Data Protection in the Employment Relationship
- The German View -

Gregor Thüsing*
University of Bonn

I. Introduction

In a nutshell, data protection law is the legal response to the various threats posed to privacy[1] – no matter whether they originate from the state or an individual.

It has a comparatively long history in Germany: It first received public attention in connection with profiling done to combat the "Rote Armee Fraktion (RAF)" left wing terrorists. This led to the adoption of the first law worldwide on data protection in the state of Hessen in 1970.[2] The first federal act on the protection of personal data, the Bundesdatenschutzgesetz (BDSG = Federal Data Protection Act), dates back to 1977. Another step forward was the Volkszählungsurteil (Census case) of the Bundesverfassungsgericht (Federal Constitutional Court)[3] in 1983 which created the constitutional mandate for the protection of personal data. In this decision, the Constitutional Court held that the Grundgesetz (Basic Law, i.e. the German Consitution) does not only protect privacy as such but that the respect of a person's private life also encompasses the protection of personal data.[4] Thus the constitution mandates some degree of legal protection for personal data.

Whereas data protection at first was mainly focused on protection from privacy infringing state actions, the need for an effective protection of personal data was highlighted in recent years by several scandals involving processing by private companies. Among the best-known was widespread screening of employees by the Deutsche Bahn AG (the state-run rail company) in 2009 and 2010 and the Deutsche Telekom AG (the former state telecommunications carrier) in 2010. Retail chain Lidl was heavily criticized for employee surveillance in the same timeframe. These incidents have scandalized the populace and have seriously jeopardized the reputation of the companies involved and made data protection an everyday topic even before the NSA scandal.

Due to those scandals as well as a general awareness of threats to privacy as a consequence of new technologies, the social-political debate deals much more with this field of law nowadays. As regards the employment relationship, the European Commission

---

* With collaboration of Dr. Gerrit Forst, Dr. Stephan Pötters and Dr. Johannes Traut.

[1] Cf. Nick Platten, Background to and History of the Directive, in: David Bainbridge, EC Data Protection Directive (1996), ch. 2.

[2] Alexander Genz, Datenschutz in Europa und den USA (2004), p. 9; see alsohttp://www.iuscomp.org/gla/statutes/BDSG.htm (as at April 14th, 2014).

[3] Bundesverfassungsgericht (Constitutional Cour, BVerfG), 15 December 1983, cases 1 BvR 209/83 et alia.

[4] This important case is summarized below (chapter IX) .

pointed out that 'the emergence of a knowledge based economy with technological progress and the growing role attributed to human capital have intensified the collection of workers' personal data in an employment context. These developments give rise to a number of concerns and risks and brought the issue of effective protection of employees' personal data into focus.[5]

Since 1995 with the adoption of the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) data protection law is harmonized by European law, its reform is no longer a purely national but rather primarily a European topic. Therefore, the focus discussion is currently on the reforms proposed by the European Commission in 2012.[6]

But in spite of all new technical threats, scandals and recent developments – the fundamental conflict in the employment relationship as regards the field of data protection remains the same: How to strike a balance between the employee's understandable desire for privacy on the one hand and the employer's vital interests on the other, such as preventing crimes or any other violation of rules set out for his firm by means of surveillance etc.?[7] This conflict of interests is at the heart of each problem that is going to be discussed in this paper. Ensuring proportionality between these contrary principles is therefore of paramount importance for the interpretation of data protection provisions in an employment law context, no matter whether they are European or national rules.

II. At a glance: General principles governing German and European data protection law

1. Justifying the processing of personal data (Section 4 BDSG)

The structure of data protection law is simple and strict: All processing of personal data has to be justified. As far as the national data protection law is concerned, this principle is enshrined in Section 4 (1) of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG). According to this provision, "the collection, processing and use of personal data shall be lawful only if permitted or ordered by this Act or other law, or if the data subject has provided consent." The same principle applies to the law of the European Union (cf. Article 7 of the Data Protection Directive 95/46/EC).

This principle does not only apply to public bodies such as the police, but also restricts the use of personal data by private individuals like an employer. Hence, every employer has to justify all collection, processing and use of the employees' personal data. According to Section 4 (1) BDSG, there are three permissible grounds for justification:

- the processing is allowed under the BDSG,
- the processing is allowed under another law addressing data protection issues, or

[5] See First Report on the implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 final.

[6] In particular 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) 11 final, available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (as at April 14th, 2014).

[7] Cf. Gregor Thüsing, Arbeitnehmerdatenschutz und Compliance (2010), para. 2.

- the data subject (i.e. the employee) has given his or her consent.

2. Fundamental principles governing the processing of the employee's personal data by the employer

Data protection law is governed by several other general requirements that have to be met when processing personal data in the employment relationship. Those principles are laid out in a 2001 opinion of the **Article 29 Working Party** on the processing of personal data in the employment context:[8]

- ✓ FINALITY: Data must be collected for a specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes.
- ✓ TRANSPARENCY: As a very minimum, workers need to know which data is the employer collecting about them (directly or from other sources), which are the purposes of processing operations envisaged or carried out with these data presently or in the future. Transparency is also assured by granting the data subject the right to access to his/her personal data and with the data controllers' obligation of notifying supervisory authorities as provided in national law.
- ✓ LEGITIMACY: The processing of workers' personal data must be legitimate. Article 7 of the Directive lists the criteria making the processing legitimate.
- ✓ PROPORTIONALITY: The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. Assuming that workers have been informed about the processing operation and assuming that such processing activity is legitimate and proportionate, such a processing still needs to be fair with the worker.
- ✓ ACCURACY AND RETENTION OF THE DATA: Employment records must be accurate and, where necessary, kept up to date. The employer must take every reasonable step to ensure that data inaccurate or incomplete, having regard to the purposes for which they were collected or further processed, are erased or rectified.
- ✓ SECURITY: The employer must implement appropriate technical and organizational measures at the workplace to guarantee that the personal data of his workers is kept secured. Particular protection should be granted as regards unauthorised disclosure or access.
- ✓ AWARENESS OF THE STAFF: Staff in charge or with responsibilities in the processing of personal data of other workers need to know about data protection and receive proper training. Without an adequate training of the staff handling personal data, there could never be appropriate respect for the privacy of workers in the workplace.

[8] Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf (as at April 14th, 2014).

III. National data protection law within the European regulatory framework: It's all about proportionality

Data protection law applicable in Germany can be derived from two sources: the law of the European Union and national German law. In case of a conflict between the different provisions, the law of the Union reigns supreme: National law that is in breach of European primary law – that is the law of the treaties – may not be applied nationally. All national legislation has to be applied and interpreted by the courts as far as possible in conformity with the law of the Union, regardless whether it is primary or secondary law.

It is therefore worthwhile to first look at the law of the Union in order to grasp the system of data protection law as it is in Germany: Data Protection law and the protection of privacy are deeply rooted in European law. Even the primary law of the European Union places great emphasis on the protection of citizens' privacy and personal data and mandates protection of personal data as can be gleaned from the Charter of Fundamental Rights. According to Art. 6 para. 1 of the Treaty of the European Union the Charter of Fundamental Rights is part of the primary law of the Union. Art. 8 of the EU Charter of Fundamental Rights contains an explicit guarantee of the protection of personal data. It reads as follows:

> **Article 8 Protection of personal data**
>
> 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.

On the level of the secondary law the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (**Data Protection Directive**) is the central instrument regulating the processing of personal data. This directive was developed and has to be interpreted according to the law of the European treaties, in particular Art. 8 of the EU Charter of Fundamental Rights.

The Data Protection Directive applies to all automated processing of personal data with the exception of the fields which fall outside the scope of the law of the European Union – such as national security or defence – and processing by a natural person in the course of a purely personal or household activity. Thus the Directive regulates not only data processing by private citizens – in particular data processing in a commercial setting – but also data processing by state agents, for instance in the field of law enforcement or social security. Since the Data Protection Directive has no specific rules for the processing of employee data by the employer, the general rules apply for processing in an employment relationship.

The legal form "Directive" is a legislative act of the European Union which requires member states to achieve a particular result without dictating the means of achieving the result (Art. 288 Sec. 3 TFEU). This contrasts with the self-executing regulation which is directly applicable in all Member States (Art. 288 para. 2 TFEU).

Thus the Directive necessarily requires a national implementing act, which is then directly applicable in that member state. The Data Protection Directive has the peculiarity to be implemented not by one but by several German implementing Acts on both federal

and state level, which individually only cover part of the Directive's scope. Data Processing by private citizens as well as data processing by federal agencies is covered by the Bundesdatenschutzgesetz (Federal Data Protection Act – BDSG). Data processing by agencies of the federal states – for instance by law enforcement purposes – is regulated by the respective state Data Protection laws. In practice the BDSG is by far the most important implementing act, as it covers data processing by private citizens.

Despite length and multitude of these implementing acts, the member states actually have very limited leeway in determining the legality of processing: The Directive does not merely establish a basic standard but aims to reconcile – as can be gleaned from its name – the protection of personal data with the free flow of data within the common market. In order to set uniform rules for the common market, the data protection directive 95/46/EC sets a European uniform standard from which member states may not derogate – neither in the direction of stricter rules nor by relaxing them.[9] The substantial law standards are – at least as long as the directive is properly implemented into national law – the same in all member states.

Article 6 and 7 of the Directive contain the most important provisions in regard to the substantial standard of law. Article 6 establishes the principles relating to data quality:

> **Article 6**
>
> 1. Member States shall provide that personal data must be:
> (a) processed fairly and lawfully;
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
>
> 2. It shall be for the controller to ensure that paragraph 1 is complied with.

Most important of these principles is the principle enshrined in lit. b and c which may be summarily called the principle of purpose limitation. Data may only be processed for specified purposes and only insofar as it is necessary to fulfill that purpose. This obliges the person controlling the data processing (**controller,** Art. 2 lit. d of the Data Protection Directive) to reflect his processing activities and define the purposes clearly.

Art. 6 lit. a of the Directive also requires that processing must occur lawfully. Meant by this is that any processing needs an explicit legal basis – this is echoed by Section 4 of the BDSG (see above). The legal grounds for processing are enumerated in Art. 7 of the Data Protection Directive:

[9] Court of Justice of the European Union (CJEU), 6 November 2003, case C-101/01, paras. 96 f. (Lindqvist).

Article 7

Member States shall provide that personal data may be processed only if:
(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

These alternatives are non-exclusive. Most important in the context of private processing is certainly lit. f), the balance of interest. All other variants enumerated in Art. 7 are no more than descriptions of particular cases in which the balance of interest may tip in favour of the controller. Since this balance of interest can only be assessed on a case by case basis, implementing acts which ban certain kinds of processing altogether are quite problematic at least in the private sector. It is unlikely that one can assume that the balance of interest will always tip in favour of the person whose data is being processed (**data subject**).

Therefore in many cases implementing acts have to be interpreted quite broadly in order to meet the standard of the Directive. The Directive does not only require the member states to adopt implementing acts in accordance with the Directive, but also requires their interpretation in accordance with the Directive.

Nevertheless, within its scope the influence of the Directive is very far-reaching and even derogates the national Constitution: Even though personal data may also be protected by the member states constitution – as is the case in Germany with Art. 2 in conjunction with Art. 1 of the Grundgesetz ("Basic Law", ie the Constitution of Germany; GG) – these provisions also have to be interpreted in accordance with the EU Charter of Fundamental Rights and the Directive. Bearing in mind that the Directive itself strikes the balance between the protection of personal data and in particular commercial interests, this balance has to be transferred to the national Constitutions. It is currently unclear if and to what extent the member states have leeway in determining the balance.

However, it is safe to say, that the Court of Justice of the European Union (CJEU) and its interpretation of the Directive does not leave a large margin for manoeuvre for the Member States. In its leading case *Lindqvist* the Court held that the harmonisation of the national laws is "not limited to minimal harmonisation but amounts to harmonisation which is generally complete. […] It is true that Directive 95/46 allows the Member States a margin for manoeuvre in certain areas and authorises them to maintain or introduce particular rules for specific situations as a large number of its provisions demonstrate. However, such possibilities must be made use of in the manner provided for by Directive 95/46 and in accordance with its objective of maintaining a balance between the free

movement of personal data and the protection of private life."[10]

IV. Processing of personal data under Section 32 BDSG

As pointed out above, all processing of personal data has to be justified by the responsible controller. This is expressed by Section 4 (1) BDSG: "The collection, processing and use of personal data shall be lawful only if permitted or ordered by this Act or other law, or if the data subject has provided consent."

In the employment context, the most important provision that serves as a basis for the justification of the processing of personal data is Section 32 BDSG. Section 32 BDSG – in the government provided, but unofficial English translation[11] – reads:

> **Section 32: Data collection, processing and use for employment-related purposes**
>
> (1) Personal data of an employee may be collected, processed or used for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract. Employees' personal data may be collected, processed or used to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the collection, processing or use of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in excluding the collection, processing or use, and in particular the type and extent are not disproportionate to the reason.
> (2) Sub-Section 1 shall also be applied when personal data are collected, processed or used without being processed by automatic procedures nor processed, used in or from a non-automated filing system, nor collected in such a filing system for the purpose of processing or use.
> (3) The rights of participation of staff councils shall remain unaffected."

Para. 1 allows data processing only insofar as it is "necessary" for hiring decisions or carrying out or terminating the employment contract. This wording led several commentators to interpret the provision very narrowly and for instance exclude employee screenings without concrete grounds for suspicion.[12] This approach, however, is treacherous and often not in line with the Directive. The latter applies, as everywhere else, the interest of balance test which does not limit processing to cases where this is strictly speaking necessary. One example is the aforementioned employee screening: Processing only slightly interfering with employees privacy – for instance automatically checking that payments made by the company to contractors are not paid to the same bank account as an employee's salary – can be justified by the employers overwhelming interest to combat fraud in his company.

Moreover, Section 32 (3) BDSG extends the scope of the protection beyond the scope of the Data Protection Directive as it implements and includes also non-automated.

---

[10] CJEU, 6 November 2003, case C-101/01, paras. 96 f. (Lindqvist).; This approach was reaffirmed very distinctly in CJEU, 16 December 2008, case C-524/06, paras. 51 f. (Huber v Germany), and lately in CJEU, 24 November 2011, case C‑468/10 (ASNEF).

[11] See http://www.gesetze-im-internet.de/englisch_bdsg/index.html (as at April 14th, 2014).

[12] See Achim Seifert in: Spiros Simitis (ed.), Bundesdatenschutzgesetz (7th ed. 2011), § 32 paras. 103, 108; Martin Kock and Julia Francke in: Neue Zeitschrift für Arbeitsrecht (NZA) 2009, p. 646, 648; unclear Michael Kort in: Der Betrieb (DB) 2011, p. 651, 653.

This, of course, is very far reaching as even an employer looking at his employee could be interpreted as processing personal data, e.g. his skin colour. This is, however, not per se prohibited as the Directive explicitly does only apply for automated processing and processing involving a file (Art. 3 para. 1 of the Directive 95/46/EC). Therefore member states are free to regulate non-automated processing.

V. The data subject's consent (Section 4a BDSG)

Apart from Section 32 BDSG, another important option to justify the processing of personal data in the employment context is the employee's consent. As laid down in Sections 4 and 4a BDSG, consent is one of the grounds on which personal data may be processed legitimately.

But what exactly is "consent"? Pursuant to Article 2(h) of the Directive 95/46/EC 'the data subject's consent shall mean "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." In general, the data subject's consent has to be given "unambiguously", see Article 7(a) of the Directive 95/46/EC.

From these provisions we can derive four requirements that have to be met: Consent must be

- freely given,
- specific,
- and informed.
- It may consist of any indication of the data subject's wishes by which he/she signifies his/her agreement to personal data relating to him being processed.

1. Freely given

The first condition can be considered as the most contentious notion in relation to employment law. Economic pressure may amount to duress so as to vitiate consent.[13] It is even arguable that in the context of employment consent is basically never given entirely freely. Although this might be going too far,[14] special attention has to be paid to whether the worker has a genuine free choice. If this is the case, there is no reason why the employee's consent should not, according to current EU law, legitimize the processing. This interpretation is also in conformity with the Union's primary law, especially the subject's fundamental rights. The European Court of Human Rights (ECHR) has held that individuals are capable of consenting to waive fundamental rights under the EU Charter of Human Rights (EChHR).[15] Article 8(2) of the EU Charter of Fundamental Rights also explicitly mentions consent as a possible justification.

It also has to be pointed out that the employee's consent does not constitute a blank cheque for the employer. The processing still has to comply with the other data protection principles, in particular the principle of proportionality. In short, it may be difficult but not impossible to show that the employee's consent has been given freely.

[13] Cf. UK Privy Council, 6 April 1979, case *Pau On v Lau Yiu Long*.
[14] Cf. Rosemary Jay, Data Protection – Law and Practice (3rd ed., 2007), p. 152.
[15] ECHR, 9 April 1997, case 29107/95, (Stedman v UK); cf. Rosemary Jay, Data Protection – Law and Practice (3rd ed., 2007), p. 152.

2. Specific

The second requirement to be examined is the term specific. This notion is rather vague. *Jay* holds that consent clauses may still be broad as long as they are clear about all relevant matters.[16] This interpretation is too generous. The German wording of the Directive ("für den konkreten Fall" = "in a concrete case") suggests a narrower approach limiting the legitimising effect of the employee's consent to a specific processing of specific personal data. Hence the requirement of specificity rules out all vague and generalised forms of consent that would legitimise any data processing in relation to an employment relationship.

3. Informed

Thirdly, the consent must also be informed. The data subject must be aware of the nature of the processing and any important features which might affect him or her.[17] This also implies that the data subject must be able to assess the consequences of his or her consent with regard to his fundamental rights. Otherwise the consent would not be in conformity with the primary law. It is of particular importance that the subject knows which personal data will be processed and for what purpose.[18] As to the degree of knowledge necessary to make consent valid it might be useful to draw parallels to the doctrine of informed consent that has been developed for negligence cases in relation to medical treatment;[19] these parallels may be particularly instructive in regard to the processing of sensitive data.

4. Indication of the data subject's wishes

Fourthly, the consent has to consist of an indication of the data subject's wishes. Therefore, silence or mere passive acquiescence is not sufficient.[20] On the other hand, consent can be inferred from conduct[21] as long as it does not have to be "explicit" as it is the case in relation to sensitive data. According to recital (17) of the Directive 2002/58/EC "consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website." The national German law seems to be even stricter – but this is misleading as it has to be interpreted in conformity with the EU law. According to Section 4a BDSG, the data subject's consent has to be in *written* form. This is not necessary in order to be in conformity with the Directive and therefore shouldn't be interpreted too literally, but it clearly shows that the subject's consent must be founded on a clear indication of the agreement to a particular processing.

---

[16] Rosemary Jay, Data Protection – Law and Practice (3rd ed., 2007), p. 152.
[17] Rosemary Jay, Data Protection – Law and Practice (3rd ed., 2007), p. 152.
[18] Cf. Peter Gola and Rudolf Schomerus, Bundesdatenschutzgesetz (10th ed. 2010), section 4a paras. 10 ff.
[19] For comprehensive information about the doctrine of informed consent see Alasdair Maclean, The doctrine of informed consent: does it exist and has it crossed the Atlantic?', Legal Studies (LS), Vol. 24 (2004), pp. 386ff. and Josephine Shaw, 'Informed consent: a German lesson', International and Comparative Law Quarterly (ICLQ), Vol. 35 (1986), pp. 864ff., who demonstrates that this doctrine is well developed in civil law countries like France, Switzerland and Germany.
[20] Cf. Rosemary Jay, Data Protection – Law and Practice (3rd ed., 2007), p. 153.
[21] Cf. CJEU, 21 November 2001, case C-414/99 (Zino Davidoff SA v A&G Imports Ltd).

5. Consent in the employment context

The underlying rationale of the provisions regarding consent is a very old doctrine that applies to various areas of law: *volenti non fit iniuria*. Nevertheless, the legitimacy of this universal idea has been questioned in relation to data protection in the employment relationship. As has already been mentioned (see above II.2.), in 2001 the Article 29 Working Party issued an opinion on the processing of personal data in the employment context.[22] The Working Party held that consent "should only be a fall-back position if no other Art. 7 criteria or Art. 8 exception is applicable." Reliance on consent should only be confined to situations where the employee has a genuine free choice and is subsequently able to withdraw the consent without detriment.[23] It is indeed arguable whether the employee's consent could still be freely given in situations where none of the other criteria of Article 7 or Article 8 of the Directive is satisfied. For example, if the giving of consent is a condition of employment, it is very likely that the employee will accept the relevant clause in order to not lose the job opportunity.[24] To sum it up, the inequality of bargaining power which is inherent in the employment relationship[25] may force the employee to consent to a certain processing of data.

For this reason, the German government is discussing a reform of the national data protection law that would (in principle) lead to an abolition of consent in the employer employee relationship.[26] In Finland, the Act on Protection of Privacy in Working Life prescribes that the employer is entitled to process personal data only in cases where this is necessary for the observation of the rights and obligations of the parties to the employment relationship; there can be no exemption from this necessity requirement, even with the consent of the employee.[27] In Belgium, the employee's consent alone may not legitimise the processing of sensitive data.[28]

This issue was further discussed on a European level. The social partners were consulted by the Commission and research studies were undertaken.[29] The Commission

[22] Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf (as at April 14th, 2014).

[23] Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf (as at April 14th, 2014), p. 23.

[24] Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf (as at April 14th, 2014), p. 23.

[25] See Otto Kahn-Freund, Labour and the Law (1972), p. 7; the inequality of bargaining power as an "axiom" of labour law is not uncontested today, cf. Abbo Junker, Individualwille, Kollektivgewalt und Staatsintervention im Arbeitsrecht, in: NZA 1997, p. 1305; Lord Wedderburn, Labour law 2008: 40 years on, in: International Law Journal (ILJ), Vol. 36 (2007), pp. 39.

[26] See Section 32l of the bill proposal (24.08.2010). The bill is available at: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_Beschaeftigtendatenschutz.pdf?__blob=publicationFile (as at April 14th, 2014).

[27] See http://www.eurofound.europa.eu/eiro/2001/06/feature/fi0106191f.htm (as at April 14th, 2014).

[28] See the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87 final, p. 11.

[29] The different communications and studies are available at http://ec.europa.eu/social/main.jsp?catId=708&langId=en (as at April 14th, 2014).

also took the view that the role consent can play in an employment relationship is limited, due to the dependant and subordinate situation of the worker.[30] But later on, after the social partners had failed to conclude a European agreement on the protection of personal data in the employment context, the Commission held that the Directive 95/46/EC should not be amended.[31]

So, in the end: just much ado about nothing? Not quite. In summary, it can be said that the employee's consent still serves as ground for justification in EU and national data protection law. But, as the discussions have shown, the relevant provisions have to be applied restrictively and attention has to be paid whether the subordinate structure of the employment relationship does not exclude the possibility of freely given consent.

VI. Risk-based approach: Different categories of personal data and different purposes for processing them

As pointed out above, data protection in the employment context is primarily about ensuring a proportionate balance between the employer's and the employee's fundamental rights and interests. The central question is: How to strike a balance between the employee's understandable desire for privacy on the one hand and the employer's vital interests on the other?[32]

The employer's interests can be very diverse. As long as his or her objective is legitimate, it can theoretically justify all processing of personal data, as long as the employer respects the principle of proportionality. The employer may, for example, process data in order to prevent crimes or any other violation of rules set out for his firm by means of surveillance, he may process data for matters of recruitment, effective human resource management such as job allocation, transfer of employees, health and safety compliance, work-related injuries and their compensation disputes, for preventing the leakage of trade secrets, etc. This leads us to the conclusion that there are few *per se* illegitimate purposes. Criminal activities of the employer would be one, but most seriously considered purposes can possibly justify data processing.

But not all goals the employer pursues have the same validity. Some objectives are more important than others and those differences are mirrored in the structure of the different provisions of data protection law. For example, there is a special provision dedicated to the processing of personal data to investigate crimes (Section 32(1), second sentence BDSG).

Another important distinction made by the BDSG (and the Data Protection Directive 95/46/EC) relates to certain types of personal data. For example, the provisions on certain data, which are categorized as being particularly sensitive, are much stricter. Section 3(9) BDSG defines sensitive data as all information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life (cf. also Article 8 of the Data Protection Directive). The processing of those sensitive data has to

[30] Communication from the Commission, Second stage consultation of social partners on the protection of workers' personal data, p. 10 f., available at http://ec.europa.eu/social/main.jsp?catId=708&langId=en (as at April 14th, 2014).
[31] Communication from the commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87 final, p. 5, 10.
[32] Cf. Thüsing, Arbeitnehmerdatenschutz und Compliance (2010), para. 2.

fulfil stricter legal requirements than the processing of other data. Section 28, for instance, regulates the processing of personal data for commercial purposes. Under Section 28(1) no. 2 BDSG, personal data may be processed, "as far as necessary to safeguard legitimate interests of the controller" and if "there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of processing or use." However, this very broad clause does not apply to sensitive data. Under Section 28(6) BDSG, the collection, processing and use of sensitive personal data shall only be lawful if

> "1. necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his or her consent,
> 2. data are involved which the data subject has manifestly made public,
> 3. necessary to assert, exercise or defend legal claims and there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of collection, processing or use, or
> 4. necessary for the purposes of scientific research, where the scientific interest in carrying out the research project significantly outweighs the data subject's interest in ruling out the possibility of collection, processing and use and the purpose of the research cannot be achieved in any other way or would require a disproportionate effort."

Another example for the distinction between sensitive and other data are the provisions on the data subject's consent: In general, the consent has to be given 'unambiguously', see Article 7(a) and Article 26(1)(a) of the Data Protection Directive. In relation to sensitive data, the provisions of the Data Protection Directive are stricter, as the data subject has to give his 'explicit' consent, see Article 8(a) of the Data Protection Directive.

Whereas the law is stricter whenever sensitive information is concerned, the processing of "generally accessible data" is much easier to justify, cf. Section 28(1) no. 3 BDSG or Section 29(1) no.2 BDSG.

These examples demonstrate that the legislator has pre-balanced the balancing of interests that has to be done in every individual case (proportionality test).

VII. Central issues of data protection law in the employment relationship

1. Personal information in the hiring process / job interviews

Job seekers around the world need to be prepared to answer a range of questions before being employed. However, the German courts have limited the right of the prospective employer to ask questions for decades.[33] According to jurisprudence, in a job interview the prospective employer may only ask questions when he has a legitimate interest to know the answer. If the prospective employer asks a question he may not ask, the applicant is allowed to lie without having to be afraid to be dismissed for the lie later on.[34]

Since 2009, the „legitimate interest" test has a statutory basis in Section 32 Federal Data Protection Act. According to this rule, the prospective employer may process data only if the processing of this data is „necessary", meaning proportionate (see above under

[33] Seminal Bundesarbeitsgericht (Federal Labour Court, BAG), 5 December 1957, case 1 AZR 594/56.
[34] See e.g. BAG, 6 September 2012, case 2 AZR 270/11.

VI.). Moreover, Sections 19 pp. Genetic Diagnosis Act (Gendiagnostikgesetz) render it illegal to process the data of applicants and employees (very limited exceptions apply for health security reasons). Finally, the General Antidiscrimination Act (Allgemeines Gleichbehandlungsgesetz) prohibits to discriminate against applicants on the ground of race or ethnic origin, sex, religion or philosophical belief, disability, age or sexual orientation. If the prospective employer processes data on any of these subjects, this may indicate a discrimination of the applicant. The prospective employer will then have to prove that in fact, he did not discriminate against the job seeker.

On this background, the prospective employer is allowed to ask an applicant for contact details such as his name, address, phone number, driver's licence etc., as long as the processing of this data is necessary.

On the other hand, the employer is usually not allowed to inquire into the ethnic origin or race of an applicant, a trade union membership (exceptions may apply for trade unions as employers and/or employers' unions), disability, sickness or disease (as long as it does not pose a threat to others and does not limit the ability of the applicant to work), religion or philosophical belief (exceptions may apply for religious groups as employers), sexual orientation, pregnancy (as it indicates a discrimination on the basis of sex)[35] or membership in a political party (exceptions may apply for political parties as employers).

Also, the employer is not allowed to inquire into data that does not relate to the prospective employment relationship in any way. Usually this covers data such as family structure, marital status, credit information, litigation history, club membership and so on. In some countries, prospective employers seem to ask applicants for their social networking passwords. In Germany, a question like that is virtually unthinkable and would probably trigger a public outcry as well as administrative action in the form of fines, or worse.

Finally, the employer may be allowed to ask for criminal convictions or pending investigations.[36] However, he is limited to processing data that might affect the applicant to pick up the prospective work and/or to do it properly. Therefore it may be legal for a logistics company to ask a prospective lorry driver whether he has ever been convicted for traffic related crimes, but they would not be allowed to ask him for, e.g., a conviction for insulting people. A financial institution may ask an applicant for criminal convictions related to business (fraud, money laundering etc.), but not whether he has been convicted for, e.g., drunk driving. Pending investigations may be inquired into if they might limit the ability of an applicant to pick up work or might otherwise affect the employment relationship. However, the presumption of innocence needs to be respected, so that jurisprudence is rather restrictive with respect to pending investigations.[37]

2. Video surveillance / CCTV in the workplace

Nowadays, video surveillance of publicly accessible areas or also of private company premises is widely used.

a) Applicable provisions of the Federal Data Protection Act (BDSG)

The use of CCTV / video surveillance is mainly governed by three provisions of the

[35] BAG, 6 February 2003, case 2 AZR 621/01.
[36] See e.g. BAG, 6 September 2012, case 2 AZR 270/11 and BAG, 15 November 2012, case 6 AZR 339/11.
[37] See BAG, 15 November 2012, case 6 AZR 339/11.

Federal Data Protection Act (BDSG) that can be relied on by the employer in order to justify the processing of the personal data of the people monitored by the cameras:

- Section 6b BDSG: This provision governs the use of CCTV technologies in publicly accessible areas, e.g. supermarkets, train stations, shops, etc.
- Section 32 BDSG: This provisions is applicable for the surveillance of employees in any other situation, i.e. non-publicly accessible areas of the workplace
- Section 28 BDSG: This provision is applicable if the video surveillance is used for purposes not related to the employment relationship, e.g. when customers or other third parties are being monitored

All of those provisions require a legitimate interest or purpose for the video surveillance and a proportionality test.

b) Legitimate purposes

The purposes have to be stipulated in a concrete way before the installation of the surveillance system, meaning they have to be documented and made available by means of an index of procedures to any interested person, see Section 4g (2) BDSG.

The main reason why employers install CCTV technologies is probably to protect the company against vandalism, theft or other property crimes or to protect persons (employees, clients etc.) from criminal activities. So in general, the main purpose of video surveillance is not the monitoring and control of employees. However, both are often congruent. Thus, at banks or in parking garages, in the area of cash desks of department stores or museums – virtually casually –employees are also being monitored. Be it casually or intentionally, video surveillance of employees is only admissible within strict limits.

c) Proportionality test

Irrespective of which particular provision of the BDSG is applicable (whether Section 6b BDSG governing the use of video surveillance in publicly accessible areas or Section 28 BDSG or Section 32 BDSG) – when it comes to the assessment of the permissibility of video surveillance, the central yardstick of evaluation is always a proportionality test. It has to be evident that surveillance is “necessary”, i.e. there must not be any other effective alternative to video surveillance. In addition, the relation of means and purpose has to be proportionate. It is not allowed to use video surveillance in connection with minor offences, e.g., in order to control an existing ban on smoking.

If video surveillance of publicly accessible areas complies with Section 6b BDSG and those publicly accessible areas also happen to be workplaces – e.g., the video surveillance in a bank or a supermarket – the employees will have to accept video surveillance as immanent in their workplace. However, in cases where the employees are not the real object of observation, any evaluation of the results of monitoring for the purpose of a control of productivity or behaviour-related information is inadmissible. Therefore, the evaluation of video surveillance of a bank used for the purpose of protection against robbery would be justified, but not for the purpose of controlling the employees’ behaviour. However, in a department store, video surveillance might perhaps be legitimately used for the purpose of protection against theft by the employees.

But in general, work is usually not performed in publicly accessible areas. In that case, it is only allowed to use video surveillance in compliance with Section 28 or 32 BDSG. In this context, the principle of proportionality has to be observed strictly. The

Federal Labour Court held that even the mere possibility of surveillance at any time puts considerable pressure on the employee which is incompatible with his right to the respect of his personal rights.[38] The Federal Labour Court draws the conclusion that video surveillance in the workplace is only justified in exceptional cases where the employer has vital interests. In general, it has to be assumed that the following principles are established case law:

- Before starting video surveillance, there have to be sufficient grounds for suspicion (for example in case of theft, etc.), which justify an intrusion into the data subject's personal rights. Any vague assumption or a general suspicion of all employees is not sufficient.
- In principle, video surveillance is generally only permissible if carried out openly rather than secretly, by means of visible equipment and only after the staff has been provided with sufficient information.
- As an "ultimo ratio", last ditch measure, surveillance by hidden cameras is permissible if it is the only possibility to protect the employer's legitimate interest.
- Video surveillance is subject to co-decision by the works council or by the staff council.
- Findings obtained by illegal monitoring are subject to a ban on any further use. They also cannot be used as evidence in a dismissal lawsuit.

3. Surveillance of internet and e-mail at the workplace

The use of the internet at work generates vast amounts of data. From a technological point of view, employers may use this data to survey the behaviour of their employees. From a legal perspective, monitoring the use of the internet and applications like e-mail by employees raises a range of questions: A crucial point is whether such surveillance is covered by the *Telekommunikationsgesetz* (Telecommunications Act, TKG) or not.

If the TKG is applicable, an employer is allowed to survey the use of the internet and applications like e-mail only for technical purposes (such as virus scanning) and to calculate fees (if the employee has to pay for private usage). The TKG does not allow an employer to monitor data for, e.g., reasons of corporate compliance. For employers it is seminal to note that a violation of the TKG is likely to constitute a crime under Section 206 *Strafgesetzbuch* (Criminal Code, StGB). In practice, it is therefore strongly recommended to act as if the TKG is applicable, even if it should not be from a theoretical perspective.

If the TKG is not applicable, surveillance of internet and e-mail usage by employees is covered by the BDSG. As seen above, Section 32 BDSG allows a processing of data if it is "necessary", meaning proportionate.

Although it is therefore of utmost importance for employers to know whether the TKG applies, this is arguable and quite uncertain. The decisive question is whether the employer is a *Diensteanbieter* (provider of services) in the meaning of the TKG or not. If he is a provider of services, he is subject to most of the rules of the TKG. The crucial rule here is Section 3 No. 6 TKG. According to this provision, a provider of services is a person that provides telecommunication services professionally or that helps to provide such services.

[38] Cf. in particular BAG, 21 June 2012, case 2 AZR 153/11.

In the past, the prevailing opinion in Germany held that an employer was a provider of services if he allowed his employees to use his telecommunication facilities for private purposes (e.g. calling home or using private webmail services), even if they were allowed to do so to a limited extend or in brakes only. The employer was not considered to be a provider of services if he prohibited the private use of such facilities. This differentiation is still quite common. This means in effect that internet and e-mail surveillance is not possible (other than for technical or billing reasons) if the employer allows his employees to use telecommunications facilities for private purposes.

During the last couple of years however, several Landesarbeitsgerichte (Higher Labour Courts, LAG) argued that the employer is not a provider of services even if he allows his employees to use telecommunications facilities privately.[39] The main argument for this opinion is that the TKG governs the competition on the market for telecommunication services. But an employer does not compete with telecommunications companies if he allows his employees to use the telecommunications facilities for private purposes. He does not act for profit. An employer simply wants to create some amenities for his employees and wishes to facilitate their work-/life-balance. Therefore, he should not be covered by the TKG.

As the second opinion is quickly gaining ground, it is likely that it will become predominant in the near future. The effect is that internet and e-mail surveillance will have to be proportionate under Section 32 BDSG. Although the legal situation is uncertain and every processing will have to be assessed in the light of the individual case, one can identify certain principles: Data that is obviously private (e.g. invitation for a dinner) may not be processed. Log files containing technological data only (e.g. time when an e-mail was sent, amount of data transferred) can be processed more easily than files with "real" content (e.g. text or pictures). The amount of data processed needs to be reduced as much as possible. Transparent processing is the rule, secret processing the absolute exception. Secret processing may take place to prove criminal behaviour, but even then it has to be considered carefully and can be a last resort only.

4. Transfer of data in international corporate groups

Corporate groups regularly need to transfer personal data of employees between group members: Employee data often is processed by the head of the group, at least for certain purposes (e.g. pension schemes). Also, certain group-wide services may be pooled in one of the group members (e.g. IT services). Under these circumstances, data often needs to be transferred from group member A to group member B. This transfer is a processing of data that needs to be justified. A justification of the transfer of data within Germany is subject to the same rules as any other processing of data. However, things get more complicated if group member A and group member B are not located within the same country.

As long as group member A and group member B are both located within the European Union, a transfer of personal data is to be treated like a transfer of data within Germany. However, under the Directive 95/46/EC, special rules apply if group member A

[39] Higher Labor Court (Landesarbeitsgericht, LAG) of Berlin and Brandenburg, 16 February 2011, case 4 Sa 2132/10; LAG Hamm, 10 July 2012, case 14 Sa 1711/10, cf. also Higher Administrative Court of Hessen (Verwaltungsgerichtshof, VGH), 19 May 2009, case 6 A 2672/08.Z.

is located in an EU country and group member B in a non-EU-country ("third country"). Germany implemented these rules in ss. 4b, 4c BDSG.

According to Article 25 Directive 95/46/EC, the Member States shall provide that the transfer of personal data to a third country may happen only if the third country in question ensures an adequate level of protection. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances of a data transfer. The European Commission may find that a third country ensures an adequate level of protection. A decision of the European Commission on this subject is binding for the Member States.

Third countries featuring an adequate level of protection from the point of view of the European Commission currently are Andorra, Argentina, Australia, Canada, Switzerland, the Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand and the Eastern Republic of Uruguay.[40]

Article 26 Directive 95/46/EC allows for derogations from the principle set out in Art. 25 Directive 95/46/EC. Derogations may apply if

- the data subject has given his consent unambiguously to the proposed transfer; or
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
- the transfer is necessary in order to protect the vital interests of the data subject; or
- the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

However, the applicability of these derogations needs to be assessed in the light of each individual case. Therefore, they do not form a reliable basis for a data transfer in an international group of companies.

If the third country does not feature an adequate level of protection and none of the derogations set out above applies, group member A may nevertheless transfer the data to group member B located in a third country, provided that group member A adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.

There are various ways to adduce such adequate safeguards:

- *Standard contractual clauses:* The European Commission has published three

[40] A list of countries is available at http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-1 (as at April 14th, 2014).

sets of model contracts governing the transfer of data between parties located in a Member State and a third country.[41] These standard contractual clauses need to be agreed by the parties without amendments to create adequate safeguards in the meaning of Art. 26 Directive 95/46/EC. Standard contractual clauses are preferable if no more than two (or very few) members of a group need to transfer data between each other. However, they are no longer manageable if data transfer is to take place between various group members, as this would require a complex network of contracts. In such a situation, binding corporate rules are preferable (see below).

- *Individual contractual clauses:* In theory, it is possible for the parties to agree upon individual contractual clauses adjusted to the needs of the parties. However, these clauses would have to be accepted by the data protection authorities. Even if these are willing to give their consent, bureaucratic burdens render individual contractual clauses a highly impractical instrument.
- *Binding corporate rules:* Binding corporate rules are an alternative to standard contractual clauses in cases where more than two (or very few) group members need to transfer data to each other.[42] As to the arrangement of such corporate rules it is crucial that they are drafted in a legally binding way, equally mandatory for all companies of the group, and that this arrangement is implemented within the respective company in form of instructions by the respective employer vis-à-vis all employees.

Special rules apply with respect to the United States of America:[43] The USA are considered to be one of the states *without* an adequate level of data protection by the EU. However, in 2000, the EU entered an agreement with the USA on a so-called "safe harbour" (Safe Harbor Agreement). According to the agreement, an adequate level of data protection is assumed in companies which avow that they respect the principles stipulated in the agreement and which have their practises examined accordingly. In theory, the implementation of these obligations is controlled by independent audit firms, and the Federal Trade Commission of the US Department of Commerce is entitled to punish violations by imposing considerable fines. Recent studies however revealed that the safe harbor principles are widely disregarded in practice.[44]

[41] For details, see http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm (as at April 14th, 2014).

[42] For details, see http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm (as at April 14th, 2014).

[43] For details, see Commission Decision 520/2000/EC and at http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm sub USA (as at April 14th, 2014).

[44] For details on the transfer of data in international corporate groups see Gerrit Forst, Verarbeitung personenbezogener Daten in der internationalen Unternehmensgruppe, in: Der Konzern 2012, p. 170 – 185.

VIII. Some remarks on the proposed reform of the European legal framework

While there is much debate on how specific questions should be solved by German legislation, the more important developments are currently happening on the European level, in particular the reform of the data protection legislation.

In 2012, the European Commission proposed a major reform of the EU legal framework on the protection of personal data. The cornerstone of the reforms initiated by the Commission is the **proposal** for a "**General Data Protection Regulation**".[45]

This proposal explicitly addresses data processing in the employment context for the first time on the European level. However, it is rather a non-regulation as Article 82 of the proposed Regulation establishes a so-called opening clause for the Member States. Section 1 of this Article reads as follows:

> "Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment."

What is really meant by this clause, remains unclear: Can the Member States substantially derogate from the regulation's standard? The wording of Article 82 ("within the limits of this regulation") suggests otherwise. But if this is true, what is Article 82 good for? Does it merely express a request?

Moreover, the utility of an opening clause can be justly questioned. One of the major shortcomings of the current framework is less the substantive law – the balance of interest allows adequate and above all flexible solutions – but rather its disparate implementation and application throughout the Union.

In particular the administrative practices of the national supervisory authorities competent for the application are so far not effectively harmonized. This is a serious flaw: As the field data protection is particularly dependent upon efficient enforcement by state agencies,[46] the administrative practice significantly determines the practical application of the substantive data protection rules. The existence of independent supervisory authorities is an essential component of the protection of individuals with regard to the processing of personal data.[47] The current consultation process within the framework of the Article 29 working Party (WP), while producing helpful input and guidelines, cannot set mandatory standards and enforce them. It is even less capable to overrule individual decisions by national supervisory authorities. The general lack of cohesion is aggravated by structural weaknesses of some supervisory authorities which lack financial and personnel resources

---

[45] 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) 11 final, available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (as at April 14th, 2014).

[46] Cf. BVerfG, 15th December 1983, case 1 BvR 209/83 et. alia.

[47] CJEU, 16th October 2012, Case C-614/10, para 37 (Commission ./. Austria).

to properly discharge their mission.

The Commission now tries to tackle that problem by strengthening the supervisory authorities and ensuring harmonization of their practice:

- The proposed regulation's provisions on structure, duties and competences of supervisory authorities are far more detailed than currently (cf. Articles 46-54 of the proposed Regulation).
- The supervisory authorities are given broad powers to levy fines against offenders (Article 79) and powers of investigation (Article 53).
- A new and potentially very powerful consistency mechanism is introduced to ensure the uniform application of the regulation.[48]

These measures combined have the potential to achieve a unification of the administrative practices. Therefore the call for more harmonization is rightly one of the Commission's major selling points for the proposed Data protection regulation.[49] The hope of a truly harmonized data protection framework has in particular led business, on the whole, to speak out in favor of the reform.

Certainly the benefits of a better harmonization would be enormous. However, it would be a heavy blow indeed if the harmonization would not extend to the field of employee data processing. The latter is one of the more burdensome hurdles to working in several member states.

Article 82 could therefore call the entire reform package into question. This may be an exaggeration as most likely its impact is very limited as any legislations would have to be "within the limits of the regulation". In any case, its exact meaning should be clarified at least.

Another questionable novelty is the approach the regulation takes towards the employee's consent as a possible justification for a processing operation. Under the regulatory framework as proposed by the Commission, the employee's consent may be too restricted to be of any practical use.

IX. List of important cases

1. The mother of all data protection cases: The Census verdict of the Federal Constitutional Court[50]

What is the case about?

In 1982, the German federal parliament (Bundestag) passed an Act on a population census to be conducted in the following year. This brought on a huge societal debate about the data protection risks and the usefulness of the population census. Most of the arguments of the opponents focused on data protection problems. There were fears that the

[48] For more detail see Gregor Thüsing and Johannes Traut, The Reform of European Data Protection Law: Harmonisation at Last?, in:, Intereconomics, Vol. 48, No. 5, September/October 2013, p. 271.

[49] European Commission, "How will the EU data protection reform strengthen the internal market", available at http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/4_en.pdf and "Why do we need an EU data protection reform?", available at http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf (as at April 14th, 2014).

50 BVerfG, 15 December 1983, case 1 BvR 209/83 et al.

data could be linked back to the individuals, as there were more than 160 questions to be answered in the questionnaire. In addition, the forms contained code numbers and were to be kept for a considerable length of time. The data was to be collected, under the supervision of local authorities, by 600.000 collectors. The data was not only to be used for statistical purposes, but also for comparison with and correction of resident registers.

The Court held:

In this decision, the court developed the legal meaning of the citizens' fundamental right of informational self-determination as a part of the general right of personality as laid down in Article 2 and Article 1 of the Grundgesetz (Basic Law, i.e. the German Constitution). The general aim of the population census was upheld, but the judges demanded further procedural safeguards to protect this right. Additionally, the data transfer to the local authorities was considered to be unconstitutional as it blurred the boundaries between data collection for anonymous statistical purposes and the processing of personal data by those authorities. In developing the fundamental right of informational self-determination the court laid the foundations of both constitutional and sub-constitutional German data protection law.

2. Telephone surveillance I (Federal Constitutional Court)[51]

What is the case about?

The constitutional complaint concerned the authority of the Bundesnachrichtendienst (Federal Intelligence Service) to monitor, record and evaluate telecommunications traffic and to transfer the obtained data to other public agencies. Under the challenged legal provisions, monitoring was permissible in two forms: "Monitoring of Individuals" (Section 2 of the so-called G 10 Act) and "Strategic Surveillance" (Section 3 of the G 10 Act). The complainants questioned whether these regulations were compatible with Article 10 of the Basic Law that guarantees the "Privacy of correspondence, posts and telecommunications" as a fundamental right.

The Court held:

Article 10 of the Basic Law not only provides protection from the state taking note of telecommunications contacts. Its protection also extends to the procedures by which information and data are processed following permissible acts of taking note of telecommunications contacts, and it extends to the use that is made of the obtained knowledge. Furthermore, Article 10 of the Basic Law obliges the Federal Intelligence Service to take precautionary measures against the dangers which result from the collection and utilisation of personal data. These precautionary measures include, in particular, that the use of obtained knowledge be bound to the objective that justified the collection of the data in the first place. The court also decided that the competence of the Federal Intelligence Service under Section 1 and Section 3 of the G 10 Act to monitor, record and evaluate the telecommunications traffic for the timely recognition of specified serious threats to the Federal Republic of Germany from abroad and for the information of the Federal government is, in principle, consistent with Article 10 of the Basic Law. The transfer of personal data that the Federal Intelligence Service has obtained from

[51] BVerfG, 14 July 1999, case 1 BvR 2226/94 et al.

telecommunications monitoring for its own objectives to other government authorities is consistent with Article 10 of the Basic Law; it must, however, comply with the following prerequisites: (1) the data is necessary for the receiving agency's objectives; (2) specific requirements placed on changes of objective are met; and (3) the statutory thresholds for transfer comply with the principle of proportionality.

3. Online searches and reconnaissance of the Internet (Federal Constitutional Court)[52]

What is the case about?

This case dealt with the "North-Rhine Westphalia Constitution Protection Act". As a reaction to international terrorism and organized crime, this Act enabled the police and other public authorities to use software for secret access to information technology systems ("online searches" through so-called Trojan horse software and other forms of spyware) and reconnaissance of the internet.

The Court held:

The Constitutional Court held that the provision on "online searches" violated the general right of personality (Article 2 and Article 1 of the Grundgesetz) in its particular manifestation as a fundamental right to the guarantee of the confidentiality and integrity of information technology systems, and that the Act was null and void. The provision in particular does not meet the requirements of the principle of proportionality. In view of the gravity of the encroachment, the secret infiltration of an information technology system by means of which the use of the system can be monitored and its storage media can be read is constitutionally only permissible if factual indications exist of a concrete danger to a predominantly important legal interest. What is more, the encroachment is in principle to be placed under the reservation of a judicial order.

The Court also held that also the empowerment to secret reconnaissance of the Internet violates the constitution. The secret reconnaissance of the Internet encroaches on the secrecy of telecommunication (Article 10 of the Basic Law) if the authority monitors secured communication contents by using access keys which it collected without the authorisation or against the will of those involved in the communications. Such a grievous encroachment on fundamental rights is, in principle at least, also conditional on the provision of a qualified substantive encroachment threshold. This was not the case in the relevant provision of the challenged Act. The provision permitted intelligence service measures to a considerable degree in the run-up to concrete endangerment without regard to the grievousness of the potential violation of legal interests, and even towards third parties. What is more, the provision did not contain any precautions to protect the core area of private life.

If, by contrast, the state obtains knowledge of communication contents which are publicly accessible on the Internet, or if it participates in publicly accessible communication processes, in principle it does not encroach on fundamental rights.

[52] BVerfG, 27 February 2008, cases 1 BvR 370/07 and 1 BvR 595/07.

4. Search of the employee's locker (Federal Labour Court)[53]

What is the case about?

The employer was running a wholesale market. The plaintiff was one of his employees. The employer suspected the employee of stealing lingerie from the market. Without the employee's permission, the employer secretly opened a locker that was used by the employee for storing personal items, and found ladies underwear in the locker.

The Court held:

Opening and searching the locker was illegal under Section 32 BDSG. The purpose (fighting theft) was legitimate, but the secret opening of the locker violated the principle of proportionality as it was not necessary in order to pursue this legitimate aim. It would have been sufficient if the employer had opened the locker after informing and in presence of the employee. The BAG also held that the information obtained from this illegal search could not be used as evidence in a subsequent dismissal protection case.

5. The video surveillance / CCTV cases of the Federal Labour Court

What are the cases about?

There are many data protection cases on video surveillance. Even before the relevant provisions of the BDSG entered into force (Section 32 BDSG was added to the BDSG in 2009), the BAG had already established the major principles of the law.[54] The legislator merely codified this case law. Many of the cases dealt with CCTV installations in supermarkets[55] or similar shops.[56]

The Court held:

Substantiating the proportionality test in all individual cases, the BAG held that before installing CCTV devices, there have to be sufficient reasons for suspicion (for example an unsolved theft), which justify the surveillance. Some vague assumption or a general suspicion with respect to all employees is not sufficient. In principle, video surveillance has to be carried out openly rather than secretly. Secret surveillance is only acceptable as an *ultima ratio*, in order to protect the employer from grave violations of his interests (e.g. theft or other criminal activities). If these conditions are met, information gathered by means of secret surveillance techniques can be admissible in dismissal protection cases. In this context, Section 6b (2) BDSG, that prescribes the use of warning signs, has to be interpreted as a procedural provision that does not hinder the use of such information in lawsuits.

[53] BAG, 20 June 2013, case 2 AZR 546/12.
[54] The leading case is BAG, 27 March 2003, case 2 AZR 51/02.
[55] BAG, 21 June 2012, case 2 AZR 153/11.
[56] A recent case was about video surveillance in a liquor/beverages store: BAG, 21 November 2013, case 2 AZR 797/11; cf. also BAG, 27 March 2003, case 2 AZR 51/02.

6. Data processing on the basis of an employer/works council agreement (Federal Labour Court)

What is the case about?

According to Section 77 *Betriebsverfassungsgesetz* (Works Councils Act, BetrVG), the employer and the works council – a shop level representative body elected by the employees – may enter a *Betriebsvereinbarung* (works agreement) that is, in principle, binding for the employer and for all the employees of the respective enterprise. These works agreement are an "other legal provision" in the meaning of Section 4 (1) BDSG and they may therefore justify the processing of data (see above).

In a 1986 case,[57] the BAG had to decide whether the parties to a works agreement were allowed to agree upon terms and conditions of the processing of data that were disadvantageous to the employees in comparison to the rules of the BDSG.

In this case, a works agreement regulated the use of telephones of the employer for private purposes by the employees. The employees were allowed to use the telephones for private purposes, but they had to pay for it. The agreement entitled the employer to process the telephone numbers dialled as well as the time and the length of the connections, so that he was able to calculate the fees owed by the employees and to combat fraud.

The works council later argued – for reasons that are of no importance here – that the agreement was illegal as it *firstly* violated fundamental rights of the employees and as it *secondly* contradicted the rules of the BDSG.

The Court held:

The BAG rejected the first argument. Considering the second argument, it held that the potential content of a works agreement was not limited by the BDSG. If the agreement was an "other legal provision" in the meaning of Section 4 (1) BDSG, it was – according to the judges – not limited to substantiating the rules of that act. Instead, the parties were free to agree upon terms and conditions for the processing of data that were disadvantageous to the employees compared to the rules of the BDSG. Limitations to the freedom of the parties to agree upon such terms and conditions were to be derived from the constitution and sub-constitutional mandatory law (not including the BDSG) only. Although the court upheld this position in a 1995 decision, it is highly contested in the contemporary debate.[58] However, in 2013, the BAG upheld the earlier decision again and repeatedly stressed that a works agreement was an "other legal provision" in the meaning of Section 4 (1) BDSG and to be valid, it had to be proportionate to be compatible with fundamental rights only.[59]

[57] BAG, 27 May 1986, case 1 ABR 48/84; upheld by BAG, 30 August 1995, case 1 ABR 4/95.
[58] For details, see Gregor Thüsing, Arbeitnehmerdatenschutz und Compliance (2010), paras. 99 – 116.
[59] BAG, 9 July 2013, case 1 ABR 2/13 (A).

X. Enforcing data protection law: Important supervision and advisory bodies

1. The Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI)

The BfDI's key task is to control other public authorities, see Section 24 BDSG. The public authorities may also seek the BfDI's advice in data protection matters, see Section 26(3) BDSG. The BfDI also supervises and controls the execution of the Law on Prerequisites and Procedures for Security Clearance Checks Undertaken by the Federal Government (Security Clearance Check Act, Sicherheitsüberprüfungsgesetz, SÜG). This law governs the prerequisites and the procedures for carrying out a security check on a person who is to be assigned to a security-sensitive type of employment (e.g., the Secret Service).

The BfDI does not enforce the rules on data protection vis-à-vis private companies, because this is done by local enforcement authorities of the different German States (the Länder).

The BfDI represents Germany within the Article 29 Working Party.

2. The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI)

The BSI investigates security risks associated with the use of IT and develops preventive security measures. It provides information on risks and threats relating to the use of information technology and seeks out appropriate solutions. This work includes IT security testing and assessment of IT systems, including their development, in co-operation with industry. Even in technically secure information and telecommunications systems, risks and damage can still occur as a result of inadequate administration or improper use. To minimise or avoid these risks, the BSI's services are intended for a variety of target groups: it advises manufacturers, distributors and users of information technology. It also analyses development and trends in information technology.

The BSI also warns the public if it is aware of internet-related criminal activities that could affect larger groups of consumers. For example, the BSI provides help to victims of identity theft and identity fraud.

3. The Data Protection Working Party established by Article 29 of the EC-Data Protection Directive

The Working Party is a key player in European Data Protection Law. In addition to advising the European Commission, one essential task of the Working Party is to advance harmonisation of data protection within the European Union. As a general rule, the group meets five times per year for two-day sessions in Brussels, and subgroups support its work. Until the end of 2005, it has adopted more than 100 opinions. In the past years, subgroups were actively dealing with subjects like Internet, passenger data and binding corporate rules.

4. The European Data Protection Supervisor (EDPS)

The EDPS is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. He does so by supervising and monitoring the EU administration's processing of personal data, advising on policies and legislation that affect privacy, and cooperating with similar authorities to ensure consistent data protection. The supervision of other EU bodies takes various forms. The bulk of it is based on notifications of processing operations presenting specific risks. These need to be prior checked by the EDPS. Based on the facts submitted to him, the EDPS will examine the processing of personal data in relation to the Data Protection Regulation (Regulation (EC) No 45/2001). In most cases, this exercise leads to a set of recommendations that the institution or body need to implement so as to ensure compliance with data protection rules.