DATA PROTECTION IN A NUTSHELL

What Employees Need to Know

STIFTUNG DATENSCHUTZ

INTRODUCTION

If you work with personal data in your company, practice or any other organization, you must be familiar with the basic rules of data protection and the essential obligations that result from them. This applies to members of management as well as employees in all areas and in a wide variety of employment relationships, even if you only occasionally work with personal data.

This brochure is intended to help you by presenting the most important points in an uncomplicated and practical way. We have deliberately refrained from listing the exact legal regulations – such detailed knowledge is only required by management, data protection officers and supervisors who work regularly and on a large scale with personal data. Their task is also to issue concrete work instructions for your company. This brochure is intended to supplement the company-specific data protection regulations.

By the way: Even though this brochure speaks throughout of “companies”, “supervisors” and “employees”, the instructions also apply to associations, unions, board members and other organizations and individuals.

---

hellmann
WORLDWIDE LOGISTICS

The English version was made possible by the kind support of Hellmann Worldwide Logistics.

WHICH LAWS REGULATE DATA PROTECTION?

The most important laws for data protection are the **European General Data Protection Regulation** (GDPR) and in Germany the supplementary **Federal Data Protection Act** (BDSG). Among many other materials, they are available on the information platform of the Stiftung Datenschutz on the implementation of the EU data protection reform at stiftungdatenschutz.org/DS-GVO-Info (most documents German only).

Since May 2018, the GDPR applies directly in all EU member states. These may have their own complementary regulations. For Germany, the old Federal Data Protection Act was replaced by a new Federal Data Protection Act. Among other things, this accompanying law contains **special regulations for the processing of employee data and for the payment assessment of debtors (scoring)**.

In addition, there are a large number of special data protection regulations in very different laws. For example in Germany, the duty of secrecy of medical personnel is regulated in the Criminal Code, the handling of letters in the Postal Act and the handling of health data in insurance companies in the Social Security Code V.

WHAT IS DATA PROTECTION NEEEDED FOR?

Data protection law enables the fundamental right that every person should be able to decide for him- or herself which of his or her personal data should be accessible to whom and when. Data protection should not protect the data itself, but always the person to whom the data relates.

The concern for a strong protection of personal information is countered by the right of the company to work economically with data. The data protection law regulates in which situation which of the two rights should prevail.

Personal data are processed at many places in the company: of course in the HR department (employee and job candidate data), but also in purchasing (suppliers), in sales (customers), in the IT department... This data may only be used for operational purposes. The management is obliged to issue the relevant instructions and to keep them up to date as well as instructing the employees about them and to obligate employees to confidentiality.

Many companies also appoint a data protection officer (a requirement in Germany, if they consistently employ at least 20 people dealing with the automated processing of personal data).

In the event of violations in the handling of personal data, there is a risk – in addition to the disadvantages for the people concerned – of claims for damages and fines; the company's reputation with customers, suppliers and the public can suffer lasting damage.

WHAT EXACTLY IS PERSONAL DATA?

Personal data are any information about a natural person that can be directly or indirectly attributed to that person.

- Directly attributable: Name, possibly function if, for example, there is only one IT manager in the company.
- Indirectly attributable: Personnel number, IP address

By the way: Personal data can also cover assumptions and presumptions. If a credit agency calculates the creditworthiness of a person with the help of a score value, this value is an assumption about the customer's solvency or willingness to pay or about the probability of a future credit default. Such assessments also belong to personal data.

In addition, there are special categories of personal data that are even more strictly protected: This includes data revealing ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic and biometric data, health data or data on sex life or sexual orientation of a natural person. There are special rules for the processing of such data; therefore, the handling of such data should not be considered further here. In any case, the processing of such special data should always be subject to the advice of experts.

WHO IS RESPONSIBLE FOR DATA PROTECTION AT WORK?

Once again: Everything that is said here about “companies” and “employees” also affects associations, foundations, public and community institutions and their employees, volunteers, interns, etc. in the same way.

THE COMPANY MANAGEMENT CREATES THE FRAMEWORK CONDITIONS

Employees shall not process data except on instructions from the company. Therefore, company management is required to provide accurate instructions for data handling. Without such an instruction, data may only be processed if there is a legal obligation to do so. In addition, supervisors should at all times be in a position to issue instructions relevant to data protection and answer questions.

THE EMPLOYEES CARRY OUT THE INSTRUCTIONS

Practical cases

- You process incoming job applications. Are you allowed to add data from social networks?
- You create a circular letter to all customers and send their addresses to the print shop. Is this data transfer contractually regulated? Is it permissible and is it secure?
- An important customer tells us on the phone that his birthday is today. Can you store this information in the customer database?

If you process personal data, check your procedure in two steps:

1. Is there a work instruction that specifies how the specific task is to be completed in a legally compliant and data-secure manner? Then follow these instructions.
2. In the absence of such data processing requirements, **it is up to you to decide whether the processing is to be carried out in accordance with data protection laws**. If you are uncertain about the evaluation, you must contact your supervisor or the company data protection officer.

Rule of thumb

Sometimes it is obvious, sometimes it is unclear whether one's own data processing is permissible under data protection law. The rule of thumb can help you here:

If it was your own personal data that was being collected, processed or disclosed: Would you have any concerns for yourself?

If your answer is "Yes", you should contact your supervisor or the company data protection officer.

THE COMPANY DATA PROTECTION OFFICER

The company must appoint a company data protection officer in Germany i**f it consistently employs at least 20 people dealing with the automated processing** of personal data. The data protection officer's task is to advise management and employees with regard to data protection-compliant data processing. On the other hand, the officer does not have the task of enforcing data protection. This task lies with the company management and the employees.

As an independent auditor who is bound to secrecy, however, the data protection officer is available as a contact person for all employees. **The data protection officer will process every report on data protection-relevant circumstances in the company confidentially.** Should you have any questions regarding data protection, you can therefore not only contact your supervisor, but also the company data protection officer at any time, without having to fear that this will lead to any disadvantage for you.

THE DATA PROTECTION SUPERVISORY AUTHORITY ADVISES, MONITORS AND POSSIBLY IMPOSES FINES

Every federal state in Germany has an authority responsible for supervising companies' data protection procedures and following up on reports and complaints. The federal data protection authority is responsible for supervising federal agencies and authorities as well as the companies in the telecommunications and postal sectors.

The framework for fines has been considerably increased by the General Data Protection Regulation. Companies are now threatened with a maximum fine of up to EUR 20 million or up to four percent of their worldwide annual turnover in the event of serious data protection violations.

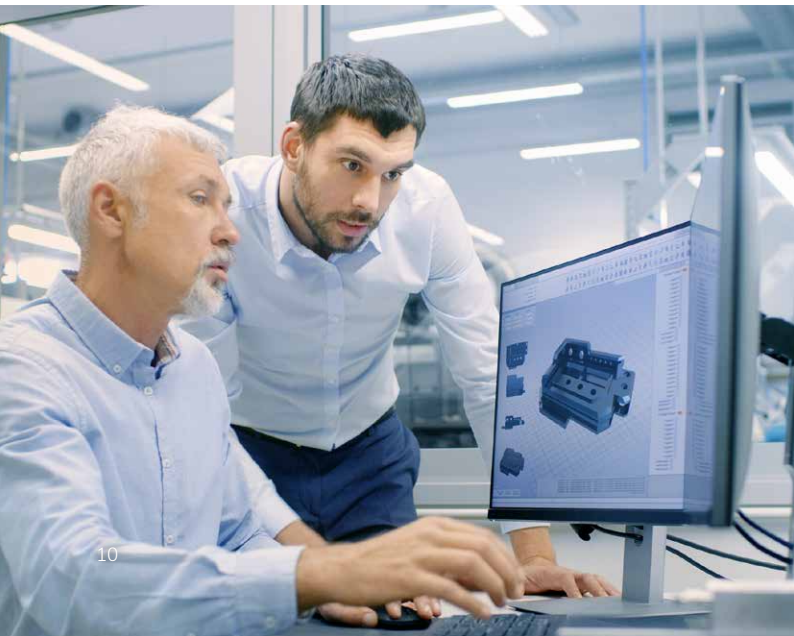
PRACTICAL TIPS

The data protection laws provide the following four obligations for data handling:

3. Data processing must be **permitted** at all by a legal basis.
4. People affected must be **informed** about the processing of their data.
5. Data processing must be carried out in a **secure** manner.
6. Data must be **erased** as soon as they are no longer needed.

IS DATA PROCESSING ALLOWED?

The company may not process any personal data without fulfilling one of the statutory permissions **(consent, legal obligation, company agreement, contract or contract preparation at the customer's request, legitimate interest of the company)**. The decisive factor here is always whether the personal data are actually required in order to achieve the specific purpose.



Examples of permitted data processing

- The e-mail address may be stored if the customer subscribed to a newsletter.
- The HR department may store CVs and certificates for the purposes of recruitment and HR administration.
- The HR department may store CVs and certificates of rejected job candidates in an applicant pool for later filling of positions, if the applicants have agreed to this beforehand.
- The internal audit department may collect employee data in order to check the correct procedures of the company. In cases of doubt, it is necessary under data protection law not to collect the data under a specific name but under a code (pseudonymized data).
- The IT department is authorized to automatically check and filter a large number of network traffic content in order to provide network traffic or to monitor SPAM.

Your test question

Is there a provision, a company agreement, a contract, an objectively legitimate interest or consent allowing information about the people affected to be processed, disclosed or otherwise used?

IS THE DATA SUBJECT INFORMED ABOUT THE DATA PROCESSING?

The affected person should be able to clearly see that personal data relating to him or her is being stored and processed. He or she should know from which company and for what purpose and which data are affected. A reference to a right of objection is also a must.

Your checklist for the obligation to provide information

Is the concerned person sufficiently informed about

- ☐ the full name and
- ☐ the complete address of your company,
- ☐ the full address of the data protection officer (if there is one),
- ☐ all the purposes for which the affected person's data are processed, including the legal basis of the processing and the "legitimate interests" where the authorization results from a balancing of interests,
- ☐ the categories of recipients of the data, if data transfer is planned,
- ☐ possible processing of the data outside the European Economic Area,
- ☐ how long the data will remain accessible until it will be deleted or access will be restricted,
- ☐ the rights of the people affected, i.e. their rights of withdrawal, their rights to lodge a complaint or the fact that a decision – for example on the granting of credit – is taken directly by an IT system after automated decision-making?

IS THE PROCESSING OF THE DATA SECURE?

Companies and employees have to ensure that personal data **are not lost** and **cannot be viewed or altered by unauthorized persons**. Care must also be taken to ensure that all necessary data transmissions are carried out in a secure manner.

It is therefore a **secondary obligation** under the employment contract **to protect both information about natural persons and confidential company information from unauthorized disclosure and falsification**.

DATA SECURITY RULES

Data acquisition
Only information required for the respective purpose may be collected. Too much personal data are unlawful. This is also important because people affected can request information about their data stored in the company. The company is then obliged to disclose all data stored on the person.

Paper files
Documents containing personal data must **not be disposed of in normal waste or waste paper containers**, but must either be shredded with a document shredder or disposed of in data waste containers provided for this purpose.

Communication
Be careful in general when passing on data. Always be careful to enter the **correct e-mail address and fax number**. And also check whether the person behind the e-mail address or fax number is **authorized to receive the information**. Never simply rely on a fax number or e-mail address given over the phone. For example, if a person requests information about a contract over the phone and then provides a fax number or e-mail address, it could also be a trick. If in doubt, always use the postal service or a reliable address.

When transmitting important personal data (above all **HR data, health data**), ensure that it is received personally and encrypt it when you send it as an attachment to an e-mail.

You should therefore **generally** send confidential and **personal data in encrypted form or by postal service**.

Data transport
Outside the operating rooms, personal data must always be transported on the **company's own portable media** (USB sticks, hard disks) and **only in encrypted form**. Third party data carriers must not be used without verification.

Data loss
If **data are lost** (USB stick left lying, e-mail with attachment sent to wrong addresses), the reporting method applicable to your company must be observed, e.g. the **supervisor**, the **data protection officer** and/or the **service desk** must be informed (see section "What to do in case of data breaches").

Encryption, passwords
In most cases, companies issue corresponding work instructions. Otherwise, it is best to adhere to the specifications of the Federal Office for Information Security (www.bsi.bund.de) – whose recommendations also make sense for the private domain. **When leaving the computer, it must be locked** (for Windows computers: WINDOWS key + L, for Mac computers: Control + Shift + Eject). Reactivation may only be possible by entering a password. In addition, the lock must be activated automatically after a specified time so that no unauthorized person can use the computer if you have forgotten to lock it.

Protection from eavesdropping
Make **calls with confidential content** in such a way that unauthorized persons cannot follow the call.

General vigilance
Speak to people you do not know and who you notice on the company premises and ask them for their name and function, if necessary. Report your observations; do not pass by carelessly.

If you notice something
If you become aware of inadequate data processing, inform your supervisor or the data protection officer, who will treat your information confidentially.

Your test question

Have I done everything in my power to ensure that my colleagues and outside third parties who are not responsible for the specific matter do not become aware of the content of my data processing? Have I followed all the instructions?

STORE, DELETE OR RESTRICT ACCESS TO DATA?

Every company must ensure that access to personal data is **restricted** or that the relevant data **are deleted after the statutory time limits** have expired.

Example

For example, it is permissible to monitor certain areas of the plant, such as the entrance to the warehouse, by video camera. However, only a very **limited group of people** may access the **recordings** of the video cameras, access must be logged and after a few days the recordings must be deleted by overwriting them. However, video images must not be used, for example, to determine the arrival and departure of individual employees over a period of weeks.

Personal data processed by the company may not be deleted by employees at their discretion. Management must issue work instructions for deletion.

Example

Application documents must be deleted six months after the position has been filled, i.e. the documents must be returned to the data subject or destroyed. However, travel expense reports for interviews with applicants' addresses must be kept for ten years for accounting purposes in Germany.

The obligation to delete applies to all storage locations (e-mail accounts, web servers, cloud storage) and of course also to printed versions of electronic data.

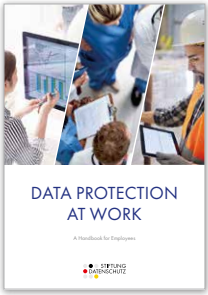
Sometimes the legal retention periods are in conflict with the deletion obligations: While personal documents of an unsuccessful applicant must be deleted six months after the position is filled, their address will be stored on their travel expense statement for ten years as required by German tax law. However, access to this information must be restricted during this time so that access in day-to-day business or for other purposes is no longer possible.

WHAT TO DO IN CASE OF DATA BREACHES

No company is 100% secure. To ensure that data protection incidents are not concealed, they must be reported to the responsible data protection supervisory authority. This is the task of the management or the data protection officer. You personally should be able to prove at any time that you have fulfilled your obligation to report to the company.

Your approach in the event of a data protection violation

So if you detect a data protection incident, contact your supervisor and the company data protection officer immediately. Create a short report (What data has been lost or accessed? How did this happen? What consequences do you suspect?) and send it to your supervisor and to the company data protection officer.



In addition to “Data Protection in a Nutshell – What Employees Need to Know”, the Stiftung Datenschutz has also published the brochure “Data Protection at Work – A Handbook for Employees” (DIN A5, 44 pages).

The brochure aims at managers, employees in HR and IT departments and all legal laymen who have to deal with personal data in their daily work. (The information also applies to associations and other organizations.) Both documents are also available in German. All versions can be obtained from the Foundation‘s website in PDF and printed form.

Publisher
Stiftung Datenschutz

Author
Dr. Philipp Kramer

About the author
Dr. Philipp Kramer is a lawyer in Hamburg. He advises international corporations and medium-sized companies in the fields of data protection law, new media, IT law and copyright law. He regularly publishes on IT law topics and holds lectures at seminars on data protection, IT security and competition law. In addition, he is editor-in-chief of the Datenschutz-Berater and first chairman of the Hamburger Datenschutzgesellschaft e.V. as well as visiting lecturer at the Universität Hamburg and visiting lecturer at the Ulm University of Applied Sciences.

ABOUT THE STIFTUNG DATENSCHUTZ

The STIFTUNG DATENSCHUTZ (Foundation for Data Protection) was established in 2013 by the Federal Republic of Germany. The independent institution serves as an information platform for the implementation of data protection law and as a discussion platform for data policy. The federal foundation promotes the dialogue between society, politics, business and research. As a neutral actor, the STIFTUNG DATENSCHUTZ complements the data protection supervisory authorities at federal and state level.

STIFTUNG DATENSCHUTZ

Stiftung Datenschutz
Frederick Richter (Responsible in the sense of the German "Pressegesetz")

Karl-Rothe-Str. 10–14
04105 Leipzig, Germany
T +49 341 5861 555-0
F +49 341 5861 555-9
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

Version 2.1, March 2020