RECOMMENDATIONS ON THE REGULATION OF TECHNICAL CONTROL AND SURVEILLANCE IN THE EMPLOYMENT CONTEXT IN GERMANY

AUTHOR

Dipl.-Jur. Falk Hagedorn

The Project is co-funded by the European Union's Fundamental Rights and Citizenship Programme

DECEMBER, 2012

Content

<u>Note:</u> The EU project 'Privacy at Workplace'[1] has supported the elaboration[2] of these proposed regulations. They are based on the 'Universal Code of Conduct on the Protection of Personal Data Acquired through Monitoring by Technical Means in [the] Employment Context' and have been adapted according to German Law.[3] In this way they do not claim to be complete, but serve rather as ideas for drawing up agreements between works committees and management[4] or generally as internal guidelines which apply to employee data protection and especially to the issue of the control and surveillance of employees.[5] The user is obliged to observe all developments – and especially those relating to the Data Protection and the Labour Law – at all times and to implement them by means of his own rules and regulations. It is recommended that a specific contact person – a referee – be nominated and that this person be given sufficient authority to ensure the correct use of employees' personal data. In this way the position and responsibilities of the person charged with data protection are unaffected.

1. Background, Objectives of the Agreement

1.1.

The continuous changes in Information Technology necessarily produce changes also in the in the world of work – and hence in the regulations which were drawn up in respect of employees' personal data. The use of up-to-date and efficient ICT (Information and Communication Technology) in business has thrown up a multitude of questions, which to date have not been clarified at the appropriate level – or inadequately so. Apart from a very few, sector-specific rules, the protection of employees' personal data is currently missing from Germany's general law such as, perhaps, Data Protection Law (BDSG), the Telecommunications Law, the Tele-media Law and the Works Council Constitution Act (BetrVG). Due to the lack of law and to the consequent growing need for regulation and improvement, there exists, as earlier, the practical need on the one hand, to protect, the personal rights of the employee and, on the other hand to maintain the rights of the employer.

---

[1] Further information on the Project is available at http://www.pawproject.eu

[2] Author: Dipl.-Jur. Falk Hagedorn, Scientific Staff member Institute for Economic Law at the Georg-August-University, Göttingen, Dept. of Prof. Dr. Wiebe, LL.M. (Civil Law, Competition- and Intellectual Property Rights, Media- und Information Law).

[3] The rules of the Universal code of conduct on the protection of personal data acquired through monitoring by technical means in employment context were partly created with reference to the 'ILO Code of practice on the protection of worker's personal data" and also, especially, according to the requirements of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[4] One regulation involving House Agreements is offered, since the employer and the Works Council according to § 75 Para. 2 p.1 of the BetrVG a duty of care applies, which requires the free development of the personality of the employee to be demanded and protected.

[5] In companies where there is no Works Council, the employer must otherwise ensure the adequate consideration of the rights and interests of the employee in relation to any processing or use of his personal data.

1.2.

With this background the agreement aims to create appropriate conditions for the private economy, in respect of the use of modern ICT in already existing situations or in imminently difficult work-related situations where an equitable settlement is desired.

Accordingly, the following regulations are aimed firstly at protecting the employee against the illegal processing or use of their personal data. For the rest, the interest of the employer should also be acknowledged.

The agreement creates of framework for a Data Protection Management System (DPMS) which enable employers to make processing or use of personal data within the employment context. At the same time this framework within the enterprise should ensure a verdict of compliance in respect of any audit and certification process for the employer's DPMS in accordance with the principles of the Universal Code of Conduct on the Protection of Personal Data Acquired through Monitoring by Technical means in an Employment Context.

The agreement takes into account the fact that, whilst the parties to the contract of employment face each other as legally equal contractual partners, in fact, the employer, largely due to his greater economic and structural weight enjoys a position of superiority. In view of earlier, later and ongoing data scandals, the agreement focuses in particular on framework conditions for creating monitoring and surveillance measures in the employment context.

The Agreement should serve as a good basis for supporting a climate of trust in the workplace between employer and employees and to ensure industrial peace. Accordingly, with the use of ICT, the desired aims should always be realised by cooperation between the employers' and employees' sides. With such cooperation the interests of all parties should be considered fairly and equitably.

2. Scope of application

2.1. Territorial scope

This agreement applies to the scope of the BetrVG in the whole of *[Company Name]*.[6] Similarly it applies to the use of ICT inside and outside the works premises.

2.2. Objective scope

This agreement and its provisions lay down universal and binding standards for the use of ICT in the workplace and, through this, related issues of monitoring and surveillance in the sphere of employment. It lays down basic rules for the development, introduction, application and

[6] Insert name and legal status of the enterprise.

further development of ICT, which may affect the personality rights of employees.[7] The principles are also valid for data in printed form.

2.3. Personal scope [8]

This agreement and its Annexes apply to all employees in *[Company Name]*[9] of the BetrVG. The company will certainly arrange that the senior executives are informed of the agreement and of its Annexes and observe the standards which are laid down in them. The company will have the details of the contents of the agreement etc. as well as the obligation to observe and maintain the standards laid down therein in writing.

3. Definitions

Definitions in respect of this agreement are clarified in Annex I.

4. General Principles

4.1.

In the use of employees' personal data the general principles of the law on data protection are to be observed, and in particular the following principles are to be respected:

1) Prohibition with permission reserved;
2) Direct collection of data;
3) Economical use of data;
4) Data avoidance;
5) Transparency;
6) Purpose limitation;
7) Necessity.

An explanation of the principle, together with statements concerning the guarantee of comprehensive personal data protection for employees will be found in Annex II.

4.2.

The employer must provide the basic requirements of the data processing system and in this connection the following specific points must be included or observed:

---

[7] It is recommended that the principles laid down in the agreement should be applied as the basis for the ideal use of an employee's personal data.

[8] Simplified verbal terms such as employee refer equally both to men and women

[9] Name and legal status of the enterprise to be inserted.

1) A clear description of the system used
2) Transparent, full and complete documentation concerning the system used and
3) Full and complete confirmation of the right of access and of any interfaces with other systems

5. The legal basis for the processing or use of employees' personal data; special types of personal data; the burden of proof

5.1.

Personal data of employees should only be processed or used on clear legal grounds.

5.2.

The processing or use of special forms of personal data in the sense of Annex I. Point 2 requires a special examination and analysis of the legal basis.

5.3.

The employer bears the burden of proof of the need to use data and its legal basis.

6. Special requirements for the consent of the employee

6.1.

The informed consent according to §§ 4, 4a of the Federal Data Protection Act concerning the personal data of employees is legitimate if the decision of the employee has been made freely. In this sense free will is accepted if the consent is not made under any form of pressure. The criterion of free will must be demonstrated under employment conditions and in particular by detailed examination if the power relationship is unbalanced.

6.2.

To protect the employee, the employer can process or use the data only with the consent of the employee and provide that the requirements laid down are strictly observed.

1) Before the employee agrees, the competent Works Council must be fully informed of the concrete facts of the case and that the employee has clearly consented to the employer's request for his agreement.

2) The employee must, before giving his unambiguous[10] consent, be advised that the consent is voluntary[11] and that he can withdraw it later without giving reasons and without being threatened by negative consequences.
3) The employee must be informed appropriately before he gives his consent[12]
4) The employee must be given a genuine opportunity to refuse his consent.
5) The consent must be given in writing.
6) Clarification to the employee of the significance of his consent, the voluntary nature of which and the possibility to withdraw it are to be recorded together with the detailed facts of the matter.

7. The purpose of the processing or use of data

7.1.

Before any personal data is collected, the purpose of its processing or use and treatment must be clearly formally and finally defined. Further arguments concerning possible purposes are to be found in Annex III. Employees and those representing their interests are to be informed suitably about the purposes of processing or use the data. To enable the evidence to be preserved the purposes of processing or use the data must be recorded.

7.2.

Insofar as a regulated operation or process is being conducted, the aims and purposes must be provided.

7.3.

The purposes must be

1) in accordance with legal principles and
2) subject to the best possible protection of the personality rights of employees.

7.4.

If specific tasks are to be carried out or done, employees' personal data can only be processed or used if the processing or use are clearly legitimised before the data are retrieved.

[10] Unambiguous in the sense that there can be no doubt of the existence of the agreement and of its content.
[11] This means that the employee must be aware from the statement of his consent, that he is not compelled to give his data and, accordingly, can refuse his consent. In particular there is no free will involved, if the employee misled or compelled, if social pressure was applied or his refusal to consent was to his disadvantage.
[12] The content and scope of the information depend on the actual reason for its use.

7.5.

The retention of personal data relating to employees in stock is prohibited.[13]

7.6.

Special limitations relating to purpose[14] are to be observed in processing and use of personal data relating to employees.

7.7.

The personal data of employees are to be cancelled if the specific purpose no longer applies.

8. A narrow interpretation of the principle of purpose limitation

8.1.

The principle of purpose limitation should be interpreted narrowly.

8.2.

Each concrete processing or use of employees' personal data must have a clearly documented purpose associated with it. If any doubt existed as to whether the purpose matched the envisaged use, then the data must be put aside.

9. Change of purpose

Any subsequent change in purpose is basically prohibited. Possible exceptions in respect of this could be possible however, if

1) this was required subject to data protection legislation,
2) interest representative parties were to participate and collective law processes were to be employed and
3) the employees concerned were informed[15] in writing about the change of purpose.

[13] Cf. basically Federal Constsutional Law 65, 1, 46.
[14] Cf §§ 31 und 39 of the Federal Law on Data Protection (BDSG).
[15] The written form can be by means of e-mail.

The previous information concerning the employee in question is dispensable, if the change the purpose serves a legally permitted internal full statement of facts and if the previous information would endanger the success of the process. The employees must be informed about the data processing as fast as possible after the facts being presented.

10. Obligation of separation

10.1.

Employee-related personal data collected for different purposes, are totally separate according to the actual purpose of collecting, processing and use of data.

10.2.

The data controller must by appropriate technical organisation and organisational measures[16] ensure compliance with the provision of 10.1.[17]

11. Obligation to provide information

11.1.

Regarding the protection of their personality rights in the employment context, the employer provides all employees with adequate and regular information that takes into account any current developments.

11.2.

This information shall include in particular the introduction or modification of computer-related rules of conduct, control and monitoring potential of the employer, as well as provisions in terms of collective rights. The parties shall agree upon the selection of an

[16] To the field of special data protection legal requirements belongs the arrangement of the internal organisation cf. in general § 9 S. 1 of the Federal Law on Data Protection (BDSG) together with the appendix. § 9 S. 1 BDSG specifies the security and protection requirements of the Federal Law (BDSG). According to S 2 of the appendix § 9 S. 1 BDSG especially those measures should be observed which in their various ways suit the personal data to be protected or categories of data to which access is controlled, as are transmission, input, order, availability and the division of Authority. Also to be observed that according to § 9 S. 2 of the BDSG (Federeal Data Protection Law) measures are only necessary if their cost is reasonable when considering their relationship to the target protective purpose.

[17] Observing the obligation of separation can perhaps be ensured by saving data on different servers or also by logical separation. In this way the type of data saved defines, what form of division is rational and appropriate. To avoid confusion with other sets of data, highly sensitive data should, as a general rule, be handled by its own server.

adequate information medium (e.g. information per Intranet or corporate information booklets).

11.3.

The employer shall be obliged to disclose to the employees an annual comprehensive overview of systems and processes, in which/through which personal data is processed or used.

11.4.

Before carrying out control and surveillance measures, employees are to be informed about this in good time and thoroughly in a linguistically appropriate (especially a clear and comprehensible manner). The obligation of the company to provide information extends in particular to the following information:

1) Purpose of and reasons for the measure
2) Duration and scope of the measure
3) Applied methods and technology used
4) Type of data collected and duration of its storage
5) Planned further data processing and use, and
6) Rights and obligations in connection with the measures.

11.5.

Violations with relevance to the protection of personality rights in the employment context are immediately to be reported to the employee. Corresponding documents shall be made available to the employee at his/her request. This shall not affect the provisions regarding the protection of confidential information. If serious harm to the rights or legitimate interests of employees threatens, the employer must also immediately inform the competent supervisory authority of this. § 42s sentences 3-4 and 6 of the Federal Data Protection Act must be applied accordingly.

12. Covert measures (secret monitoring)

12.1.

Covert measures for the control and surveillance of employees[18] have a particularly high intensity of intervention, and even in the case of their legal admissibility these should be taken into consideration only as ultima ratio.

12.2.

Covert measures may be permitted under highly exceptional circumstances, when

1) a concrete, documented[19] criminal offence or other serious breach[20] in connection with the employment is specifically suspected,
2) less drastic means to allay suspicion have been exhausted,
3) the covert measure is practically the only means that remains, and
4) the covert measure is overall proportionate.[21]

12.3.

The processes, tools and methods necessary for this are to be selected and arranged by taking into account the representation of interests. In particular, it must be ensured that the covert measure takes place only for a pre-determined, and suitable period of time The evaluation of the relevant data must be done by a third party who was involved neither in the decision-making to undertake a covert measure, nor in its implementation.

12.4.

If the concrete suspicion is not confirmed within the meaning of Section 2 Nr. 1, any data obtained through the covert measure must be immediately deleted.

---

[18] E.g. covert video surveillance. In individual cases, the admissibility of covert measures is controversially debated. For the purposes of exemplary employee data protection such measures should be preferably avoided.

[19] The suspicion must be sufficiently concrete in personal, spatial and functional terms.

[20] In § 32 section 1 sentence 2 of the Federal Data Protection Act the law governs only the prosecution of concrete suspicion ("to detect criminal offences"). According to prevailing opinion, § 32 paragraph 1 sentence 1 of the Federal Data Protection Act serves as the legal basis for measures (usually suspicion independent) to prevent crimes related to the employment relationship (so-called anti-corruption measures). Purely preventive measures are subject to data protection implementation risks and should be carefully reviewed for their legal admissibility. It is strongly recommended to coordinate the further procedure with the relevant supervisory authorities and to make such dependent on their requirements.

[21] See regarding video surveillance fundamentally BAG, NZA 2003, 1187, 1193.

12.5.

The employees must be informed about the general possibility to use covert measures for the control and surveillance of employees. The employees concerned must be informed about the concrete measures as soon as possible.

13. Security aspects

13.1.

The employer must ensure the information security by adopting such appropriate technical and organisational measures[22] that provide for the required level of confidentiality, availability and integrity of data to be processed or used in the company.

13.2.

For this purpose, the employer must implement in particular an information security management system (ISMS). The ISMS is used to permanently define, manage, control, maintain and continuously improve the information security. The requirements of the production, implementation, operation, monitoring, maintaining and improving a documented ISMS are to established across the entire organisation by taking into account the IT risks.[23]

13.3.

It is the employer's responsibility to specify such processes and procedures[24] for the handling of the personal data of employees that comply with the relevant legislation.[25]

---

[22] Cf. § 9 sentence 1 of the Federal Data Protection Act together with its appendix recital 16.

[23] Regarding this in general, see "Information Security Guidelines - IT basic protection compact" of the BSI, at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile). See also the general requirements of an ISMS such as the IT basic protection standards of the BSI. (available at: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html) or the BITKOM and DIN-compass for IT security standards, "compass of IT security standards - guideline and reference book", 4th edition (available at: http://www.nia.din.de/cmd?level=tpl-artikel&languageid=de&cmstextid=kompass).

[24] E.g. four-eye principle used as organisational measure. This principle aims to reduce the risk of errors and abuse. For this purpose, in all cases more than one person is involved in the major decisions and critical activities, rather than centralising competence in a single person. Regarding this, see https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m04/m04129.html https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden_IS-Revision-v2_pdf.pdf?__blob=publicationFile.

[25] Other possibilities include role- and authorisation concepts, the establishment of protection needs, risk analyses, and provisions for data protection.

14. Data secrecy, education and training

14.1.

Employee's personal data must be kept confidential. They are subject to the data secrecy provision (§ 5 of Federal Data Protection Act), which prohibits those employed in data processing the unauthorized use of personal data (§ 5 sentence 1 of Federal Data Protection Act). Persons employed in the data processing are, after appropriate instruction upon starting their activity, required to keep the secrecy of data (§ 5, sentence 2 of Federal Data Protection Act) and to be trained according to § 4g paragraph 1 sentence 4 No.2 of Federal Data Protection. The obligation to maintain data secrecy shall be maintained even after terminating their activity (§ 5 sentence 3 of Federal Data Protection Act).

14.2.

The obligation must be preceded by suitable and appropriate training. The training is designed to obtain a goal-oriented professional qualification by the workforce. In addition to general data protection law and labour law knowledge it is aimed particularly at knowledge about the legal use of employee's personal data. In any case it must be ensured that the training provides extensive knowledge regarding the control and supervision of employees.

14.3.

Before the case of need arises, the employer must develop specific training measures and inform the works council about these. If, and to the extent to which it is necessary, the employer and works council must vote for a training concept.[26]

14.4.

The working hours required for participation in training should be authorised for the employees. If possible, the training must take place during the regular, normal working hours. Costs necessary for participation in training must be borne by the employer.

[26] The content of a qualification concept may include among others: course objectives, core contents, participants, dates and place of the qualification measure.

15. Documentation of the data processing and use

15.1.

The employer must have the processing and use of employee's personal data comprehensively documented. Here too, he ensures that a list of all data controllers and systems is created, and where and by means of which personal data will be used. This list will be supplemented with additional information[27] to ensure procedural rules.[28]

15.2.

The procedural rules must be managed in a way that allows everyone to inspect it in.

16. Audit

16.1.

To ensure the legal compliance of the processing and use of personal data of employees with the requirements of this agreement, IT processes, which are relevant in terms of employee data protection, are regularly audited. Similarly, measures that can in this regard ensure and to improve the level of protection sustainably, will be reviewed. The employer shall draw up a detailed report to enable and support the evaluation of legal compliance.

16.2.

To avoid conflicts of interest, audits are preferably carried out by an independent third party who has the necessary technical expertise.[29] Alternatively, internal audits can be done, if the employer ensures that privacy audits are carried out by an independent and autonomous institution, which has the necessary technical expertise.[30] In both cases, the selection has to be made by the joint agreement of the parties at the workplace.

---

[27] Type of the stored data, purpose of the processing or use, access authorisations etc.

[28] The practical guideline of BITKOM can assist the drafting: http://www.bitkom.org/files/documents/BITKOM_Verfahrensverzeichnis_V_2.0.pdf).

[29] In particular, it should be ensured that the third party is a certified specialist auditor (certification according to ISO/IEC 27001), who can show in-depth knowledge regarding the use of personal employee data.

[30] Regarding the requirements see recital 29.

16.3.

The outcome of each audit is recorded in an audit report and made permanently available to the parties at the workplace. Specifically, the audit report must deal with and discuss extensively at least the following points:

1) Actual state of the level of data protection;
2) Risk evaluation regarding this;
3) Indication of any gaps in protection and / or improvement potential; and
4) Implementing measures derived from this, with a time schedule (measurement plan).

17. Rights of the employee

17.1.

Every employee shall, as provided by § 34 of the Federal Data Protection Act have the right to information and explanations regarding all his/her stored personal data (the right to information). The employer shall designate a contact person for this. The right of employees to inspect the files remain unaffected by the right to information.

17.2.

Pursuant to § 35 of the Federal Data Protection every employee has a right to rectification, erasure or blocking of his/her personal data.

18. Participation right of the works council

18.1.

Through appropriate process structuring the employer shall ensure that the works council exercises its participation rights fully and as early as possible.[31]

18.2.

Here, he must pay particular attention to ensure the exercise of co-determination rights when introducing and applying information and communication technology for the purpose of control and supervision of employees.

[31] According to the BetrVG, the works council disposes over - depending on the underlying issue - different participation rights (see especially § § 81 paragraph 1 No. 1, 87 para 1 No. 6, 94 WCA). These rights must be granted also in the context of employment. (cf. § 32 para. 3 of Federal Data Protection Act).

19. Infringements, interpretation of the agreement

19.1.

If a competent works council alleges any infringement of this agreement, it is the employer's responsibility to rebut this. The final determination of whether there is an infringement shall be established by an *[independent Arbitration Committee]*.[32]

19.2.

If an infringement is detected, it must be stopped immediately. Infringements of this agreement caused by any activity or omission[33] will be sanctioned with individual work-related contractual consequences. This also applies to responsible managers, provided that what their activity or omission has contributed to the infringement. Regarding other consequences of any proved infringement to be represented by the employer, the aforementioned *[independent Arbitration Committee]* decides.[34]

19.3.

The undersigned parties agree to start negotiations immediately in the case of any dispute regarding the interpretation and application of this agreement with the objective of reaching an amicable settlement. In case of doubt the provisions of this agreement shall be interpreted in terms of a privacy-friendly processing or use of personal data. If no agreement is reached on individual issues, the issue shall be referred to the aforementioned *[independent Arbitration Committee]*.[35]

20. Severability Clause

20.1.

Should any provision of the present Agreement or part thereof be or become invalid or unenforceable, or should the agreement contain a regulation gap, the validity of the remaining provisions in this agreement shall not in any way be affected or impaired.

---

[32] Insert designation. If not available, it is recommended to set up preferably a company, independent arbitration committee to resolve disputes locally. The signatory parties should agree upon appropriate regulations (composition, rules of procedure, chairmanship by rotation, decision-making etc.).
[33] Tolerating an act is also considered as an omission.
[34] Insert designation.
[35] Insert designation.

20.2.

The undersigned parties undertake in such cases to replace the invalid or unenforceable provision or the regulation gap with a new provision, which best achieves the purpose of the invalid provisions in a legally valid way.

21. Entry into force, termination, validity, written form, Annexes

21.1.

This agreement shall enter into force upon signature.

21.2.

It can be terminated bilaterally with a three-month notice period at the end of the relevant quarter, although not before *[Date]*.[36]

21.3.

Until a new agreement is concluded, the provisions of this Agreement shall continue to apply.

21.4.

All Annexes specified in this Agreement form an integral part of the Agreement. Additions and changes to this Agreement must be in written form. This also applies to a waiver of the written form. This document contains three Annexes:

1) Annex I.Definitions
2) Annex II. Explanation of the general data protection principles, ensuring full employment data protection
3) Annex III. Statements on the purpose in the employment context

[Place, date, signatures of the Parties]

[36] Insert date.

Annex I - Definitions

Unless otherwise provided for in this Annex, the definitions of the BDSG (Federal Data Protection Act) apply in their current version.

1. *Personal data* means any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject). Personal employee information is information about personal or material circumstances of an identified or identifiable employee. Data shall be deemed as personal, if they can be clearly assigned to an employee or this assignment can be made at least indirectly (person-relatable data).

2. *Sensitive personal data* include information on the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual life

3. *Employees* are all natural persons who are employed by an employer. The term is to be broadly construed [37] and besides workers it includes inter alia also persons employed for the purpose of professional training, worker-like people, and candidates as well as persons whose employment is terminated.[38]

4. *Utilization* means any collection, processing and use of data.

5. *Automated utilization* means the use of personal data by means of data processing systems.

6. *Data retention* includes any processing or use of employees' personal data without finally determining the objective and purpose.

7. *Information and Communication Technology* means all technique in the field of Information processing and Communication.

8. *Control and surveillance* measures are those measures that provide for the use of information and communication technology for the purpose of controlling and supervising employees. Information and communications technology can be used e.g. for the control and monitoring of e-mails, the use of Internet and social networks, by means of optical-electronic devices (video surveillance), using access control systems (RFID, Biometric Matching System) and also outside of the business premises (GPS-/GSM-locating).[39]

---

[37] See more extensively the divergent understanding of the data protection, employment- and industrial relations law.

[38] Status of employees thus extends to all phases of employment (initial phase, implementation, termination phase). It should be noted that the underlying understanding of the term diverges depending on the special field of law (cf. the definitions in data protection law, social security law, labour law and industrial constitution law).

[39] See, regarding the protection of personality rights in the context of employment in detail *Hagedorn*, "Privacy at Work – Country Report Germany" (Status: June 2011), available at: http://www.pawproject.eu

Annex II - Explanation of the general data protection principles, ensuring the full employment of data protection

1. General data protection principles

When utilising the personal data of employees, the following principles must be adhered to:

a) *Prohibition with permission reserved* (§ 4 para 1 of Federal Data Protection Act)

The processing and use of personal data is basically prohibited. The only exception is if there is an express legal basis for the processing or use, or the employees have consented to the processing or use of their personal data.

b) *Direct collection of data* (§ 4 para 2 sentence 1 of Federal Data Protection Act, so called „open data collection")

Personal data shall be collected in principle from the employees themselves and with their participation. Exceptions to the principle of open data collection are possible if a legal provision requires other means of data collection or the data collection from the employee itself would require a disproportionate effort.

c) *Data avoidance and data minimisation* (§ 3a 1 of Federal Data Protection Act)

The processing or use of personal data and the selection and design of data processing systems must aim at using as little personal information as possible. In particular, employees' personal data must be anonymised (§ 3 para 6 of Federal Data Protection Act) or pseudonymised (§ 3 para 6a of Federal Data Protection Act), as far as this is possible according to the intended processing or use and does not require disproportionate efforts as compared to the desired protective purpose.

d) *Transparency*

The processing and use of personal data must be transparent for the employee. This requires knowledge of the structure of the data processing and use, data processing procedures, the technology used as well as the data streams. In other words, the employee should know that data is collected about him/her and what data and for what purpose, at what place and for what reason is stored. A secret data collection is basically prohibited and is only possible in exceptional cases under very strict conditions. The principle of direct data collection (see above), the employer's information requirements and the employee's information rights serve the establishment of transparency.

e) *Purpose limitation*

Every single processing or use of personal employee data must be based on a specific legitimate purpose. Employees' personal data can be basically processed or used only for purposes for which they were collected. Exceptionally it is allowed to change the purpose with the consent of the employee.

f) *Necessity*

The processing or use of personal employee data must be really necessary, i.e. it must be limited to the extent that is necessary. The characteristic of necessity is largely understood in the sense that proportionality must be tested. The test is necessary to take a subjective measure as basis, therefore it must take place regarding the specific case and in consideration of the specific circumstances. The concept of necessity is already highly controversial in the context of employment, due to which the processing or use of personal employee data should be particularly thoroughly examined in terms of necessity.

2. Ensuring comprehensive employee data protection

a) The employer must ensure compliance with the data protection principles in accordance with exemplary employee data protection. Here, he is committed to guarantee the protection of personal data of employees in all phases of employment (thus, from its conclusion until after its termination).

b) The employer is obliged to select candidates solely on the basis of such data that originate directly and personally from the candidate concerned.

In addition to the standard application documents such data may be used, which the candidate has made available for the employer for retrieval (e.g. setting data in a job fair) or delivered specifically to a recruiter for the purpose of forwarding the data to the employer.

The applicants must be informed about the circumstances of the use of applicant's data (automated use, enterprise-wide use, etc.) already in the job posting. The admissibility of the disclosure of applicant's data in ways other than those specified in the job posting is subject to the consent of the applicant. Regarding unsolicited job applications, applicants must be informed about the handling of applicant's data and must be given the opportunity to refuse to consent to the processing and use of their data and within a reasonable time. If a candidate is rejected, his documents must be immediately returned the applicant's data must be deleted immediately, unless the applicant agrees explicitly to a longer-term storage of his data for the purpose of any subsequent employment.

c) The employer shall be obliged to delete the personal data of employees who have left the company immediately upon termination of employment or dispose of such data in compliance with the Data Protection Act.

d) If legal requirements or contractual obligations to retain such data hinder the deletion of personal data, the data must be blocked for other purposes.

Annex III - Purpose limitation in the employment context

The use of employees' personal data is based mostly on clause § 32 of the Federal Data Protection Act.[40]

Thereafter, the use of data is possible either "*for purposes of the employment relationship"*, if this is necessary for a decision to consider the employment relationship, or, following such consideration, to implement or terminate the relationship[41] (§ 32 para. 1 sentence 1 of Federal Data Protection Act). In relation to the § 32 para 1 sentence 2 of the Federal Data Protection Act[42] specifies stricter requirements when the admissibility of the use of data "*to reveal criminal offences"*[43] is in question. This section applies both to criminal offences which are committed in connection with the employment relationship and those committed only when employment is possible.[44]

According to the legislator's intention, breach of contract or conduct contrary to the organisation's rules falls within the scope of § 32 Section 1 Sentence 1 of Federal Data Protection Act that governs other violations of the law.[45] According to § 32 paragraph 2 of the Federal Data Protection Act, the final paragraph regarding manual data processing also applies.[46] According to the explanatory memorandum, the principles of data protection in a workplace relationship are to this extent applied.[47] Through this, any data collection with respect to employees (e.g. records of managers and interviewers from applications and annual discussions with managers, as well as all notes regarding performance) fall within the protective scope of § 32 para 1 of the Federal Data Protection Act.[48]

Since many individual issues are controversial, it is generally extremely difficult to make a clear and reliable statement on the permitted uses in the context of employment. In any case, it is appropriate to review carefully the admissibility of measures introduced by the employer. This is especially true given that the control and monitoring potential of the employer is also

[40] For its competitors, regarding § 28 of Federal Data Protection Act see *Hagedorn*, a. a. O., pp. 19.
[41] Cf in general re the Data Protection principle of necessity Annex I Nr. 1 lit. f.
[42] According to its wording, the regulation is inspired by § 100 para. 3 sentence 1 of the Telecommunications Act (TKG); In terms of content, it meets the requirements specified by the Court regarding the covert surveillance of workers, Thüsing, NZA 2009, 865, 868 by drawing on *BAG*, NZA 2003, 1193 and NZA 2008, 1187.
[43] E.g. theft and cases of corruption, BT-Drs. 16/13657, page. 36. Regarding the question what the relationship between § 32 para 1 sentence 1 and sentence 2 of the Federal Data Protection Act was, see Franzen, RdA 2010, 257, 260 f.
[44] Deutsch/Diller, DB 2009, 1462, 1462.
[45] BT-Drs. 16/13657, S. 36; Schmidt, RDV 2009, 193, 195 regarding the problematic aspects of the regulation.
[46] See regarding the extension of the scope of application of the Federal Data Protection Act also § 8 para1 BewachV.
[47] BT-Drs. 16/13657, page 37 by drawing on BAGE 54, 365; 119, 238.
[48] Wank, in: ErfK for labour law, § 32 of Federal Data Protection Act, recital 2.

and largely subject to the extent to which the employer as the owner of the company's resources allows the employees to use the means of information and communication.[49]

It is strongly recommended to continuously develop, if necessary, the concept of the use of personal data and communication systems at the workplace. In order to protect the employees' personality rights, the use of technical monitoring devices should be restricted as much as possible.

[49] It should be noted in this context that the Works Council's right of co-determination does not tackle the question of permitting private use, LAG Hamm, NZA-RR 2007, 20, 21 f.; Ernst, NZA 2002, 585, 586; Lindemann/Simon, BB 2001, 1950, 1954.