DATA PROTECTION AT WORK

A Handbook for Employees

STIFTUNG DATENSCHUTZ

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

DEAR READERS,

No matter the size of the business you work for, your employer must ensure that data protection rules are followed. However, a company can only comply with the law if its employees are aware of the rules and follow them in their daily work. This brochure is intended to help you do this. With this brochure, the Stiftung Datenschutz would like to make a concrete contribution to clarifying the rules on data protection for all employees – especially small and medium-sized enterprises, for whom the EU General Data Protection Regulation, which is fully applicable since May 2018, often poses a particular challenge.

In the text of this issue, we work with real-life practical examples and would like to bring data protection closer to you – as a task that can be mastered. Often a basic sensitivity is already helpful: you do not always have to know the exact legal provisions, but a certain feeling is important as to whether dealing with information could violate the law.

In such a situation, if you ask your supervisor, the company data protection officer or the legal department, you are helping to ensure that your company acts in accordance with data protection regulations.

Our information is intended for managers, employees in HR and IT departments, freelancers, tradespeople and anyone else who has to deal with personal data in their daily work. Most of them are certainly legal laymen. To make the brochure easier to read, we have therefore not always used the usual legal terminology, but have tried to use a language that everyone can understand.

Even though we speak consistently of "companies", "supervisors" and "employees", the references also apply to associations, boards of directors and other organizations and individuals.

If you have any suggestions, criticism or ideas for improvement regarding "Data Protection at Work", please feel free to contact us:
mail@stiftungdatenschutz.org

Frederick Richter

TABLE OF CONTENT

FOR WHOM IS THIS BROCHURE INTENDED?

FOR EMPLOYEES

Every employee who actively works for the company, whether as a manager or as an intern, must be familiar with the core obligations of data protection. Although only the management, the legal department and the company data protection officer have to deal with the legal regulations on data protection in depth, in today's working world almost every employee also makes his or her own decisions on data processing.

Even if you do not constantly work with personal data – as for example in the HR, marketing or IT department – you must observe and apply the legal requirements if you want to avoid sanctions and adverse consequences for your company or even for yourself. This brochure is designed to help you do this. It supplements the work instructions that your management may have issued on data handling.

FOR MANAGEMENT

As a company manager, you are obliged to inform your employees about data protection. This means that your employees know that they may only process personal data in accordance with your instructions. You can use this handbook to raise awareness among your employees and inform them about the basic requirements.

This brochure cannot replace specific instructions on how to handle certain types of data and should therefore be supplemented by further instructions, if necessary. However, the brochure provides the basic information required by law and general data protection-related work instructions.

FOR COMPANY DATA PROTECTION OFFICERS

As company data protection officer, one of your tasks is to inform and advise “the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions” (Art. 39 GDPR). For this purpose, you can offer classroom trainings or e-learnings, but you can also use this handbook.

DATA PROTECTION IN THE COMPANY

COMPANY SECRETS

Trade and business secrets

Companies and other organizations have **information** which **is known only to certain groups of people** and which should not be made public. This is usually referred to as trade or business secrets. Typical business secrets are recipes, production processes and information about financial circumstances.

Employees who are aware of trade or business secrets in the course of their work must keep them secret; this is regulated in the German Law for the Protection of Trade Secrets. Management usually ensures that this **confidentiality is contractually agreed** – not only with employees in work contracts, but also with external service providers such as temporary employment agencies or suppliers in service contracts. In this way, the contracting parties are obliged to protect trade and business secrets.

Confidentiality and data protection

Information about natural persons also belongs to the trade and business secrets, for example the information about employees available in the HR department.

This “personal data” is particularly protected: by the **European General Data Protection Regulation** and in Germany by the supplementary Federal Data Protection Act. The purpose of data protec-

tion is to prevent **unauthorized persons** from obtaining **information about a natural person** or the holders of such information from using it in an unjustified manner.

The rules are strict. A data protection violation may already have occurred if

- personal data are stored or copied that is not required for the work tasks,
- Information about customers is passed on without permission,
- particularly sensitive information such as data concerning health is sent unencrypted by e-mail without the consent of the person affected.

What exactly is “personal data”?

Personal data are any information about a natural person that can be directly or indirectly attributed to that person. (We call this person “data subject” or “people affected”.) This applies to members of management as well as employees, employees of suppliers as well as guests and customers or interested parties.

Examples

- The person's name can be assigned directly to the person.
- The person's function can also be directly assigned if, for example, there is only one IT manager in the company.
- The person's personnel number can be assigned indirectly: Although the personnel number itself does not yet refer to the specific person, the personal reference can be established by inividuals who know which name belongs to which personnel number.
- An IP address can even be indirectly assigned to a specific person.

These examples show that the context must be considered when deciding whether personal data are involved, especially in the case of **indirect personal references**.

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.

BUSINESS SECRETS AND DATA PROTECTION

In addition to trade and business secrets, personal data are also subject to special protection. Comprehensive data protection regulations must be observed when processing such data, as violations – not only intentional, but also negligent (i.e. out of ignorance or carelessness) – can lead to adverse consequences for the company and also for the acting employee. First and foremost, of course, it is a matter of keeping disadvantages away from those affected by unlawful or insecure data processing. This brochure provides you with a basic overview of the statutory provisions and numerous practical tips. It is intended to help you make the right decisions about data protection in your everyday work.

THE IMPORTANCE OF DATA PROTECTION WITHIN THE COMPANY

The data protection regulations protect personal data in the company not only as an asset of the company. In particular, the individuals whose data are processed should be protected. In this way, the legislator wants to prevent people from suffering damage as a result of unauthorized or improper handling of their data.

Examples of inappropriate handling of personal data

An employee of the HR department wants to inform a supervisor about a medical employment prohibition of an employee via unencrypted e-mail. While entering the address, the employee mistypes and accidentally sends the mail containing sensitive health-related data to the colleagues of the person in question.

As a service to customers, a company publishes the mobile phone numbers of important contacts on its website. After work, the production manager now regularly receives calls from companies that want to sell their products or recruit him.

The concept behind data protection law is that everyone should be able to decide for themselves which of their personal data should be accessible to whom and when (the so-called "right to informational self-determination"). It is important to understand that **data protection should not protect the data itself. It is always about the person to whom the data relates**. Data protection is personal protection – and not an end in itself! 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.

Companies and organizations must always ensure that personal data are handled in accordance with the law. To this end, they usually implement certain **controls**:

For example, employees who work with personal data (in the HR department, in IT, in customer service, in sales, in the works council...) must be **instructed about data protection-compliant behavior** and must be bound 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). His or her contact details must then also be communicated to the supervisory authority. You can find out more about the role of the data protection officer in the section "Who is responsible for good data protection?".

The company management must regulate the handling of personal data by means of work instructions. However, there are workflows that the company cannot specify down to the smallest detail. Employees must then apply the relevant data protection regulations themselves and decide whether or not certain processing of the data is allowed. This does not only affect departments in which personal data are handled intensively, such as HR departments; many employees also make their own data processing decisions for the company in their everyday work, be it when sending an e-mail or entering personal data in company databases. In doing so, legal data protection obligations must always be taken into account, otherwise the otherwise the company – and possibly even the acting employees – is threatened with sanctions and other negative consequences. You can find out more about this in the section "Liability for data protection violations".

Companies themselves have a strong interest in ensuring that all their processes comply with data protection regulations in order to avoid breaches of law with liability risks and risks to their reputation. In recent years, the public has also become more sensitive to the careful handling of personal data; data breaches damage the company's reputation with customers and suppliers and – in addition to violating the rights of those affected – can also cause lasting economic damage.

SUMMARY

DATA PROTECTION PURPOSES

Data protection law aims to **protect everyone from unauthorized use of their data or damage caused to them** by the mishandling of data concerning them. In order to achieve this purpose, data protection law imposes sanctions on both companies and employees. Since data protection is playing an increasingly important role in the public domain, companies that act in compliance with data protection also avoid negative press about themselves.

LEGAL BASIS

WHICH LAWS REGULATE DATA PROTECTION?

The most important regulations for data protection are the European **General Data Protection Regulation**[1] and in Germany the supplementary **Federal Data Protection Act** (BDSG). Both laws are contained in the brochure of the Federal Commissioner for Data Protection "Datenschutz-Grundverordnung". Among many other materials, it is available on the information platform of the Stiftung Datenschutz on the implementation of the EU data protection reform[2]. 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.

Data protection law **protects personal data in any form, not only on computers or in databases, but also in paper files**. Only disordered information on loose slips of paper or personal data exchanged verbally are not covered by data protection law. An exception to this exception concerns employee data in Germany, where the law is particularly strict and already covers the oral exchange between two people. If an employee in the HR department sends a colleague from the sales department information about a staff member that is not generally known, this is unlawful without a substantive reason under labor law or without the consent of the person affected.

WHEN DOES DATA PROTECTION LAW PERMIT THE PROCESSING OF PERSONAL DATA?

The so-called **prohibition principle** continues to apply in Germany under the General Data Protection Regulation: Any processing of personal data is initially **prohibited** as long as it is not exceptionally **permitted**. This permission can be granted in very different ways:

1 http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

2 DSGVO.stiftungdatenschutz.org

When is further processing permitted?

- with the consent of the affected person,
- if processing is provided for in the collective agreement or in a company agreement,
- if the processing is necessary for a contract requested by the affected person,
- to fulfill a contract with the affected person,
- if there is a legal obligation to process data,
- where a balancing of the legitimate interests of the company against those of the affected person has shown that the interests of the company are predominant.

In practice, this means that the processing of personal data is allowed if at least one of these conditions applies. The further possible legal permission "processing is necessary to protect the vital interests of a data subject[3]" is rarely used in the practice of a company.

3 "Data subject" is the legal term for a concerned person.

Your test question:
Is there a consent that permits data processing?

The requirements for consent are high. It must be based on concrete and comprehensive information so that the consenting party can really make a decision. It must also be given freely. Particularly in the employment relationship, it must be checked for each data processing consent whether the specific person or group of employees can be assumed to consent voluntarily. Especially in the application phase, voluntary consent will be difficult to state and prove. In the case of other employee consents, the employer should be able to make plausible why the employees were free in their decision.

Your test question:
Does a balancing of interests allow data processing?

The balance to be struck within the company between the processing interest of the company and the "interest in confidentiality" of the affected person must not be arbitrary. It is difficult for employees in a company to decide quickly and practically which interest weighs more heavily in their everyday work. The general clause on the weighing of interests has therefore been clarified in many cases by courts, supervisory authorities and in the legal literature.

- For certain processing operations, the interest in the use of data clearly predominates. For example, a company may send its customers advertising by mail.
- In the case of processing operations that have a greater impact on privacy, it is assumed that the person's interest in not using the data always prevails (e.g. passing on detailed customer profiles).

However, there are processing operations in which it is unclear or controversial whether the affected person's "interest in confidentiality" or the company's interest in using the data prevails. Then the management must decide – if necessary after legal consultation – whether the data processing may be carried out. A data protection supervisory authority or a court can subsequently check whether the decision has been correctly balanced.

EXERCISE

You manage the HR department of a medium-sized teapot manufacturer. The owner wants to do something for the working atmosphere and orders you to publish the birthdays of all employees on the company intranet, "for data protection reasons" without the year. You have just attended a data protection training course and are unsure whether this is okay. Please check whether the request is permissible under data protection law.

SOLUTION

Of course there is no special law for birthday lists. In most cases, there will also be no corresponding company agreement. Employment contracts do not usually contain corresponding rules either. Thus, the distribution of the birthday list to colleagues can be justified in most cases only by consent or balancing of interests (= data processing permitted if the company is interested in the use of the birthday data). The company typically – but not always – has a predominant interest in improving social solidarity in the interest of operational efficiency by offering the possibility of a birthday greeting. The year is not absolutely necessary for this. In order to clearly determine the interest of using and distributing the birthday list, every employee should be granted a right of objection. However, because of the difficult balancing of interests, you decide to ask all employees individually for their consent.

WHO IS RESPONSIBLE FOR GOOD DATA PROTECTION?

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

The company is liable for data protection violations. The management acts in compliance with data protection if it obliges the employees to fulfill their work tasks in compliance with data protection and specifies data protection-compliant actions by means of concrete work instructions. Typically, the company issues instructions on data processing relating to the respective area of work and monitors compliance with these instructions. With these instructions, the company management, as the **controller for data processing**, fulfills the legal obligation (Art. 29 GDPR) that employees “shall **not process those data except on instructions from the controller**”. Without such an instruction, data may only be processed if there is a legal obligation to do so.

If the data protection-related work instructions leave the individual employee room for decisions, the company management must inform the employees with a data protection instruction in accordance with GDPR. This data protection directive contains more general requirements than the data protection-related work instructions and enables the employees to decide in favor of data protection-compliant action in a more concrete case of application. This brochure is very much a general data protection instruction.

In addition, supervisors, department heads, etc. should at all times be in a position to issue instructions relevant to data protection and answer questions. This brochure is therefore also helpful for them.

THE EMPLOYEES CARRY OUT THE REGULATIONS

If you process data from natural persons in your daily work – such data processing already begins with the creation of address directories in the office software – **some work processes are specified by instructions and/or the IT systems**. For example, HR data processing and financial accounting systems almost always provide that only certain data can be entered and processed at all. Password lengths and password types are also often fixed.

However, if specific instructions are missing, you have to make your own

data protection decisions. To do this, you must be familiar with the requirements of data protection law.

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?

To do this, 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.

Your test question: Examination of own duties

Sometimes it is obvious, sometimes it is unclear whether one's own data processing is permissible under data protection law. The rule of thumb (see page 23) and the further explanations on permissions (see page 21) can help you here. If you are unsure, ask the competent authority. And if you do not see a suitable contact person, contact **your data protection officer** (see next page). He or she is **the most important body within the company for data protection issues**.

THE COMPANY DATA PROTECTION OFFICER ADVISES AND MONITORS

The company must appoint a company data protection officer in Germany if it consistently employs at least 20 people dealing with the automated processing of personal data (section 38 BDSG, which also regulates other requirements).

The data protection officer's task is to advise management and employees with regard to data protection-compliant data processing. Especially for projects with new data processing, the know-how of the data protection officer should be requested at an early stage. It may also be necessary to conduct a data protection impact assessment in accordance with Art. 35 GDPR, namely if the data processing is likely to result in a high risk to the rights and freedoms of natural persons. In addition, the data protection officer monitors compliance with data protection regulations including the assignment of responsibilities, awareness-raising and training of staff and is the contact point for the responsible data protection supervisory authority.

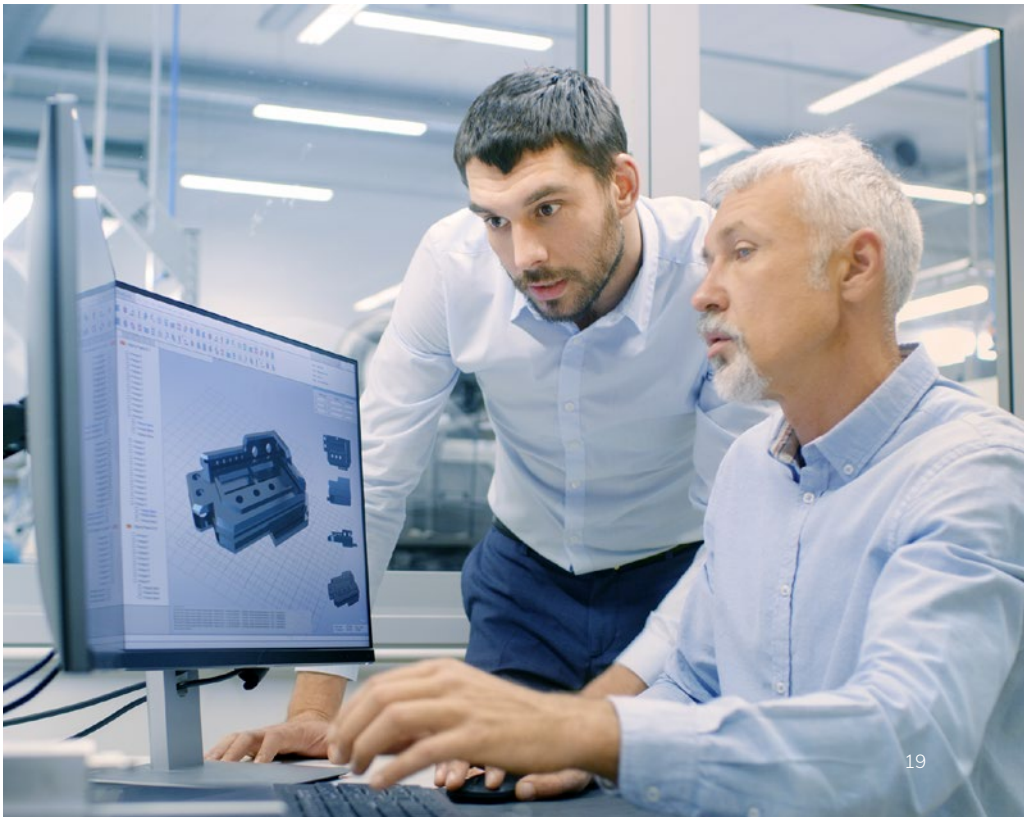
On the other hand, the officer does **not have the task of enforcing data protection**. This task lies with the company management and the employees.

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

As already described in the section "Who is responsible for good data protection?", the company is generally responsible for protecting the personal data of staff, applicants, customers, suppliers and the like. The data protection laws provide the following four obligations:

1. The obligation to check **lawfulness**: Data processing must be permitted at all by a legal basis.
2. The obligation to provide **information**: People affected must be informed about the processing of their data.
3. The obligation to process data **securely**: Data processing must respect the principles of data security.
4. The obligation to **erase data**: Data must be erased as soon as they are no longer needed.

If you handle personal data in your everyday work and the company management has not issued any special work instructions, it is your responsibility to comply with these obligations. The best way to do this is to follow the questions in this section.

IS DATA PROCESSING ALLOWED?

The first step is the permission check (see also the section "Legal basis"). 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: No personal data are required for buying bread rolls from the bakery around the corner if payment is made in cash; a car-sharing system, on the other hand, does not work without data collection (the storage of some data on the driving person is necessary for billing purposes and for assigning traffic offences).

Examples of permitted data processing

- Customer name and customer address as well as date of birth and bank details may be used to make an **online purchase** of the customer on account with SEPA direct debit. In addition, the e-mail address may then be stored; also in order to send the customer a **newsletter** about similar goods or services and thus, to carry out direct advertising. However, it is then indispensable to provide information on the right to object to advertising in addition to the general information (see answers to the second question "Is the affected person informed about data processing?").

- The HR department may process **CVs and certificates** for the purposes of recruitment and HR administration (reason for permission: decision on the establishment of an employment relationship and performance or termination of an employment relationship in accordance with the special provision of section 26 para. 1 sentence 1 BDSG as a more specific provision of Art. 6 para. 1 sentence 1 letter b GDPR).
- The accounting department in Germany must keep **travel expense accounts** of job candidates separately for ten years, but not the entire application file, only the supporting documents (reason for permission: legal obligation). The purpose of such archiving is limited ("legal restriction of processing"), i.e. the data may not be used for any other purpose.
- 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 (reason for permission: consent). The data of other applicants rejected for the specific position must either be deleted/destroyed or returned to the applicants at the latest six months after the final filling because there is no permission for further data processing.
- 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 information is then separated from the names (reason for permission: legitimate interest of the company within the scope of balancing interests).
- 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 (reason for permission: company agreement or interest of the company within the scope of balancing interests, if necessary with consent).

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?

Rule of thumb: To put it as simply as possible, at least ask yourself the following audit question:

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.

IS THE DATA SUBJECT INFORMED ABOUT THE DATA PROCESSING?

It is not sufficient in data protection law that data processing is permitted – the affected person must also be informed about the use of his or her data. They 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 (Art. 12 to 14 GDPR). A reference to a right of objection is also a must.

The information duties also apply to everyday business when personal data are collected from customers. For telephone orders, for example, a link sent to a mobile phone or a URL where the customer can retrieve the information is recommended. In the case of contractually permitted data processing, this information should already be included in the contract.

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?

The best data protection is of little use if **data security** gets out of sight. 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. Even minor carelessness can cause companies and people affected great damage, which can usually never be reversed.

Example of inadmissible insecure data handling

You send a business e-mail and do not pay attention to the correct recipient when sending it. With just one click, data can reach an unauthorized third party. Please make sure that e-mails to third parties are not sent via the normal Internet without transport encryption. Third parties may be able to view the communication content if it is not encrypted on the way to the recipient.

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**. In order to avoid mishaps in the use and disclosure of personal information and to protect themselves, employees should strictly adhere to the appropriate management guidelines. There are important **data security** requirements **that must always be observed**.

DATA SECURITY RULES

Data acquisition
Only information required for the respective purpose may be collected. Too much personal data are unlawful (see section "When does data protection law permit the processing of personal data?"). This is also important because data subjects 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. **Attention**: Not every document shredder shreds the documents sufficiently small. The DIN 66399 standard for the destruction of data media must be taken into account. Ask your supervisor or your data protection officer if you are not sure.

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 storage 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 + Command + Q). 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 individual can use the computer if you have forgotten to lock it.

Confidential conversations
Make **calls with confidential content** in such a way that unauthorized individuals 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.

Remember: Even the best corporate security regulations are useless if not all employees adhere to them at all times. The goal of the data-secure company can only be achieved as good as the implementation is at the weakest point. And the weakest point is everyday life with its requirements. But those who act against the regulations and, for example, pass on their password without authorization, can considerably impair the security of the company and are liable for any damage incurred (see also “Liability for data protection violations”).

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. This requires a **concept for the data types and their deletion obligation period**.

For this deletion concept, the question arises as to **when the concrete data are to be deleted at all**. The law does not specify a specific period, but stipulates that data must be deleted if they are "**no longer necessary** in relation to **the purposes** for which they were collected or otherwise processed" (Art. 17 para. 1 letter a GDPR). Frequently, the concrete deadline can only be determined by a legal assessment.

Example

Application documents must be deleted six months after the position has been filled, i.e. the documents must be returned to the people affected 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.

Employees can often use personal storage areas (personal file directory/home directory). These storage areas or media must be cleared of personal data by the employees themselves.

RIGHTS OF THE PEOPLE AFFECTED

The General Data Protection Regulation gives people whose data are processed in the company a number of rights in relation to these data. These are primarily information and deletion rights. A company must therefore be in a position to provide information on what data it stores on a person, for what purpose, for how long it is stored and for any data transfer. What is new is the right to data portability: if a person makes personal data about him- or herself available to a company, the company must provide this data to him or her on request in a "structured, commonly used, machine-readable and interoperable format" or transfer it to another provider at his or her request (Art. 20 GDPR). In order to meet these requirements, management must issue appropriate work instructions. The Stiftung Datenschutz has published its own brochure for companies on this new right[4].

DATA PROCESSING BY SERVICE PROVIDERS – DATA PROCESSING ON BEHALF

In the division of labor economy, it is inevitable that companies will pass on personal data to suppliers and other service providers (such as tax consultants, shredders, data centers, IT service providers, cloud computing providers, etc.) for processing, whether actively

4 stiftungdatenschutz.org/english/dataportability-en/

SUMMARY

DELETION OF PERSONAL DATA

Deletion of personal data by individual employees is **only necessary in exceptional cases**, for example if the data are stored on personal media such as USB sticks or personal drives. In any case, the operational deletion rules must be observed. If you have any questions in this regard, please contact your supervisor or the data protection officer.

by transmission or passively by granting access rights. Here the legislator prescribes a contract which **obliges the service provider and its employees to comply with the statutory data protection regulations**. The controller remains responsible for handling the data in compliance with data protection regulations; the controller is also obliged to check whether the specifications are complied with. This is referred to as data processing on behalf.

If a service provider is free to decide **which** personal data are to be processed on behalf and **how** (this usually concerns lawyers, company doctors or banks), it must be checked whether the transfer to these service providers is permitted (see section “When does data protection law permit the processing of personal data?”). Here, too, a contract is required and the personal data may only be used by the service provider for a specific purpose.

Checklist for data processing on behalf

Even the use of a web or smartphone app can be data processing on behalf. Therefore, if you are responsible for commissioning service providers and service providers are dealing with the company's personal data, check whether there is a data protection agreement with specific, legally prescribed content. In this case, beside the contract, the following must be in place:

- ☐ a description of data security
- ☐ a control procedure for the service provider through sufficiently plausible data security assessments or own audits
- ☐ documentation of the reliability assessment.

The data protection officer, if available, can help.

DATA PROCESSING ABROAD

Within the European Economic Area (European Union as well as Iceland, Liechtenstein and Norway) a uniform data protection standard has been created by the European General Data Protection Regulation (GDPR) and agreements. Here, simply the rules of this work instruction of the management regarding the handling of personal data according to the GDPR are to be applied.

However, data centers, software and cloud computing providers based outside the European Economic Area (**third countries**) are also frequently used. To ensure that the transfer to these countries does not violate European data protection standards, the GDPR obliges data receiving companies in third countries to take special measures. Ask your supervisor and – if available – the data protection officer for specific work instructions. Even an international data protection agreement with certain contents can constitute this justification. As a rule, it is up to the legal department or the lawyer of your company to draw up the necessary contracts. The data protection officer is responsible for providing advice and monitoring implementation.

SUMMARY

DATA TRANSFER ABROAD

If there is no justification for a data flow to countries outside the European Economic Area, a data protection violation occurs. If you become aware of such a data transfer, inform your supervisor and, if applicable, the data protection officer.

WHAT TO DO IN CASE OF DATA BREACHES

No company is 100% secure; every company will have a “data protection incident” at some point. For example, digital storage media, such as a USB stick or the storage disk in a laptop, can get lost or there can be a break-in on the web server or directly into the server room. The most important thing to do then is to prevent any damage to the affected people (whose information has been lost) and to the company.

To ensure that such incidents are not concealed, the law requires, in order to protect the people whose data has been lost, that **a data security incident must at least be reported to the responsible data protection supervisory authority and, if necessary, to the people affected**. If something is concealed and later uncovered, considerable disadvantages and penalties are to be expected.

But **when** must this type of data security incident **be reported** to the supervisory authority? A reporting obligation always exists, unless the incident “is unlikely to result in a risk to the rights and freedoms of natural persons”. Only experts can usually judge whether this is the case. **So if you detect a data security incident, contact your supervisor and the company data protection officer immediately.**

The report to the supervisory authority must be made within 72 hours after a member of the company or institution has discovered the incident. The period begins immediately – not when management has learned of the incident. This deadline can only be exceeded in exceptional cases. If the report is not made to the supervisory authority within 72 hours, a justification for the delay must be attached.

If the incident even causes a “high risk for the rights and freedoms of the people

affected", these individuals must also be notified. Here, too, the decision as to whether such a risk exists is the responsibility of the company management; the data protection officer advises on this assessment.

However, even incidents that do not have to be reported must be carefully documented and analyzed so that they do not repeat. These tasks are the responsibility of the management or the employees assigned to them and the data protection officer.

Your approach in the event of a data protection violation

What do you have to do if you or your colleagues have lost a laptop, a tablet, a smartphone, a memory stick, memos or files with personal data, etc.? 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**. The report can, of course, also be prepared by your supervisor upon your verbal communication.

A data protection incident may occur. However, corrective measures are then important. And it is important for your situation that you can prove at any time that you have fulfilled your obligation to report to the company. It must therefore be documented what has happened so that the necessary measures can be taken and proven to the supervisory authority. How an incident of this type can be prevented in the future must then be regulated, for example, by a company agreement or by work instructions.

LIABILITY FOR DATA PROTECTION VIOLATIONS

As already explained in the section "Who is responsible for good data protection?", the company is generally liable if data protection violations occur. Various sanctions are possible. For example, the supervisory authority can impose large fines if a company fails to report a personal data breach (see section "What to do in case of data breaches"). In connection with the German Adaptation Act to the EU General Data Protection Regulation (BDSG), liability can also arise for the company management, i.e. for the managing director personally.

Third parties, such as employees or customers, can also report data protection violations to the authorities and thus trigger a liability case.

This section looks at the liability of employees.

AM I LIABLE TO MY EMPLOYER FOR DATA PROTECTION VIOLATIONS?

One thing in advance: As an employee or worker, it is not you personally who must take the first responsibility for your mistake, but the company. However, if you have culpably brought about a data protection incident, depending on the type of fault you are guilty of, you may be liable alongside the company and be liable for damages.

The so-called limited employee liability creates advantages for you as an employee in Germany. You do not have to answer to the employer for slightly negligent unlawful data processing. However, if you act very negligently or even intentionally, your liability will approach full liability as your fault increases. Regardless of the liability for compensation, you may be subject to disciplinary, official or judicial measures.

If you could have acted differently, you are also personally liable to the employer for unlawful conduct.

LABOR LAW CONSEQUENCES

The employer must check that employees comply with data protection regulations. It must consider disciplinary action in the event of non-compliance. These measures can be a reminder, a **warning** or a **punitive transfer**; in serious cases, there may be a **termination** or even an **extraordinary termination**. The employer must not take data protection violations lightly; otherwise it would expose itself to the risk of its own regulatory sanctions, such as investigations, remedies and fines.

Examples

A bank employee was lawfully and extraordinarily dismissed because she had forwarded a customer's account data to a foreigners' registration office by telephone.

The use of a bank's customer database by an area manager to make private contact with the customer led to an extraordinary termination, which was only downgraded by a court to a warning.

FINES

If you as an employee have personally violated data protection obligations, the responsible supervisory authority can initiate administrative offence proceedings against you. Such proceedings begin – as in the case of a traffic violation – with you being contacted by the supervisory authority. You will be given the opportunity to explain your actions. Once a violation has been established, the supervisory authority can impose a fine.

Example

The case of an employee in Bavaria who had negligently inserted a large number of customer addresses into the CC field of an e-mail and sent customer information caused a stir. This made all customers aware of the e-mail addresses of all other customers of the company, which was clearly contrary to data protection. The employee was fined by the Bavarian supervisory authority – irrespective of disciplinary measures taken by the company.

Similar cases that have come to light are the sending of HR data via a freemail provider (gmail.com, yahoo.com, etc.) for processing at home or credit information about another person obtained for private purposes via a company database.

FINES AND IMPRISONMENT

Some breaches of data protection are even punishable by penalties and imprisonment. In the event of a violation of the requirements of permissible data

processing sanctioned by criminal law, you, as the employee, could face serious criminal charges. Even the unauthorized deletion of an e-mail or the unauthorized disclosure of a colleague's documents can, under certain circumstances, constitute a criminal offence. Frequently, however, the intention to cause damage or to enrich a person must be present in order to be punishable.

Example

The secret attachment of GPS devices to a vehicle in order to determine a person's movements is punishable by law if it is done in return for payment.

SUMMARY

LIABILITY

Data protection violations by employees in the company can result in liability for damages and fines, in extreme cases even criminal convictions. In cases of high personal negligence, liability for damages can affect not only the company but also the employee who committed the violation. In addition, he or she is threatened with consequences under labor law, including termination, in extraordinary circumstances.

FOR YOUR NOTES

In addition to “Data Protection at Work – A Handbook for Employees”, the Stiftung Datenschutz has also published the brochure “Data Protection in a Nutshell – What Employees Need to Know” (DIN long, 20 pages) in cooperation with Hellmann Worldwide Logistics.

The brochure summarizes the most important points in a practical and easy-to-understand manner and is intended to support company instructions on the handling of personal data. (The information also applies to associations and other organizations.) Both documents are also available in German. All versions can be downloaded at www.hellmann.com/employeeprivacy.

Publisher
Stiftung Datenschutz

Version
2.1, March 2020

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 magazine *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