the general legitimation of personal data processing for employment-related purposes where necessary

[95] Belgium, Royal Decree of 28 May 2003 on health monitoring, art 48-53.

[96] Belgium, Act of 28 January 2003 on medical examinations performed in the framework of work relations, art. 8.

[97] Belgium, Act of 8 December 1992 for the protection of privacy with regard to the processing of personal data, art 10§2.

[98] Belgium, Act of 22 August 2002 on Patient Rights (Wet van 22 augustus 2002 betreffende de rechten van de patiënt).

[99] Hendrickx, F., *Privacy en arbeidsrecht*, 1999, 136.

for carrying out the employment contract.[100] The processing of medical data through medical examinations, psychological tests or questions concerning health during job interviews have to be necessary for employment-related purposes or for carrying out the employment contract. Also consent is a possible ground for legitimate processing, if it explicitly refers to the sensitive data to be processed.[101] A medical examination is in specific cases also a legal obligation.[102] The necessity of certain medical examinations has to be judged in relation to the specific employment for which the fitness is tested. The specific employment limits the scope of medical examinations or questions. Neither the diagnosis nor the medical history may be transmitted to the employer. The physician may only transmit a conclusion on the fitness of the job applicant.[103] Psychological tests have to be treated in a similar way.[104]

The courts have allowed candidate employees to lie when employers cross the boundaries of what are permissible questions.[105] Questions concerning the general health are not allowed. The courts did allow question concerning contagious diseases, seen the risk for other workers, or concerning addiction to alcohol or drugs, seen the negative effect this can have on the capacity of the worker, or concerning doping, seen the criminal aspects.[106] Questions concerning smoking were not allowed. Nor was a question concerning HIV-infections, except when the job entails a danger of contact with infected blood.[107]
Questions concerning medical issues during job interviews have also been treated from the viewpoint of anti-discrimination law. Questions concerning pregnancy can lead to discrimination based on sex and are not allowed. The same goes for questions about disabilities.[108] If the disability has no direct relation to the work, employers can enquire about it.[109] The right to lie concerns not the agreement of the works council to the questions asked.[110]

The right to ask questions is also limited by the agreement of the works council. The law on the works councils, in Germany the Betriebsrat, gives these councils a right of co-decision on a range of matters, including on questionnaires to or assessment criteria of (candidate) employees.[111] The individual assessment is done by the employer alone.

We can conclude that based on the general data protection framework the German courts have developed a similar application concerning medical data as in the countries where medical examinations are regulated by law.
The proposal by the German government, including in the BDSG a more developed treatment of the protection of workers' personal data, codifies the basic principles of this

[100] Germany, Federal Data Protection Act, § 32 Abs. 1.

[101] Germany, Federal Data Protection Act, § 4.

[102] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1358.

[103] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1358.

[104] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1359.

[105] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1354.

[106] LAG Sachsen, 16.09.2005, 2 Sa 318/04.

[107] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1354-1355.

[108] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1356-1357.

[109] LAG Hessen, 24.03.2010, 6/7 Sa 1373/09.

[110] BAG, 02.12.1999, 2 AZR 724/98.

[111] Germany, Works Constitution Act (Betriebsverfassungsgesetz BetrVG), §94 ; Simitis, S. et al., *Bundesdatenschutzgesetz*, 1395-1396.

case law.[112] The proposal of the SPD[113] and Greens[114] are quite similar, but both prohibit the use of medical data to make health profiles and the proposal of the Greens explicitly prohibits certain medical tests, like HIV-tests, without knowledge of the data subjects.

In general health and safety regulations provide a legal framework against which the legitimacy and necessity of medical examinations can be judged. Also the anti-discrimination legislation poses boundaries to interferences with privacy, especially in recruitment. The application of the data protection principles seems not to pose many problems in this context.

More problematic is the question if certain intrusive tests may be applied, as we will consider in the following sections. Here we find more divergence, between countries using the general framework and countries which prohibit the use of certain tests in employment relations.

2.3. Genetic testing

Genetic testing is very intrusive of the right of privacy. Not only of the tested person, but also of family members. Genetic data reveals hereditary characteristics and family links. It can reveal high risk to attract incurable diseases and touches upon the right not to know. Even when legitimate in the context of work-related relations, it can reveal a wide range of unrelated health concerns.
Genetic testing can also heighten the risk of discrimination. Article 21 of the Charter of Fundamental Rights of the European Union prohibits discrimination based on genetic features. The CoE Convention on Human rights and Biomedicine, adopted in 1997 but not yet signed by all EU member states, also prohibits such discrimination and allows the use of predictive genetic tests only for health purposes or for scientific research linked to health purposes.

The Article 29 Working Party looked into the data protection aspects of genetic data.[115] It considered the protection of genetic data as a prerequisite for ensuring equality and non-discrimination. Genetic data is clearly personal data, but it is less clear if it fits in the special categories with a more stringent regime. Genetic data could be data about health. On the other hand, genetic data revealing the hear colour is not directly health data, but it could be used to determine someone's ethnic origin. The WP 29 advises to treat genetic data as particularly sensitive data within the meaning of Article 8 (1) of Directive 95/46.
Sensitive data can only be processed for a limited range of purposes, like 'preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services'.[116] It can only be processed if it is necessary for these purposes and proportional.
Given the revealing nature of genetic data, it will be difficult to fulfil the proportionality requirement. Health care is the main legitimate purpose for their further processing. The WP 29 considered that the processing of genetic data in the field of employment should be

[112] Bundestag, *Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes*, 17/4230, §32a.

[113] Bundestag, *Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz – BDatG)*, 17/69.

[114] Bundestag, *Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen*, 17/4853.

[115] Article 29 Data Protection Working Party, *Working document on Genetic Data*, WP 91, 17.3.2004.

[116] Directive 95/46, article 8,3.

prohibited in principle. Only exceptional circumstances could legitimate such processing.[117]

Several Member States prohibit genetic testing during recruitment or during the employment relationship: **Austria,**[118] **Belgium,**[119] **Estonia,**[120] and **Finland.**[121] **France** has no explicit prohibition on genetic testing in the employment context, but implicitly prohibits it as only genetic testing for medical or research purposes is allowed.[122]

In **Germany** genetic testing in employment relations received a specific regulation in the Act on Genetic Diagnostics.[123] In general it prohibits genetic testing in employment relations. The only exception is diagnostic genetic tests in the framework of preventive occupational health examinations using gen product analysis or the analysis of proteins produced by the DNA and RNA. This only as far as necessary for the identification of genetic features which cause in connection with a specific job serious illnesses. This applies to both private and public sector.

In the **Netherlands** genetic testing is allowed, but limited by the law on medical examinations. This law prohibits medical examinations and questions which present a disproportional interference with the privacy of the person. In any case examinations where the interest of the demanding party, the employer, cannot outweigh the interest of the examined person is prohibited, including examinations aiming at finding information about diseases for which no cure is available, or whose development cannot be stopped by medical intervention.[124]

In **Denmark** no specific regulation of genetic testing exists, but genetic tests are treated according to the Act on the use of health data on the labour market.[125] This Act provides that medical examinations have to use the least radical method which will serve the purpose. This proportionality clause limits the space for genetic testing.

We can conclude that concerning the use of genetic tests in employment relations we find 2 groups of practices. On one hand a total prohibition. On the other hand the use of the general framework of dealing with health data, through which the use of genetic data is limited through application of the proportionality principle. In some countries this use of the proportionality principle gets expressed in explicit limitations.

2.4. Drug testing

Drug testing is also very intrusive to the right of privacy. Due to sampling it touches on bodily integrity. Also samples used for the test can reveal a lot more than use of drugs or

[117] Article 29 Data Protection Working Party, *Working document on Genetic Data*, WP 91, 10.

[118] Germany, Gene Technology Act (Gentechnikgesetz), article 67.

[119] Belgium, Act of 28 January 2003 on medical examinations performed in the framework of work relations, article 3§1.

[120] Estonia, Human Genes Research Act, 13.12.2000, article 26, http://www.legaltext.ee/text/en/X50010.htm.

[121] Finland, Act on the Protection of Privacy in Working Life (759/2004), section 15.

[122] France, Code Civil, article 16-10.

[123] Germany, Act on Genetic Diagnostics (Gendiagnostikgesetz – GenDG), 31.07.2009, articles 19-22.

[124] Belgium, Law on Medical Examinations, article 3.

[125] Denmark, Act No. 286 of 24 April 1996 on the Use of Health Information on the Labor Market.

alcohol. And for drug tests a person has to reveal the medication taken 3 or 4 weeks before, in order to make a good choice of test or to make a correct interpretation. This means that information on a person's medical condition unrelated to drug use potentially has to be revealed.[126]

Drug testing is the collection of a specific form of health data. Again, the aim is to evaluate a worker's fitness for the job. As said before, fitness has several aspects. Is the worker capable in doing the job? This is not only a medical question, but also an economical one. Is the worker capable to be productive enough? The other issue is the safety for others. Prevention is here less of an issue, as the tests concern an activity external to the work. This is not in contradiction with the fact that alcohol and drug testing is often made part of a broader prevention policy. The aim of the test itself is not prevention, but the prevention policy is a concretisation of a proportional approach to the problem.

The ECtHR considered that drug testing in certain circumstances can be justified under Article 8§2 ECHR.[127] It accepted that such testing pursued legitimate aims, including “public safety” and “the protection of the rights and freedoms of others”.
This leaves the question in what circumstances drug tests are possible, or how is the proportionality principle applied in practice. Can drug tests be done on a regular base without suspicion or only in case of suspicion? Can they be done in the recruitment phase? Member States have developed diverging practices on this issue.

Belgium has a restrictive policy concerning drug tests on demand of the employer. The employer is not allowed to ask medical examinations to (candidate) workers during the employment relation or for recruitment, other than for the purpose of examining a worker's fitness and those allowed in the Royal Decree on Health Monitoring.[128] The occupational health practitioner can do a urine drug test if relevant for checking the fitness for the specific function and under specific circumstances. This was detailed in an advice by the National Council of the Belgian Medical Order on investigating drug use.[129] It states that a drug test on urine is not explicitly foreseen as task of the occupational practitioner in the health and safety regulations. Evaluation of the fitness for functions which are critical for safety has first to be done by clinical examination of alertness and responsiveness. In case these methods are insufficient, the physician can do a urine test under strict conditions. Such examination has to be motivated by the risks connected to the inadequate execution of a certain task and by the results of the preliminary clinical investigation which were not conclusive concerning the fitness. In other words, such test cannot be part of the general routine, not even for safety-critical functions. The possibility of such drug test has to be explicitly stated in the labour contract and in the conditions for recruitment made available for candidate employees. This means that a potential candidate has to be informed prior to sending in his job application. Such drug test is only allowed with the informed consent. It has to be done by a certified laboratory, and in case of a positive result it has to be examined again by another certified laboratory. The employer is only informed about the fitness of the (candidate) employee, not about the reason of a negative conclusion.

[126] J. O'Sullivan, Legal and regulatory aspects of workplace drug testing, in A. Verstraete (ed.), *Workplace Drug Testing*, Pharmaceutical Press 2011, 110.

[127] ECtHR, decision Wretlund v. Sweden, 09.03.2004 ; ECtHR, decision Madsen v. Denmark, 07.11.2002.

[128] Belgium, Royal Decree of 28 May 2003 on health monitoring, article 14.

[129] National Council of the Belgian Medical Order, advice on investigating drug use (advies Opsporing van druggebruik), 20.2.1993.

A recent CBA allows employers to introduce alcohol- and drug tests in the framework of a prevention policy.[130] This policy has to regulate the availability of alcohol at the workplace or occasional parties, what to do when someone appears drunk, what tests can be taken by whom, etc. In order to develop such policy a working group with worker representatives has to be established which will produce a statement of intent. In a second phase the work regulations are adapted using the normal procedure foreseen in the law. If controls are introduced it has to be mentioned in the statement of intent. The aim of the tests is to check the fitness to work, not to get a definite answer on drug or alcohol use. Urine or blood tests are not allowed, but breath tests, psychometrical tests or testing of alertness. These tests give only an indication of possible use of alcohol or drugs and sanctions cannot be based on the results of these tests alone. These tests can only be done with the consent of the person. As such this is a limited possibility for drug tests, but it allows an employer to develop a policy of regular checks or checks on suspicion.

Finland allows employers to demand a drug test certificate during recruitment for a range of jobs where performing the work under influence of drugs would entail risks. These risks are broadly defined, from endangering life or health, environmental damage, risks to confidentiality or professional secrecy to working with minors. Such drug test certificate can also be asked to employees if the employer has justifiable cause to suspect that the employee is addicted or is working under influence of drugs.[131] This leaves no space for routine checking of employees.
A drug test certificate is a certificate issued by a health care professional and laboratory stating that the employee has been tested for the use of a drug and containing a report stating whether the employee has used drugs for non-medicinal purposes in a manner that has impaired his/her working capacity or functional capacity. The employer may only process the information contained in the drug test certificate and has to treat this as health data.

In **Germany** drug tests are treated as any other medical test. Just like other medical examinations they are based on the workplace-related ground in §32 BDSG. The valid use of medical tests has to be evaluated for the specific job, so also drug testing.[132] Routine or systematic drug tests are in general not allowed. A factual base or concrete suspicion is needed for such a test, especially when the test is as intrusive as a blood test.[133] On the other hand, a lower court did accept routine controls using urine tests.[134]
The new law proposals from the government[135] or the SPD[136] do not contain specific rules concerning drug tests. The proposal from the Greens[137] prohibits drug tests without knowledge of the worker. It allows drug tests when there is a concrete danger, in other words a suspicion of drug use which can lead to accidents or dangerous situations. It also allows such tests when the job is involved in a security function or linked with the use of

[130] National Labour Council (Belgium), *CBA n° 100 of 1 April 2009 relating to a preventive alcohol and drug policy in the company.*

[131] Finland, Act on the Protection of Privacy in Working Life (759/2004).

[132] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1358.

[133] BAG, 12.08.1999, 2 AZR 55/99.

[134] ArbG Hamburg, 01.09.2006, 27 Ca 136/06.

[135] Bundestag, *Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes*, 17/4230.

[136] Bundestag, *Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz – BDatG)*, 17/69.

[137] Bundestag, *Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen*, 17/4853.

weapons. In this case also routine checks are allowed. In both case the test can only be done with consent of the worker.

Conversely, **France** allows a much wider use of drug testing. Systematic screening for drug use by workers is not allowed. But employees having safety-critical functions can be subjected to systematic screening, also without concrete suspicion. Also candidates for such functions can be systematically screened for drugs.[138]
It is the occupational physician who is responsible for establishing the need for such screening and the development of the policy. This results in widely varying practices across enterprises.

Ireland has included in its Safety, Health and Welfare at Work Act 2005 the duty to the employee to 'ensure that he or she is not under the influence of an intoxicant to the extent that he or she is in such a state as to endanger his or her own safety, health or welfare at work or that of any other person' and the possibility for employers to 'reasonably' require employees to 'submit to any appropriate, reasonable and proportionate tests for intoxicants'.[139] Intoxicants applies to alcohol and drugs. This clause still needs regulations to bring it into force. At first glance it gives the space to introduce safety and health policies by the employer which include systematic alcohol or drug testing, at least for safety-critical functions. The Railway Safety Act 2005, which is fully in force, makes it possible to require a blood or urine sample 'at random and in circumstances that are reasonable' from a worker performing a safety critical task.[140] This makes routine drug testing without concrete suspicion possible.[141]

We can conclude that the Member States apply the proportionality principle in a diverse way when it comes to drug testing. Such diverse application can complicate the development of company policies of transnational enterprises.

2.5. Special categories of data other than medical data

In this section we look at how the data protection principles are applied on other sensitive data in the Member States and if these lead to a diversified application.
The processing of sensitive data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, sex life or criminal convictions are in general prohibited. Exceptions to this rule are provided, but also in these cases restrictions are applying based on general principles like purpose limitation, legitimacy, necessity and proportionality.
Most relevant exceptions are:

- if the data subject has given his explicit consent
- if necessary for a legal obligation, but only in the context of employment law and when authorised by law
- by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim concerning its members or persons in regular contact connected to its purposes

[138] J. O'Sullivan, Legal and regulatory aspects of workplace drug testing, 126; Ministry of Labour (France), *Circulaire 90/13 on screening of addiction in the enterprise* (Circulaire 90/13 Relative au dépistage de la toxicomanie en entreprise), 9.7.1990.

[139] Ireland, Safety, Health and Welfare at Work Act 2005 (N°10 of 2005), section 13(1)(b) and 13(1)(c).

[140] Ireland, Railway Safety Act 2005 (N°31 of 2005), section 89(1)(c).

[141] J. O'Sullivan, Legal and regulatory aspects of workplace drug testing, 121-124.

The Member States differ in how they implemented safeguards connected to the processing of sensitive data. Some states, like **Italy**, **Germany** and **France** require prior authorisation from the supervisory authorities before sensitive data can be processed. Other states, like **Belgium** or **Finland**, have avoided working with prior authorisations. In routine cases the DPAs from the first group have given blanket authorisations and require only a notification or do not require a prior authorisation when a data protection officer is present in the company or organisation. In some Member States also the consent of the data subject is needed for the processing (ex. Italy). These different implementations will disappear when the General Data Protection Regulation enters into force.

Some countries, like **Germany** or **Italy** have explicitly regulated the so-called 'Tendenzbetriebe' or organisations with a political, philosophical, religious or trade-union aim, like trade unions, political parties, churches in their data protection laws. But the practice in other Member States concerning the processing of political opinions, religious or philosophical beliefs or trade-union membership in these sorts of organisations does not seem to differ a lot. The processing can be based on the exception in directive 95/46, implemented in the national data protection laws. The specificity of these organisations leads to a different result of the relevance principle.
Also, the practice to process personal data concerning union membership by the employer in order to refund union membership fees seems in general relatively similar and unproblematic.

More differences can be found in the processing of information about criminal convictions. The Member States make different applications of the relevance and necessity principles. Some Member States allow employers a wide access to some information about criminal convictions, like **Belgium** or **Italy**. Others allow employers only to ask about criminal convictions when applying for certain jobs. The range of jobs where such questions are allowed varies across the Member States, as well as which convictions are considered relevant.
Another difference concerns the access to this information. In some Member States it is only the person concerned who can obtain the information and who delivers it to the employer. This is an application of data subject participation and control. Other Member States, like the **UK** and **Ireland**, allow the employer to directly obtain the information from the authorities.

2.6. Monitoring and surveillance

In this section we look at the application of the data protection principles on monitoring and surveillance in general and concerning specific techniques as camera surveillance and e-mail monitoring. The use of a specific monitoring technology needs a consideration of the legitimacy, relevance and proportionality principles. Also the transparency and data subject participation and control principles are concerned in issues as covert monitoring or the information to workers' councils. Again we consider if applications differ among Member States.

The issue of monitoring of workers' behaviour and correspondence has been subject of a lot of debate. Point of departure is the relation between the right of control of the employer and the right to privacy of the employee. In the employment contract the employee obligates himself to work under instructions and control of the employer. The law regulating individual labour contracts will provide the legal ground for control by the employer. By signing the labour contract the employee has consented to the right to control of the

employer. However, this is not an absolute right. The employee has not traded his right to privacy away in the employment contract. Both interests will have to be balanced. The right to privacy of the employee will be limited by the right of control of the employer, but not disappear. The national labour laws also provide notions like the mutual duty to respect (Belgium[142]), dignity (Spain), good faith (France[143]), mutual trust and confidence (UK), … which limits the employer's right to control.

This right to control of the employer has to be exercised in accordance with the data protection principles. The legitimacy of such control measures will generally be based on the necessity for the performance of the employment contract. The finality and proportionality principles will be important criteria to judge if control measures are acceptable or not.
The specific surveillance measures can often also be legitimated with other purposes then controlling the work of employees. The specific purpose can lead to different applications of the proportionality principle. In other words, when control of employees is not the aim but rather security control of goods, production processes or the functioning of electronic networks, more intrusive surveillance is allowed. Purpose limitation and avoiding of function creep or processing for other purposes will be an important concern.
As the technological possibilities for such monitoring and surveillance are growing, this debate will only increase.

2.6.1. Camera surveillance

An important distinction to make is if the camera surveillance takes places in a public place or not. Surveillance of public places is often regulated by separate laws or rules and done for different purposes. In **Belgium** camera surveillance of the workplace is excluded from the law on surveillance cameras.[144] According to this law, surveillance in real time or by recording images of public space or closed places accessible for the public is only allowed with the purpose of immediate reaction against or gathering evidence of crimes, nuisances, damage or disturbance of public order and identifying perpetrators.[145] This surveillance has to be made transparent by announcing it with a visible sign.[146] Covert use of camera surveillance is prohibited.[147]

In **Germany** camera surveillance of public places is regulated by a distinct clause in the data protection act.[148] This means that camera surveillance in public places is allowed if it is necessary for pursuing rightful interests for precisely defined purposes, like theft prevention and safety, and as long as there are no indications that the data subjects'

[142] Belgium, Act on Employment Contracts, article 16, 3.7.1978.

[143] France, Labour Code, L1222-1.

[144] Belgium, Act of 21 March 2007 to regulate the installation and use of surveillance cameras (Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's), article 3 2.°

[145] Belgium, Act of 21 March 2007 to regulate the installation and use of surveillance cameras, article 5 §4 and 6 §3.

[146] Belgium, Act of 21 March 2007 to regulate the installation and use of surveillance cameras, article 5 §3 and 6 §2.

[147] Belgium, Act of 21 March 2007 to regulate the installation and use of surveillance cameras, article 8.

[148] Germany, Federal Data Protection Act, § 6b Abs. 1 Nr. 3.

legitimate interests prevail.[149] This monitoring, and the data controller responsible for it, has to be made known with appropriate means.[150]

France also has specific clauses on camera surveillance of public places or places open to public in its Interior Security Code (Code de la sécurité intérieure).[151] Such surveillance is allowed for a range of security, safety and prevention purposes[152] and has to be approved by the perfect.[153] It has to be made transparent to the public.[154] When the camera surveillance also amounts to a processing of personal data, also the French data protection law, the law 78-17 on information systems and freedoms, applies. In this case camera surveillance also needs to be notified to the supervisory authority, the CNIL. The CNIL considers that data protection applies when 1) images are not just transmitted in real time but are registered and 2) it is possible to identify people.[155]

Camera surveillance of not for public accessible workplaces is in **Belgium** covered by the CBA 68 of 16 June 1998.[156] This CBA gives a concrete implementation of the finality, proportionality and transparency principles.[157] Camera surveillance on the work floor can only be used for one of the specific purposes: 1° security and health; 2° protection of the company goods; 3° control of the production process (control of machines, in order to evaluate their technical functioning, and/or control of employees, in order to evaluate or improve the organisation of the work); 4° control of the work performed by the employee.[158] When the purpose is the control of employees (in 3° or 4°), camera surveillance can only be temporary. For the other purposes it can be permanent.[159] When control of the employee is the purpose, his evaluation may not be solely based on data gathered through camera surveillance.[160]
The employer has to give an explicit description of the purpose.[161] Camera surveillance may not be used for other purposes and has to be relevant and not excessive.[162] The employer must provide the works council or the employees with specific information on all the aspects of the camera surveillance.[163] When the purpose is the control of the work performed by the employee, this has to be included in the internal labor regulations which are made through a specific co-decision procedure.[164] In principle the camera surveillance

[149] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1372.

[150] Germany, Federal Data Protection Act, § 6b Abs. 2.

[151] France, Interior Security Code (Code de la sécurité intérieure), articles L.223-1 till L.223-9 and articles L.251-1 till L.255-1.

[152] France, Interior Security Code, article L251-2.

[153] France, Interior Security Code, article L252-1.

[154] France, Interior Security Code, article L251-3.

[155] CNIL, Circulaire 14 September 2011, http://www.referentsurete.com/cariboost_files/CIRCULAIRE_20JORF_200214_20DU_2015_20SEP_202011_20application_20CNIL.pdf.

[156] National Labour Council (Belgium), *CBA n° 68 of 16 June 1998 relating to the protection of the privacy of employees in relation with camera surveillance on the work floor.*

[157] CBA 68, commentary on article 1.

[158] CBA 68, article 4 §1.

[159] CBA 68, article 6.

[160] CBA 68, article 4 §1 4°.

[161] CBA 68, article 4 §2.

[162] CBA 68, article 7.

[163] CBA 68, article 9 §1.

[164] CBA 68, article 9 §2.

may not have an impact on the privacy of employees. If this is anyway the case, it has to be minimised and the works council has to investigate measures with this purpose.[165]
The CBA states that covert camera surveillance is only possible according to criminal law procedures.[166]

In **Germany** camera surveillance of the workplace is based on the general legitimation of personal data processing for employment-related purposes where necessary for carrying out the employment contract.[167] Preventive surveillance of workers without concrete suspicion is not allowed. Surveillance with the purpose of detecting crime is only allowed when there is a documented reason for suspicion, the processing is necessary for the detection of the crime and the interest of the data subject does not outweigh the interest of the data controller.[168] The concrete application of this interest weighing has lead to a variety of decisions. Labour courts have refused camera surveillance when less intrusive means of control were available.[169] But they have also accepted covert camera surveillance when no better option was available.[170]
The law on work councils, in Germany the Betriebsrat, gives these councils a right of co-decision on a range of matters, including on the introduction and use of technical devices designed to monitor the behaviour or performance of the employees.[171] The introduction of camera surveillance in the workplace has to be agreed upon in the works council.[172] Similar co-decision exists in the public sector for the Personalsrat.[173]

The new law proposal from the German government[174] lists several purposes for which camera surveillance can be used, like entry control, security of goods and personnel, quality control. Control of the performance of the employee is not included in this list and by consequence camera surveillance cannot be used for this. The surveillance has to be necessary for the purpose and not disproportional to the interests of any people observed. Surveillance of spaces mainly used for private purposes, like toilets or bathrooms, are not allowed. The camera surveillance has to be made visible by a recognisable sign.
The SPD-proposal[175] gives a similar, but slightly more limited list of purposes. Data may not be used for other purposes and the camera surveillance has to be visible by a recognisable sign. Control of the performance of the employee is not allowed. Targeted surveillance of a person is allowed on condition of a suspicion based on concrete facts and such surveillance is needed and not disproportional.

---

165 CBA 68, article 8 and 10.

166 CBA 68, commentary on article 4.

167 Germany, Federal Data Protection Act, § 32 Abs. 1.

168 Germany, Federal Data Protection Act, § 32 Abs. 1; BAG, 07.10.1987, 5 AZR 116/86, http://dejure.org/1987,269; BAG, 27.03.2003, 2 AZR 51/02, http://dejure.org/2003,108; BAG, 14.12.2004, 1 ABR 34/03, http://tlmd.in/u/417; BAG, 29.06.2004, 1 ABR 21/03, http://tlmd.in/u/416; BAG, 26.08.2008, 1 ABR 16/07, http://tlmd.in/u/500; Simitis, S. et al., *Bundesdatenschutzgesetz*, 1372-1373.

169 BAG, 14.12.2004, 1 ABR 34/03; BAG, 29.06.2004, 1 ABR 21/03.

170 BAG, 27.03.2003, 2 AZR 51/02.

171 BetrVG §87 Abs.1 n°6.

172 Simitis, S. et al., *Bundesdatenschutzgesetz*, 1397.

173 BPersVG §75 Abs.3 n°17; Simitis, S. et al., *Bundesdatenschutzgesetz*, 1402-1403.

174 Bundestag, *Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes*, 17/4230.

175 Bundestag, *Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz – BDatG)*, 17/69.

The proposal from the Greens[176] prohibits the use of camera surveillance for controlling the performance of the worker or in leisure or private spaces. Camera surveillance has to be made visible by a recognisable sign. The proposal also allows camera surveillance in case of a concrete suspicion.

In **France** camera surveillance in places not accessible to public and which amounts to a processing of personal data, has to respect the data protection principles contained in the general data protection act, the law 78-17 on information systems and freedoms. In the workplace these principles get complemented by the data protection clauses in the Labour Code, like the necessity and proportionality principles in Article L1121-1 Labour Code. The courts and the supervisory authority CNIL have refused to allow camera surveillance which was unjustified by the nature of the task or not proportional to the envisaged aim.[177] Continuous video surveillance of employees is not accepted.[178] Camera surveillance in douches or toilets would also be unjustified and disproportional.[179] Images taken for other purposes may not be used for controlling the activity of employees.[180]

Comparing these three countries already shows a diversified application of the data protection principles. In Belgium camera surveillance is accepted to control workers' performance, in Germany this is forbidden. Application of proportionality seems to be similar, although the concrete consideration by the courts is case-dependent and can show quite some diversity. More diversity comes from the weight given to violations of data protection law, as we consider in the section on evidence law.

2.6.2. E-mail and internet monitoring

The employer provides computer equipment and electronic communication services to his employees and has both the right to decide on what use can be made of it and the right to control of this use. This is limited by the right to privacy of the employee, which involves the protection of communications. The employee also has a right to communication. The employer cannot prohibit all private communication. He can prohibit the use for private communication of certain telecommunication means he provides as long as certain alternatives are available.
In several cases the ECtHR made clear that private phone calls and E-mails, done during working hours and through the employers' equipment, are protected by article 8 ECHR and it considered the eavesdropping as a violation.[181] In the Halford-case the Court took into account that no previous warning was given to Ms. Halford about possible listening to her phone calls and that she therefore would have had a reasonable expectation of privacy for such calls. This implies that when a warning was given, such expectation would be much lower. In the Copland-case the Court indicated that “in certain situations” the monitoring of an employee’s telephone, e-mail or internet usage at the place of work could be lawful. This suggests that according to the ECtHR the protection of private communication at work is

[176] Bundestag, *Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen*, 17/4853.

[177] CNIL, Délibération 2012-475, 3.1.2013; CNIL, Délibération 2009-201, 16.4.2009; CNIL, Délibération 2010-112, 22.4.2010.

[178] CNIL, Délibération 2012-475, 3.1.2013; CNIL, Délibération 2009-201, 16.4.2009; CNIL, Délibération 2010-112, 22.4.2010.

[179] CNIL, *Guide pour les employeurs et les salariés,* 2011, 26.

[180] Cass. (Fr.), 10.1.2012.

[181] ECtHR, Halford v. UK, 25 June 1997; ECtHR, Amann v. Switzerland, 16/02/2000; ECtHR, Copland v. UK, 3 April 2007.

not absolute.[182] Without denying this conclusion, the WP29 makes clear that advance warning to the worker is not sufficient to justify any infringement of their data protection rights. WP29 derives 3 conclusions from the case law of the ECtHR:

- Workers have a legitimate expectation of privacy at the workplace. The right of control by the employer does not override such expectations, although the provision of proper information may reduce them.
- The general principle of secrecy of correspondence covers communications at the workplace.
- Privacy includes the right to establish and develop relationships with others. Such relationships also take place at the workplace, which puts limits to the legitimate surveillance by the employer.[183]

Communication privacy is specifically protected by the E-privacy directive 2002/58/EC.[184] The principles set out in Directive 95/46/EC were translated into specific rules for the telecommunications sector by the earlier Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. Directive 2002/58/EC replaced this directive in order to update this framework to developments in electronic communications services. This directive grants also protection to legal persons (Article 1.2). This directive concerns public communications networks (Article 3.1), non-public communications services are still regulated by Directive 95/46/EC (recital 10). But use of e-mail and internet in practice mostly passes public communication networks, also when it is provided by the employer.

It is important to differentiate between the content of communication, the traffic data generated by this data and the storage of old communication in files on computers. In all vases the general principles of the right to privacy and the right to protection of personal data apply, but the specific implementation or application can be different.

Directive 2002/58/EC protects both the confidentiality of the content of communications and the related traffic data. Interception or surveillance of communications and the related traffic data by persons other than users is prohibited, except with the consent of the users concerned or when legally authorised (Article 5.1). User is defined as any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service (Article 2.a).
Storage of communications and traffic data is allowed when necessary for the conveyance of a communication (Article 5.1) or when legally authorised and carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication (Article 5.2). Traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication (Article 6.1). Exceptions are traffic data necessary for the purposes of subscriber billing and interconnection payments (Article 6.2) and the data retention laws for criminal law and national security purposes.
The protection granted to both the content of communications and the traffic data seems at first sight to make control by the employer very difficult except with the consent of the

[182] Waterschoot, P., Bespreking van enkele arresten van het Arbeidshof te Gent in verband met het gebruik van e-mail en internet op de werkplaats en het controlerecht van de werkgever daarop, *R.W.* 2008-09, 731.

[183] Article 29 Data Protection Working Party, *Working document on the surveillance of electronic communications in the workplace*, WP 55, 29.5.2002, 8-9.

[184] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

employee. National practices show that this framework is applied in a much more nuanced manner.

In **Belgium** the criminal law penalises listening into or recording of telecommunication in which one does not participate, but only during the transmission.[185] The Act of 13 June 2005 on electronic communications implements directive 2002/58/EC and protects traffic data.[186] This Act also includes some exceptions to both prohibitions. Most relevant are consent of all participants,[187] authorisation by law or when the sole purpose is to monitor the functioning of the network and the electronic communication services.[188]
This legal framework concerning E-mail and internet monitoring is further complemented by CBA 81.[189] It is the employer who decides the use that can be made of e-mail and internet (article 1 §2). This CBA concerns only the control of electronic communication data. It stipulates for which purposes such control is possible and how the proportionality and transparency principles are applied. This means that the practical application is very dependent on the shape given to the internal policy on e-mail and internet use by the employer. The law on internal labour regulations also implies that control measures have to be explicitly included in these regulations.[190]
The employer may only control on-line communications data of his employees for the prevention of illegal activities, activities contrary to morality, or activities that may harm the dignity of another person, for the protection of the confidential information and interests of the company, for ensuring safety and proper technical functioning of the network, or for controlling the compliance with the company's ICT use regulations (Article 5). The control may not have an impact on the privacy of the employee or this has to be minimised (Article 6). A specific individualisation procedure is foreseen, through which data gathered during a control gets processed to identify the person from who the communication originated (Article 11-17). When the purpose of the control is to check compliance with the company's ICT use regulations, the employer is not entitled to immediately identify the employee who does not respect the ICT policy, but shall first launch an information campaign stating that breaches have been spotted and that upon repetition thereof, the employee(s) concerned will be identified and sanctioned. Important is that this individualisation procedures do not apply on communications data whose professional character is not contested by the employee (Article 11).
The employer installing a system to control on-line communications data has to inform the working council or the employees on all the aspects of the control (Article 7-8). Also, CBA n° 39 concerning the information and consultation on the social consequences of the introduction of new technologies stipulates that the employer has to inform beforehand about the new technology and has to engage in consultation with the workers' representatives about the social consequences of this new technology.[191]

[185] Belgium, Criminal Code, Article 314bis.

[186] Belgium, Act of 13 June 2005 on electronic communications, Article 124.

[187] Belgium, Criminal Code, Article 314bis; Belgium, Act of 13 June 2005 on electronic communications, Article 124.

[188] Belgium, Act of 13 June 2005 on electronic communications, Article 125 §1.

[189] National Labour Council (Belgium), CBA n° 81 of 26 April 2002 on the protection of privacy of the employees in relation with control of electronic on-line communication.

[190] Belgium, Act of 8 April 1965 on labour regulations (Wet van 8 april 1965 tot instelling van de arbeidsreglementen), Article 6, 2° and 5°; Hendrickx, F., *Privacy en arbeidsrecht*, 96.

[191] National Labour Council (Belgium), *CBA n° 39 of 13 December 1983 relating to information and consultation concerning the social impact of the introduction of new technologies.*

In **Germany** there is no explicit regulation of e-mail and internet monitoring by employers, although several proposals have been formulated. An important criterion is if the employer has allowed private use or not of internet or e-mail. It is the employer who, based on his right of instruction, decides on the use policy of e-mail and internet he provides.
All monitoring activities have to be based on the general ground for processing workers' personal data in §32 Abs. 1 BDSG. Exception is when the employer has allowed private communication by the employees. Then the employer becomes telecommunication service provider according to the Telekommunikationsgesetz (TKG) and the Telemediengesetz (TMG), and do apply the specific data protection rules from these laws.[192]

In case no private use of e-mail and internet has been allowed by the employer, the legitimacy of monitoring depends on the necessity criterion in §32 Abs. 1 BDSG. The employer is allowed to control the traffic data of his employees to control if they adhere to his instructions on private use.[193] The possibility to control also the content of e-mails is controversial.[194]
Surveillance with the purpose of detecting crime is only allowed when there is a documented reason for suspicion, the processing is necessary for the detection of the crime and the interest of the data subject does not outweigh the interest of the data controller. Courts have accepted that employers control the files,[195] browser cache data,[196] traffic data[197] and e-mails[198] on the workers' computer.
When the employer allows private use of internet or e-mails, he has to respect the secrecy of communication. This implies that both the content and traffic data of internet and e-mail use cannot be controlled by the employer.[199] Although, when the professional character is not contested by the employee, it can be argued that §32 Abs. 1 BDSG applies.

The Betriebsrat or works council has a right of co-decision on a range of matters, including on the introduction and use of technical devices designed to monitor the behaviour or performance of the employees.[200] Monitoring of e-mail and internet use has to be agreed upon in the works council. But the use policy itself can be decided by the employer alone.[201] Similar co-decision exists in the public sector for the Personalsrat.[202]

The new law proposals from the government[203] regulates the control of traffic data and the content of the communication when only professional use is allowed of the telecommunication means provided by the employer. The control of traffic data or of the content of E-mails is allowed for assuring the performance of the telecommunication means, paying the bills for the communication, and control of the worker's performance if

[192] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1374-1376.

[193] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1376.

[194] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1376.

[195] LAG Hamm, 4.2.2004, 9 Sa 502/03, http://openjur.de/u/102818.html.

[196] VG Münster, 25.07.2006, 5 K 1808/05, http://openjur.de/u/117124.html; ArbG Hannover, 01.12.2000, 1 Ca 504/00, http://www.verdi-wir-in-der-ba.de/pv_info_inhalt/arbg_h.pdf.

[197] ArbG Düsseldorf, 29.10.2007, 3 Ca 1455/07, https://openjur.de/u/126405.html.

[198] ArbG Frankfurt, 14.7.2004, 10256/03.

[199] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1376.

[200] BetrVG §87 Abs.1 n°6.

[201] Simitis, S. et al., *Bundesdatenschutzgesetz*, 1377.

[202] BPersVG §75 Abs.3 n°17; Simitis, S. et al., *Bundesdatenschutzgesetz*, 1402-1403.

[203] Bundestag, *Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes*, 17/4230

at random but not continuous or based on a concrete reason. Monitoring of telephone conversations without knowledge of the worker is allowed if the worker has been informed about the possibility of such controls and the other participant has consented to such control. In all these cases the control has to be necessary for the purpose and not disproportional.
The SPD[204] proposal provides that an agreement on the use of telephone, internet and E-mail can be made with the employer. In case no agreement is made, the possibility of private use is assumed. When private use of the telecommunication means is excluded, the proposal allows the control of traffic data and the content of e-mails for certain purposes, including the control of the worker's performance if at random but not continuous or based on a concrete reason. Monitoring of telephone conversations is possible if both the worker and the other participant are informed and have consented. When private use is allowed, only the control of traffic data for the assuring the performance of the telecommunication means is allowed. The proposal from the Greens[205] contains similar provisions.

In **France** e-mail and internet monitoring in the workplace is regulated by the general data protection law, the law 78-17 on information systems and freedoms. In the workplace these principles get complemented by the data protection clauses in the Labour Code, like the necessity and proportionality principles in Article L1121-1 Labour Code.
The employer has the right to decide on a policy concerning internet and e-mail use. A complete prohibition of private use is considered unrealistic and disproportional.[206] When he installs a control regime he has to inform the individual worker, to inform and consult the works council and to notify the supervisory authority CNIL.
Control of e-mails is only possible for professional e-mails. Private e-mails are covered by the secrecy of communication and violations are criminally sanctioned.[207] Originally the secrecy of private e-mails was strictly protected by the courts. The Nikon-judgment made clear this protection also continued when the employer had forbidden private use.[208] Later judgments nuanced this protection by considering every e-mail as professional which is not explicitly indicated as private.[209] It is the employee who decides on the private character, like by indicating with specific words in the subject line or storing e-mails in a personal folder. But marking professional e-mails as private is contrary to the principle of good faith, inherent in the employment contract.[210] When concrete suspicions exist an employer can get permission of a judge to check the private e-mails of his employee.[211] This formal criterion allows the control of the e-mails, but not the further use of the content if they clearly have a private character.[212] The courts also take the content of the e-mails into consideration to qualify them as private or professional when relevant for the case.[213]
Files stored on computers provided by the employer are treated accordingly. Files are considered professional, except when indicated as private, and can be opened by the

[204] Bundestag, *Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz – BDatG)*, 17/69.

[205] Bundestag, *Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen*, 17/4853.

[206] Bouchet, H., *La cybersurveillance sur les lieux de travail*, CNIL, May 2004, 23.

[207] Code pénal, articles 226-15 and 432-9.

[208] Cass. (Fr.), 2.10.2001.

[209] Cass. (Fr.), 30.5.2007.

[210] Code du Travail, L1222-1.

[211] Cass. (Fr.), 23.5.2007; Cass. (Fr.), 10.6.2008.

[212] Cass. (Fr.), 18.10.2011; Cass. (Fr.), 5.7.2011.

[213] Cass. (Fr.), 18.10.2011; Cass. (Fr.), 5.7.2011; Cass. (Fr.), 2.2.2011.

employer.[214] The same applies to USB-sticks connected to professional machines.[215] Private files can only be opened in the presence of the employee, after informing and calling him or in case of a particular event or risk.[216] Such indication as private has to be specific enough,[217] and names of directories of files or hard drives are often not accepted.[218] In these cases the courts accept checking by the employer without the presence of the employee. A password is no indication of the private character, but a security measure. This also implies that the employee has to hand over the password to the employer.[219] On the other hand, when the internal policy contains more stringent rules for opening professional e-mails, the courts uphold these more stringent rules.[220]

Another quite different approach comes from the **Hungarian** DPA, where the employer is allowed to read all outgoing mail but not the incoming. Reason is that the employee has no influence on the incoming mails, but he has over the outgoing.[221]

Again the picture arising from comparing these countries is diversified. We can notice similar reasoning in dealing with e-mail and internet surveillance, but differences in the actual distinguishing between private and professional. Also, the court practice inside a country is not always consistent either. This shows the difficulties the courts have in coming to terms with new technologies and their learning curve.
Not yet visible in case law are questions due to more flexible working behaviours, like E-mails sent from home or in private hours. This flexibility will only enlarge the difficulties for courts in distinguishing between private and professional.

2.6.3. The effect of evidence law

In **Belgium** the courts have dealt more ambiguously with covert camera surveillance by the employer. They have accepted in criminal proceedings evidence obtained from covert camera surveillance, although this method of evidence gathering was in violation of CBA 68. As such this has more to do with evidence law. The courts have softened the sanction for illegally obtained evidence, first in criminal proceedings but now also in other cases. This does not change the legal framework of camera surveillance. But it erodes the reasons for respecting it.[222] A similar evolution is seen in **Germany**, although still limited to criminal cases.[223]

2.6.4. New technologies: biometrics, GPS monitoring, social networks

Technical evolutions do not stop and new technologies come gradually into general use. Examples are:

[214] Cass. (Fr.), 18.10.2006; Cass. (Fr.), 21.10.2009.

[215] Cass. (Fr.), 12.2.2013.

[216] Cass. (Fr.), 17.5.2005.

[217] Cass. (Fr.), 21.10.2009; Cass. (Fr.), 10.5.2012.

[218] Cass. (Fr.), 4.12.2012; Cass. (Fr.), 10.5.2012.

[219] Cass. (Fr.), 18.3.2003.

[220] Cass. (Fr.), 26.6.2012.

[221] Bureau of the Inspector General for Personal Data Protection in Poland et al, *Selected data protection issues. Guide for entrepreneurs*, 39.

[222] Kéfer, F., La légalité de la preuve confrontée au droit à la vie privée du salarié, in Verdussen, M., Joassart, P., *La vie privée au travail*, Anthemis, Limal, 2011.

[223] Simitis, S. et al., *Bundesdatenschutzgesetz*.

- Biometric data gets mainly used for access control. It is intrusive as certain use like iris scanning can reveal diseases.
- GPS monitoring allows for a more precise monitoring of employees on the road. Earlier monitoring tools like tachographs are in use and even obligatory, but as such did only observe driving times and not the specific places.
- Social networks pose several problems, although they do not always fall under the scope of data protection law. Dismissal cases involving workers expressing negative opinions about their employers concern the duty for respect in the employment relation. These cases show more the fact that the border between public and private has become less clear-cut. As such these cases do not concern data protection, but clearly involve privacy. Potential data protection related discussion are employers monitoring their employees Facebook accounts, but we have not encountered those yet in case law.

These technologies and others will each time be judged based on the same principles and with use of earlier case law about similar technologies (like telephone monitoring case law was used in internet cases). Still similar does not mean the same and these technologies will present a learning process concerning the application of data protection.
Specific rules concerning employment situations cannot prevent such learning processes, but can only be the result of them. By consequence an important consideration to be made is on how to improve this learning process.

2.7. Conclusion

In general we can conclude that the application of general principles leads to a patchwork of divergent national applications. This is often due to differences in other laws, leading to different contexts in which the general principles are applied. But we also see considerable variation in the application of the general principles as such. One such area is new technologies, where there is a learning curve to be negotiated on how to deal with them and their impact on social behaviour. Another area is where differences are evident in long-standing customs, like dealing with alcohol or giving information about criminal convictions.

3. POLICY OPTIONS AND RECOMMENDATIONS

KEY FINDINGS

- This study first concludes that legal harmonisation of data protection legislation is important for the employment context. Both employers and workers have an interest in the harmonisation of data protection laws.
- A second conclusion is that the application of data protection in the employment context based on general principles leads to a patchwork of different solutions, especially when new technologies are involved.
- A third conclusion is that to develop data protection rules in employment matters, the specificity of the political process in labour issues has to be taken into account. The data protection authorities lack legitimacy in the employment context. The social partners, as legitimate actors in employment matters, have to be involved and given ownership of the process to develop rules concerning data protection in employment matters.
- An effective approach needs to present a mix of hard and soft law. Hard law can create legal certainty, while soft law allows for learning processes and trust building.
- Article 82 GDPR, including the proposed amendments, reflects the different tensions present in the debate on data protection in employment matters. The underlying tensions can only be resolved properly through a trust-building process, a political process that takes all interests into account. Such a process has to involve the social partners more directly.
- The proposed amendments to Article 82 GDPR, which include minimum standards for data protection in employment relations, reflect a wish to develop at least a minimal framework for data protection in employment relations. But they also lack coherence. On the other hand, these minimum criteria can be used as leverage to task the European Commission and the social partners to take the responsibility to develop a more coherent framework. A review of Article 82 GDPR is recommended and the Commission should be asked to substitute the minimum standards included in Article 82 with a coherent Directive on data protection in employment relations.
- The effective application of data protection on new technologies will often constitute a learning process. This justifies a consultation on a regular basis between the social partners and the DPAs at national and European level. Such consultation should create awareness of the impact of new technologies and create the necessary trust to develop common solutions.

In this chapter we look again at the four strategies and the policy options they offer. We look at the positions of the social partners and those reflected in the discussions in the European Parliament. To conclude, we evaluate the policy options and formulate some recommendations.

3.1. Competences and strategies

Data protection was taken up by the EC and now the EU for specific objectives. These objectives are reflected in the competences used. But data protection touches on several

other areas of law and cannot be considered in isolation. In practice, data protection in employment relations interferes with individual and collective labour law, while also health law, non-discrimination law, criminal and evidence law can come into play. A multi-layered approach thus has to be adopted. Harmonisation efforts have to take into account the specific nature of each of these areas.

This section will look into the EU competences used and the harmonisation strategies connected to the areas concerned. We will consider the four strategies used for harmonisation of labour law in depth, and infer the policy options specific on data protection in employment relations.

The legal base of Directive 95/46 was Article 100 EC Treaty, which allowed the Council to "adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market". Recital 3 of Directive 95/46 made clear that it had a dual aim. On the one hand, fundamental rights of individuals had to be safeguarded. But the functioning of the internal market, with free movement of goods, persons, services and capital, also required the free flow of personal data between Member States. Data protection was envisaged from an internal market perspective.

The new proposed General Data Protection Regulation has its legal base in Article 16(2) and Article 114(1) TFEU. Article 16(1) TFEU states the fundamental right that "Everyone has the right to the protection of personal data concerning them", similar to Article 8 of the Charter of Fundamental Rights. This strengthens the fundamental rights perspective. The EU can make regulating this fundamental right and translating it into a practical legal framework an objective as such.

The internal market perspective is still present in Article 114(1) TFEU, which has the same function as the earlier Article 100 EC Treaty and aims at harmonisation in the functioning of the internal market.

Article 16(2) TFEU makes clear that the European Parliament and the Council have the competence to lay down rules concerning activities that fall within the scope of Union law, and the rules relating to the free movement of such data. The scope of Union law is broader than the internal market, but still it is not a general competence. Also, the Charter only applies to Member States when they implement EU law. In any case, the perspective moves more in the direction of a fundamental rights approach.

These legal bases designate shared competences, which have to be implemented taking the principle of subsidiarity into account. Using the competence for legal harmonisation with the objective to enhance the functioning of the internal market, the EU can touch upon different areas of law. As such harmonisation does not pose a problem, when there is a clear need for legislative action above the national level.

The draft Directive of 2004 concerning the processing of workers' personal data and the protection of privacy in the employment context had a completely different legal base: Article 137(2) EC Treaty, now Article 153(2) TFEU. This is part of the social policy chapter of the treaty. This chapter has different objectives, like the promotion of employment, improved living and working conditions, proper social protection, dialogue between management and labour, etc. This chapter also designates shared competences, which have to be implemented taking the principle of subsidiarity into account.

This social policy chapter has different tools that reflect different legal strategies to harmonise labour and social security law. Four legal strategies can be discerned through the development of European social policy and labour law.[224]

The first is harmonisation through EU hard law instruments. This is the strategy traditionally used to develop the internal market. With directives and regulations the European institutions develop a relative detailed legal framework, with little space for national differences. By consequence this strategy is intrusive on the national context, which can create political hurdles. On the other hand, the more intrusive, the better the harmonisation that is achieved.

The draft Directive of 2004 is an example of this approach. Article 153(2) TFEU gives the European Parliament and the Council the competence to adopt, by means of directives, minimum requirements in areas such as "(b) working conditions; (c) social security and social protection of workers; … (e) the information and consultation of workers". This allows the adoption of an instrument with a detailed application of data protection in employment relations.

The second is European-level social dialogue, foreseen in Article 155 TFEU. This strategy was the paradoxical result of the blocked development of EU harmonisation of labour law due to unanimous decision-making and was enshrined in the EC Treaty with the Maastricht Treaty.[225]

The social partners can negotiate agreements at EU-level, which can be given legal force by the Council, if the issue is within the remits of Article 153 TFEU, or by the Member States. Article 154 foresees that the Commission consults with the social partners when it intends to submit proposals in the social policy field and later on the content of the proposal. If the social partners wish to do so, they can take over the initiative and negotiate an agreement according to Article 155 TFEU.

This strategy has not produced the results originally expected. It has been designated as 'bargaining in the shadow of the law', given the fact that the initiative or threat of the Commission to legislate was the main motivator for results.[226]

The third method is the open method of coordination. This is a soft law approach to achieve policy coordination, but avoiding binding legislation. This policy harmonisation method is foreseen in article 156 TFEU. Non-binding does not mean it cannot have a potential impact in practice. It works through research, exchange of best practices, establishment of guidelines, periodic monitoring and evaluation. The continuous dialogue and influencing should achieve a mutual learning and harmonising effect.

This method has its advocates and its critics. In practice, the EU often uses soft law where Member States are unable to agree on the use of a legally binding measure. As such, this does not discredit soft law approaches. They can function as trust-building methods.[227]

---

[224] Bercusson, B., *European Labour Law*, 2009.

[225] Bercusson, B., *European Labour Law*, 2009, 126.

[226] Bercusson, B., *European Labour Law*, 2009, 148-151 ; Smismans, S., The European Social Dialogue in the Shadow of Hierarchy, 2009, *Jnl Publ Pol*, 28, 1, 161-180.

[227] Trubek, D. Trubek, L., Hard and Soft Law in the Construction of Social Europe : the Role of the Open Method of Co-ordination, *European Law Journal*, Vol 11, N°3, May 2005, 343-363 ; Bercusson, B., *European Labour Law*, 2009, 185-187.

The fourth strategy is the strategy of fundamental rights or the constitutionalisation of labour law. The Charter of Fundamental rights, containing a wide range of social rights, is the concretisation of this strategy. Such a 'fundamental rights approach' is another way to avoid narrow and detailed harmonisation. Fundamental rights provide a flexible framework, using principles applicable in and adaptable to very diverse contexts.

Human rights scholars will object to calling this a 'fundamental rights' approach, as it presents the constitutional or treaty rules containing fundamental rights in opposition to more developed laws. Good protection of fundamental rights will need the development of detailed legal systems that makes the application of these rights accessible in practice. What is presented as a 'fundamental rights approach' is rather a reduction to generally applicable principles. We refer to the strategy of using 'general principles', as it expresses better the legal technique used in this approach.

This general principles approach is an answer to the transformation of industrial relations, which seem to follow the direction of decentralised collective bargaining, and to a context in which labour law is under pressure from globalisation and flexibilisation.[228] The erosion of centralised collective bargaining also implies the erosion of mechanisms of collective interest-building and negotiation underlying the earlier harmonisation or social dialogue strategies.

Two main responses have been given to this situation.[229] The first is to try to manage the diversity by harmonising goals instead of means. Soft law approaches like the open method of coordination are an example of this approach. The second response is the establishment of minimum requirements and conditions; a 'floor of rights'. The social rights in the Charter are an example of this approach, but also implementations like the GDPR could function as such.

These four strategies can be concretised into four main options to deal with data protection in employment relations, although mixed responses are possible as well.

- Option 1: A new Directive on the protection of personal data in the employment context
- Option 2: The social partners negotiate agreements concerning data protection through the social dialogue on European level
- Option 3: Through soft law methods the social partners and data protection authorities are involved in the development of guidelines or agreements and exchange of practices
- Option 4: No specific action is taken to complement the GDPR in employment relations.

Option 1 comes down to a renewed proposal of a Directive complementing the GDPR in employment relations. The draft of 2004 shows that it is feasible to develop a workable framework. The positive aspects of this approach are that it creates more legal clarity and harmonises further data protection EU-wide. Although most enforcement issues are best dealt with in the GDPR, it can also deal specifically with international data transfers in transnational companies, the role of workers' representatives and of European Work Councils.

[228] Hendrickx, F., The Future of Collective Labour Law in Europe, 66.

[229] Hendrickx, F., The Future of Collective Labour Law in Europe, 72.

From the perspective of a transnational company trying to develop an EU-wide data protection policy, the national patchwork problem would be resolved to a certain degree, although perhaps too restrictively from a business point of view. Still, this provides the most coherent approach.

The counter argument to this approach is that the main problem is not a technical one. From 2001 to 2003 the European Commission consulted with the social partners and presented its views on a European framework on the protection of workers' personal data. This framework was intended to be an addition to the general framework of Directive 95/46/EC. In 2004 a draft Directive was drawn up but never proposed to the European Commission. In the Social Agenda 2005-2009 the Commission again announced that it would propose an initiative concerning the protection of the personal data of workers. But this intention did not produce results either. Similarly, several attempts were made in Sweden and Germany to develop a comprehensive law on data protection in employment relations, but which somehow became stranded each time.

This gap between the intention to make legislation and the resulting outcome is not the reflection of technical difficulties linked to the application of data protection. In the first instance it reflects the difficulties connected to harmonising labour law. This is not just a question of legal technique, but of building trust.

Alongside harmonising laws, interests also have to be harmonised through social dialogue. Options 2 and 3 are such trust-building exercises.

At national level social dialogue helps to solve problems concerning the application of data protection in the workplace. A good example is the CBAs concerning data protection-related issues in Belgium, which create ownership and knowledge of data protection-issues by the social partners.

The problem with both approaches is that social dialogue at EU-level has not delivered comparable results. The social dialogue has produced agreements on telework (2002), work-related stress (2004), harassment and violence at work (2007).

If social dialogue does not result in agreements, the European Commission can still take up the issue as in option 1. In other words, the social dialogue in option 2 excludes the ordinary legislative procedure from option 1 when it is successful, but still contains it as a fallback option in case of failure.

Option 3 has the extra disadvantage that it does not solve the problem of data protection in a patchwork of national regulations. Still, soft law approaches can be useful as both a trust-building and a learning exercise. It also allows for involving other stakeholders. Regular attention of both the social partners and the DPAs to data protection in the workplace could improve common solutions to specific issues. Such soft law efforts directed at specific issues or technologies are not mutually exclusive with but rather complementary to the more general hard law initiatives.

The DPAs already produce soft law through the WP 29 and its advice. But the DPAs have limited legitimacy in the employment context. Initiating regular exchange between the social partners and the DPAs would improve the common learning process and trust-building. Even a limited initiative concerning the data protection problems connected to new technologies or scientific developments could be useful. It could monitor where

problems with divergent solutions exists and develop suggestions and guidelines for a more common approach.

Several options are available for such soft law initiatives. The social partners can take the initiative to include the Article 29 Working Party or the European Data Protection Board (its successor under the proposed GDPR) in the preparation of agreements during the social dialogue or of advice by the European Economic and Social Committee. The European Data Protection Board could also take itself the initiative to invite the social partners for consultation on advice concerning employment-related issues.

One example of development of soft law is the RFID framework. On 12 May 2009 the European Commission issued a Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (RFID). A main element in this recommendation was the development of a framework for privacy and data protection impact assessments by the industry in collaboration with civil society stakeholders, to be endorsed by the Article 29 WP. This development did not go smoothly and a first draft was refused by the Article 29 WP, but resulted in 2011 in the Privacy and Data Protection Impact Assessment Framework for RFID Applications.[230] The Recommendation itself was prepared with the contributions of an RFID expert stakeholders group, composed of more than 25 members from industry, civil society, national and European DPAs. Similar processes with broad inclusion of stakeholders could be envisaged to come to terms with new technologies in the employment context.

Option 4 assumes that the GDPR is sufficient to deal with questions raised in the employment context. Still, it runs the risk of leaving the patchwork of different national applications intact. Another problem with the general principles-based approach is that it relies on problem-solving through case law, which is an expensive method of creating legal certainty.

On the other hand, if another option is preferred to deal with data protection in the employment context, for certain issues it could be preferable to deal with them in the GDPR. Especially when employment concerns are also of concern elsewhere and a general way to deal with them is available. Examples are the discussion on consent and issues concerning enforcement and the role of DPAs.

3.2. Positions of the social partners

Both trade unions and employers' organisations agree that there is too much variation across the Member States in the implementation of data protection. The patchwork of national data protection laws creates problems, also in the employment context. Both have a different view on what is the problem and the solution, but both perspectives do point to the EU level as the appropriate level to deal with these issues.

BUSINESSEUROPE and BDA prefer one common general framework of data protection. As such they approve the option of a General Data Protection Regulation. Such a general framework would simplify the application of data protection and would allow transnational companies to develop an EU-wide company policy on data protection.

[230] Spiekermann, S., 'The RFID PIA – Developed by Industry, Endorsed by Regulators', in Wright, D. & De Hert P. (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

An extra directive on data protection in employment relations is not favoured. They prefer a general framework with principles that are flexible enough and adaptable to many contexts. Such a general framework is sufficient if the employment context has been properly taken into account. More specific aspects can be negotiated at national, sectoral and company level. A complementary directive creates too many restrictions for such negotiations. The introduction of too many specific rules concerning employment in the GDPR, like the inclusion of a list of minimal standards in Article 82§1 GDPR, creates a similar problem.[231]

The European Trade Union Confederation (ETUC) deplores the fact that the Commission does not present any proposals guaranteeing the respect of private life at the workplace in the framework of an employment relationship. It would welcome the Commission using use this renewed opportunity on the topic to prompt the social partners to negotiate on the matter.

Issues that would need to be covered are the scope of the processing of these data (also manual processing), the role of consent (limited), drug and alcohol testing, intrusions into the lifestyle of workers; monitoring workers' emails or internet use, the right of access to personal data, the exclusion of the use of any personal data collected illegally, the use of GPS-tracking devices, the prohibition of targeted monitoring and control at the workplace.
ETUC would in particular like to see a strengthening and enhancement of national data protection authorities. National authorities are often understaffed and cannot devote their scarce resources to employee-related data protection issues. It would be very helpful if the authorities were equipped with powers similar to that of labour inspections.

ETUC would also like more effective remedies and sanctions, including enforcement cross-borders. It would be a great improvement if trade unions could represent individuals and bring an action before the national courts.[232]

The German union Ver.di and the Austrian ÖGB also point to the problem of enforcement. They would like stronger DPAs and the possibility for worker representatives to represent workers in court on data protection complaints. Enforcement in an international context has to be improved as well.

A specific issue is also to treat biometric data as sensitive data.[233]

These opinions do not differ from those expressed in the consultations in 2003, where unions were in general for a new directive on employment relations, while employers' organisations did not see a need for such extra legislation.

3.3. The GDPR and employment relations

In this section we look at the proposed GDPR from the viewpoint of the strategies and policy options considered.

Several issues raised are already dealt with in the GDPR. The discussion about consent is dealt with in Article 7 of the GDPR. Also enforcement mechanisms are best dealt with in the

[231] Interview Eva Barlage-Melber (BDA), Magdalena Bober, Cecilia Zappalà (BUSINESSEUROPE) 18.3.2013.

[232] http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/etuc_en.pdf

[233] http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/verdi_de.pdf; http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/ogb_de.pdf

GDPR as they have a wider application than employment relations. The question on legal representation of workers in complaint procedures or before court by workers' representatives or unions can best be dealt with in the GDPR. Articles 73-76 of the GDPR give “any body, organisation or association which aims to protect data subjects’ rights and interests concerning the protection of their personal data” the right to lodge complaints or start court proceedings on behalf of data subjects. If this possibility is accepted, it is only logical to consider unions as such organisations in the employment context. Such interpretation can be made explicit in these articles or in the recitals concerning them.

The GDPR deals specifically with employment relations in Article 82. It reflects a mix of approaches. Article 82 §1 gives Member States the possibility to “adopt by law specific rules regulating the processing of employees' personal data in the employment context”. Member States obtain the competence to complement the GDPR, but not to deviate from it. Those specific rules have to stay 'within the limits of this Regulation'. This paragraph sees specifications of the application of data protection in the employment context not as an EU-level task. If needed, it can be done at national level. It is an expression of the view that, considering subsidiarity, the EU should leave the employment context to the national states. As such, this is a method to guard against restrictive rules in employment matters, but with the disadvantage that it leaves room for a patchwork of national rules.

Article 82 §3 gives the Commission the possibility to step in with delegated acts, at least for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data. This introduces a method of extra harmonisation into the labour context, but with exclusion of other actors like the EP, the Council or the social partners. As such, it is an expression of doubt about the option taken in Article 82 §1 and functions as an emergency procedure to act when the national patchwork creates too many problems. This raises the question of whether it is better to take the policy option to provide complementary rules for employment relations by one of the other mechanisms considered above.

The Opinion of the Employment Committee proposes amendments that include several minimum standards for processing data in the employment context into the GDPR. These amendments also show that a need is recognised to provide for rules at the EU-level.

The proposed minimum standards contain rules on processing with and without the knowledge of the employee, video-surveillance, medical examinations, surveillance of telecommunications, prohibition of blacklists, rights of worker representatives, transfers of information.

In other words, an attempt is made to turn this article into an extensive framework for data processing in employment context. On the other hand, the whole gives an incoherent and ad hoc impression. It is difficult to squeeze a coherent data protection framework into one paragraph with minimum standards. These amendments also raise the question of whether it is better to provide complementary rules for employment relations by an extra directive.

This Article 82 GDPR can be considered as reflecting the different tensions present in the debate on data protection in employment matters. §1 reflects option 4 for a general principles-based approach where the GDPR provides this general framework. Referring extra rules on employment matters to the national level is a defence against regulation that is too restrictive.

The proposed minimum standards reflect an attempt to create more specific rules, as foreseen in option 1. Also §3 leaves this option open. That this can lead to incoherent or ad hoc rules is preferred to the risk of inadequate protection of workers' personal data.

The underlying tension can only be resolved properly through a trust-building process, a political process that takes all interests into account. Such a process has to involve the social partners more directly. The European Parliament can also use the GDPR as a stepping stone to set such a process in train. The end result will have to be some sort of complementary rules, be they hard law or soft law, which provide enough protection for personal data of workers, while also not being too restrictive for employers.

3.4. Recommendations

This study concludes that legal harmonisation of data protection legislation is important for the employment context. Diverse practices concerning data protection in employment relations create a patchwork of national laws and practices. This causes problems for transnational enterprises and hinders the development of Europe-wide data protection policies inside those enterprises. Such diverse practices can also create enforcement problems when employee data gets transferred across borders. This leads to the conclusion that **both employers and workers have an interest in the harmonisation of data protection laws**.

A second conclusion is that the application of data protection in the employment context based on general principles leads to a patchwork of different solutions, especially when new technologies are involved. Technical developments create legal uncertainty for the application of data protection. Creating legal certainty through case law is an expensive and slow method. Legislative work can provide legal certainty. On the other hand, relying on flexible general principles provides a good fallback option. Soft law processes can function as learning processes on how to deal with new technologies.

A third conclusion is that to develop data protection rules in employment matters, the specificity of the political process in labour issues has to be taken into account. The data protection authorities lack legitimacy in the employment context. **The social partners, as legitimate actors in employment matters, have to be involved and given ownership** of the process to develop rules concerning data protection in employment matters.

Data protection in employment relations cannot be isolated from labour law. Effective rule-making in this area needs to include trust-building. As well as harmonising laws, interests also have to be harmonised through social dialogue. **An effective approach needs to present a mix of hard and soft law.**

Based on these conclusions, we can formulate recommendations for the European Parliament.

The proposed amendments to Article 82 GDPR reflect a wish to develop at least a minimal framework for data protection in employment relations. The need and intention to develop such a framework has been expressed over the years at different levels. **Such a framework would be a positive development if it effectively harmonises data protection in employment relations and if it is a technically well-developed framework.**

The development of such a framework can take inspiration from the ILO Code of practice on the protection of workers' personal data, from the earlier draft Directive concerning the processing of workers' personal data and the protection of privacy in the employment context and from the recent proposals in the Member States.

Several issues are better dealt with in the GDPR, as they have a wider application than employment relations. One such issue is consent; another issue is better enforcement in the employment context. **It is recommended that unions and workers' representatives are among the actors that can act on behalf of data subjects in the employment context, as foreseen in Articles 73-76 of the GDPR.**

The minimum criteria in the proposed amendments to Article 82 GDPR are far from being such a well-developed framework. Although well intended, they are a collection of ad hoc rules without much coherence. **A review of these proposals' effectiveness in practice is recommended;** substituting them with more coherent proposals.

On the other hand, the inclusion of minimum criteria expresses the wish of the European Parliament for complementary rules concerning employment relations. These minimum criteria can be used as leverage to task the European Commission and the social partners to take the responsibility to develop a more coherent framework. Another amendment foresees a review of Article 82 GDPR in two years' time. **It is recommended to foresee a review of Article 82 GDPR and to ask the Commission to substitute the minimum standards included in Article 82 with a coherent Directive on data protection in employment relations.** The Commission could then consult the social partners about the proposed directive and the social partners could also develop such a framework themselves through social dialogue. The European Parliament can actively follow up this process through regular consultations of the social partners in the Employment and Social Affairs Committee.

Protection of personal data in employment relations will remain a difficult issue through the further development of intrusive surveillance techniques, test methods, etc. The effective application of data protection will often represent a learning process. This learning process now takes place on an ad hoc basis through court decisions, advice from DPAs, … and could be improved. This justifies a **consultation on a regular basis between the social partners and the DPAs at national and European level**. Such consultation should create awareness of the impact of new technologies and create the necessary trust to develop common solutions. It should help to introduce relevant issues in the social dialogue. Several options for such consultation process are available. The European Parliament can consult the social partners and the Art 29 WP on the preferred options for such consultation process and ensure that it remains informed.

REFERENCES

Interviews

- Marie-Helene Boulanger & Thomas Zerdick, DG Justice, 6 February 2013
- Peter Hustinx & Ute Kallenberger, 6 February 2013
- Dimitrios Dimitriou, DG Employment, 12 February 2013
- Ralf Bendrath, advisor MEP Jan Philipp Albrecht, 13 February 2013
- Eva Barlage-Melber (BDA), Magdalena Bober, Cecilia Zappalà (BUSINESSEUROPE), 18 March 2013

Literature

- Bercusson, B., *European Labour Law*, Cambridge University Press, 2009
- Blanpain, R. (ed), *On-line Rights for Employees in the Information Society. Use and Monitoring of E-mail and Internet at Work*, The Hague, Kluwer Law International, 2002
- Bouchet, H., La cybersurveillance sur les lieux de travail, CNIL, May 2004
- Buttarelli, G., *Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes and to suggest proposals for the revision of the above-mentioned Recommendation*, November 2010, http://www.coe.int/t/dghl/standardsetting/dataprotection/T-PD%20BUR%282010%2911%20EN%20FINAL.pdf
- De Hert P., Gutwirth S., Data protection in the case law of Strasbourg and Luxemburg : constitutionalisation in action. in eds. Gutwirth S., Poullet, Y., De Hert, P., Nouwt, J., & De Terwangne, C., *Reinventing data protection?*, pp.3 - 45, Springer, 2009
- Gutwirth, S., De Hert, P., Regulating Profiling in a Democratic Constitutional State, in Hildebrandt, M. and Gutwirth, S. (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science + Business Media B.V. 2008, 271-293
- Hendrickx, F., *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999
- Hendrickx, F. *Protection of workers' personal data in the European Union. Two Studies*, 2003, http://ec.europa.eu/social/BlobServlet?docId=2507&langId=en
- Hendrickx, F., The Future of Collective Labour Law in Europe, *European Labour Law Journal*, Vol 1 (2010), n°1, 59-79
- Kéfer, F., La légalité de la preuve confrontée au droit à la vie privée du salarié, in Verdussen, M., Joassart, P., *La vie privée au travail*, Anthemis, Limal, 2011
- Kosta, E., *Unravelling consent in European data protection legislation*, KU Leuven doctoral thesis, 2011
- Nouwt, S., de Vries, B., Prins, C. (eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, The Hague, TMC Asser Press, 2005.
- Simitis, S., et al, *Bundesdatenschutzgesetz*, Baden-Baden, Nomos, 2011.

- Smismans, S., The European Social Dialogue in the Shadow of Hierarchy, 2009, *Jnl Publ Pol*, 28, 1, 161-180
- Spiekermann, S., 'The RFID PIA – Developed by Industry, Endorsed by Regulators', in Wright, D. & De Hert P. (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.
- Trubek, D. Trubek, L., Hard and Soft Law in the Construction of Social Europe : the Role of the Open Method of Co-ordination, *European Law Journal*, Vol 11, N°3, May 2005, 343-363
- Vanwijngaerden, J., De werking van grondrechten tussen particulieren, geïllustreerd met voorbeelden, *Jura Falconis*, jg 44, 2007-2008, nr 2, p. 217-248
- Waterschoot, P., Bespreking van enkele arresten van het Arbeidshof te Gent in verband met het gebruik van e-mail en internet op de werkplaats en het controlerecht van de werkgever daarop, *R.W.* 2008-09, 730-744

Official documents

- Article 29 Data Protection Working Party, *Opinion 8/2001 on the processing of personal data in the employment context*, WP 48, 13.9.2001
- _____, *Working document on the surveillance of electronic communications in the workplace*, WP 55, 29.5.2002
- _____, *Working document on Genetic Data*, WP 91, 17.3.2004
- _____, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, WP 114, 15.11.2005
- _____, *Working document on the processing of personal data relating to health in electronic health records*, WP 131, 17.2.2007
- _____, *Opinion 4/2007 on the concept of personal data, 01248/07/EN*, WP 136, 20.06.2007
- _____, *Opinion 15/2011 on the definition of consent*, WP 187, 13.7.2011
- Bundestag, *Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen*, 17/4853, 22.02.2011
- _____, *Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes*, 17/4230, 15.12.2010
- _____, *Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz – BDatG)*, 17/69, 25.11.2009
- _____, *Beschlussempfehlung und Bericht zu dem Gesetzentwurf der Bundesregierung – Drucksache 16/12011 – Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften ...,* 16/13657, 01.07.2009
- Bureau of the Inspector General for Personal Data Protection in Poland et al, *Selected data protection issues. Guide for entrepreneurs*

- CNIL, Circulaire 14 September 2011, http://www.referentsurete.com/cariboost_files/CIRCULAIRE_20JORF_200214_20DU_2015_20SEP_202011_20application_20CNIL.pdf
- CNIL, *Guide pour les employeurs et les salariés*, 2011
- Council of Europe, *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
- European Commission, *Communication from the Commission, First stage consultation of social partners on the protection of workers' personal data*, 2003, http://ec.europa.eu/social/main.jsp?catId=708&langId=en
- _____, *Second stage consultation of social partners on the protection of workers' personal data*, 2004, http://ec.europa.eu/social/BlobServlet?docId=2504&langId=en
- _____, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on a comprehensive approach on personal data protection in the European Union*, COM(2010) 609, 4.11.2010
- _____, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM/2012/011 final, 25.01.2012
- European Data Protection Supervisor, *Guidelines concerning the processing of health data in the workplace by Community institutions and bodies*, September 2009
- _____, *EDPS Video-surveillance Guidelines*, 17 March 2010
- _____, *Follow-up Report to the 2010 EDPS Video-Surveillance Guidelines*, 13 February 2012
- European Parliament, *Opinion of the Committee on Employment and Social Affairs for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 4.3.2013
- ICO, *Employment Practices Data Protection code*, November 2011
- _____, *Employment Practices Data Protection code- supplementary guidance*, June 2005
- ILO, *Code of practice on the protection of workers' personal data*, Geneva, International Labour Office, 1997
- Ministry of Justice Finland, *Act on the Protection of Privacy in Working Life (759/2004)*, 2004, English translation on http://www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf
- National Labour Council (Nationale Arbeidsraad), CBA nr. 38 of 6 December 1983 with regard to recruitment and selection
- _____, *CBA n° 39 of 13 December 1983 relating to information and consultation concerning the social impact of the introduction of new technologies*

- _____, *CBA n° 68 of 16 June 1998 relating to the protection of the privacy of employees in relation with camera surveillance on the work floor.*
- _____, *CBA n° 81 of 26 April 2002 on the protection of privacy of the employees in relation with control of electronic on-line communication.*
- _____, *CBA n° 89 of 30 January 2007 on the prevention of theft by employees and exit-control*
- _____, *CBA n° 100 of 1 April 2009 relating to a preventive alcohol and drug policy in the company*

Other documents

- CBP, *Definitieve bevindingen in het ambtshalve onderzoek naar Verzuimreductie naar aanleiding van 'De Verzuimpolitie' van Zembla*, 3.7.2012
- DG Justice, draft Directive concerning the processing of workers' personal data and the protection of privacy in the employment context, 2004
- National Council of the Belgian Medical Order, advice on investigating drug use (advies Opsporing van druggebruik), 20.2.1993
- Riksdag, *Integritetsskydd i arbetslivet (english summary)*, SOU 2009:44, Stockholm, 2009, http://www.riksdagen.se/sv/Dokument-Lagar/Utredningar/Statens-offentliga-utredningar/Integritetsskydd-i-arbetslivet_GXB344/

EUROPEAN PARLIAMENT

CATALOGUE

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

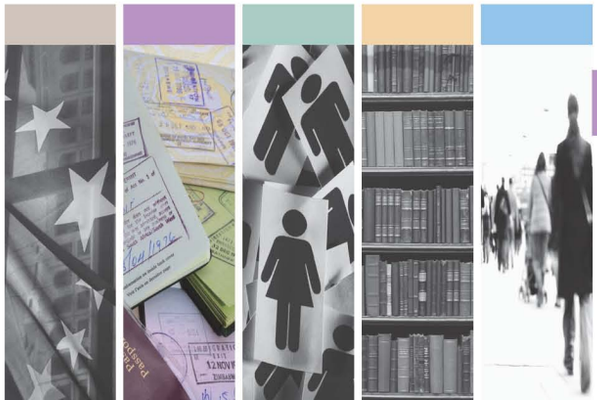
Policy Areas

- Constitutional Affairs
- Justice, Freedom and Security
- Gender Equality
- Legal and Parliamentary Affairs
- Petitions

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**

PHOTO CREDIT: iStock International Inc.



ISBN 978-92-823-4411-8
doi: 10.2861/22062

Publications Office