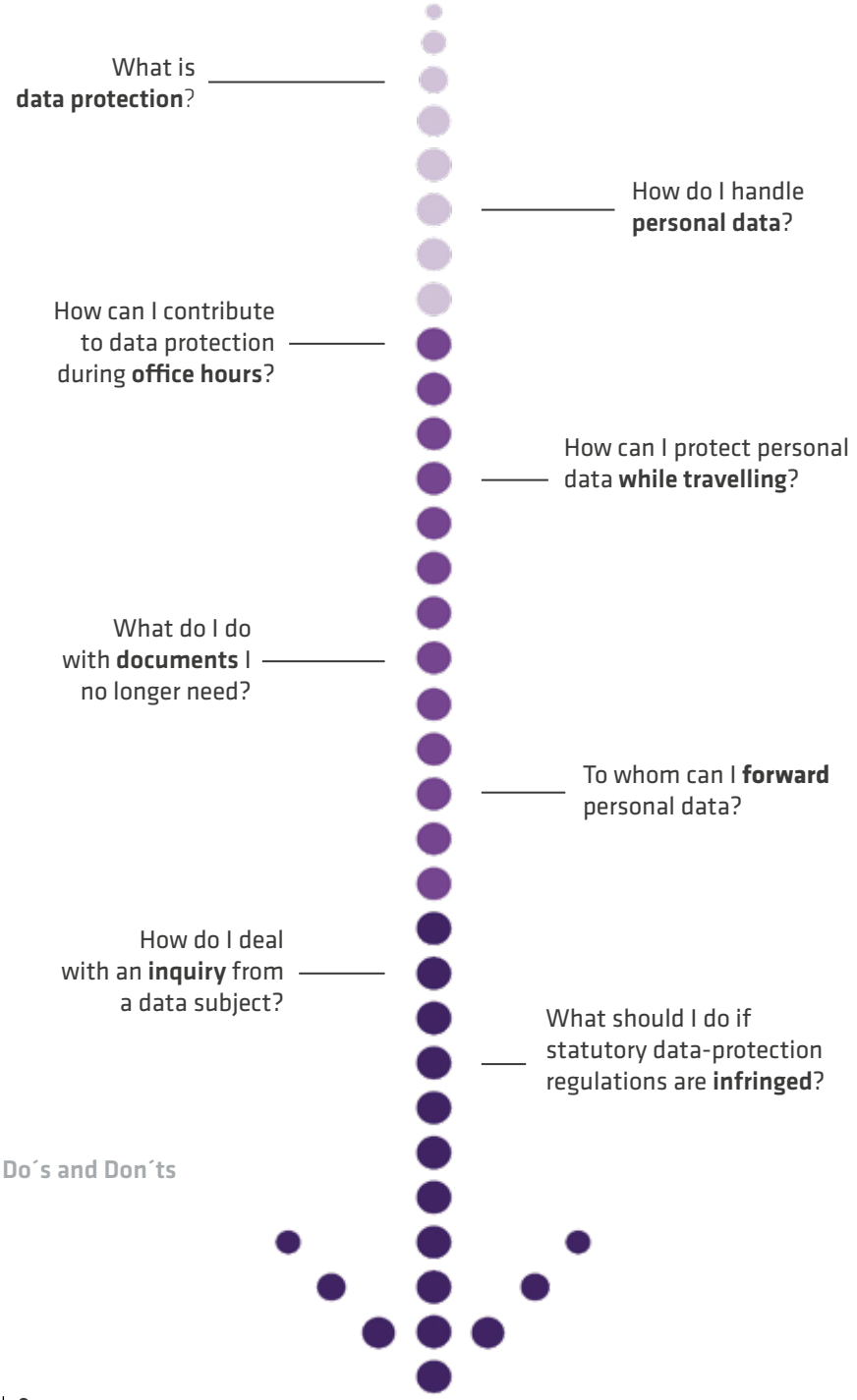
welser profile

Data Protection Guidelines

Welser Profile Group



Do´s and Don´ts

Why these guidelines?

The trust of our customers, business partners and employees[1] is of vital importance for the long-term success of our company. The protection of personal data is therefore of great concern to us. The processing of personal data contrary to current statutory data protection regulations is incompatible with our company culture and philosophy, and our company image.

Violations of data protection law can have serious consequences for us as a company. In addition to considerable fines, there is a grave threat of a permanent reputational loss and high claims for damages. Breaching statutory data protection regulations, and especially data confidentiality, can involve far-reaching disciplinary, tort law and penal administrative consequences for every single employee of the Welser Profile[2] Group as well.

[1] In this text, the term "employee" is used to mean male and/or female employees; therefore, any other gender-specific designations apply automatically to both genders.

[2] The abbreviation "Welser" is also used below for the "Welser Profile Group".

Our compliance responsibilities

Should any questions or uncertainties arise during working hours or in relation to a specific matter, please contact your line manager or our compliance officers immediately:

Markus Kepp
Data Protection Officer
(Welser Profile Group)
Tel.: (+49 2383) 914 - 5055
Email: m.kepp@welser.com

Benedikt Geusau
Head of Law and Compliance
(Welser Profile Group)
Tel.: (+43 7443) 800 - 4160
Email: b.geusau@welser.com

1. What is data protection
and how does it **affect me as an employee**?

Data protection is a fundamental right. This means that the Constitution guarantees every individual the respect of their privacy and the protection of their personal data.

Because this protection can only be guaranteed when it is actively and **jointly practised** by us as a company and you as an employee, these guidelines provide answers to key questions about the handling of personal data in the course of your work.

All direct or indirect **personal data** are subject to data protection. Therefore, not only data relating directly to a person, such as name and date of birth, are relevant here. Also included are data which can only be traced directly back to a person when combined with additional information. This might be a social security number, IP address or vehicle licence plate. In addition, data protection extends to data stored about a person (e.g. purchasing behaviour, work hour records, wages and salary).

Special care is also required when processing **"sensitive" data**. These are data which, because of their nature or content, are considered by legislators to warrant special protection (e.g. health details, information about racial or ethnic origins, trade union membership, details of political or religious opinions, or sexual orientation).

Data protection law refers repeatedly to the **processing of personal data**. This is understood to mean any process carried out in connection with personal data. More specifically, it can include the collection, creation, sorting, storage, modification, change, read out, querying, transfer or provision of personal data.

The processing of data does not necessarily have to occur automatically in an IT system. Even (partially) manual processes can be subject to processing in accordance with data protection legislation, if the data are structured in some way. Customer lists or employee files in paper form are two examples.

2. What is the procedure
for handling **personal data**?

Personal data must always be collected and processed exclusively in accordance with the applicable data-protection regulations. This is why we place great value on the provisions of European and national data protection laws (in particular the GDPR).

The **basic principles behind data protection**, in particular, must be observed when handling personal data. Of central importance here are the requirement for transparency, the principle of legality, the principle of specified purpose, the principle of data minimisation and the principle of storage limitation.

Adequate **technical and organisational measures** (TOMs for short) should be specified to ensure appropriate security during processing. The extent to which TOMs are required depends on the risk of the actual processing. Included are, for example, measures to protect the confidentiality of personal data such as access controls, i.e. measures governing the use of keycards and secure passwords or the needs-based allocation of access permissions.

These obligations primarily affect our company in our role as **the organisation responsible for processing**. However, because you as employees have regular contact with personal data and process them (e.g. by sending emails), there is a need for every employee to take account of the basic principles of data protection during the working day. Furthermore, every employee of Welser has a duty to maintain data confidentiality (even beyond the end of the employment relationship).

In brief, this means that personal data must always be processed only to the extent that actual processing is required, in accordance with the basic principles of data protection legislation and on a valid legal basis pursuant to the GDPR.
The data subject must also be informed transparently about the processing and must be guaranteed adequate processing security.

As an **employee**, you must always process and pass on personal data only to the extent required to fulfil an **express instruction** from your line manager.

3. How can I contribute
to data protection at work?

During your working day, you will often unknowingly come into contact with personal data as part of various work activities. By following simple patterns of behaviour, every employee can make a considerable contribution to the protection of these data and of data subjects, both internal and external.

Typically, employees will collect and/or further process personal data in the following situations:

- **Emails:** personal data are processed when an email is sent. At the very least, it contains the email address of the sender and recipient, and usually their names as well. In addition, other personal information is often concealed in the email signature and in the body text. If emails are sent or forwarded to a large number of addresses, the personal data are also shared with these people, too.

- **Hard-copy documents:** even hard-copy documents, whether just handwritten notes on internal or external meetings or a file of printed internal or external, confidential contract documents, often contain personal data which should be protected and whose processing is only permitted in accordance with the legal requirements.

Then there are situations during the working day which pose a potential risk to processing security and therefore to the protection of personal data. A series of technical and organisational measures has been undertaken to obviate this risk. As an employee, you can actively help with their implementation by being aware of situations requiring data protection and by adopting the correct response and mode of conduct.

Don´ts:

- Never leave documents containing personal data (e.g. addressee/sender of a letter, contact-person details, participants at an event) open on your desk.
- Never leave mobile devices (e.g. laptops, USB sticks or other data carriers) unattended in public or easily accessible places.
- Emails are not a secure form of communication. Do not, therefore, send documents containing sensitive data using unencrypted emails.
- Never allow non-employees to wander unaccompanied on company premises or in company office buildings.

- Photos and videos of people are also subject to data protection. Remember that taking private photos on company premises is forbidden.
- In addition, do not post on the internet (on your social media channels, for example) any photos or videos taken as part of your job and containing personal data or other company information of any kind.
- Never keep notes containing the secure password you have chosen in accordance with our internal rules at your workplace, and do not pass this information on to colleagues or third parties.

Do´s:

- Observe the "Clean Desk Policy".
- Keep confidential documents and data carriers secure in locked rooms or cabinets, for example.
- Lock your screen when you leave your workplace. This is done in Windows by pressing the Windows key + L.
- If you send an email to several recipients who do not know each other, use the "BCC" field to enter their addresses. This ensures that personal data (email addresses) are not forwarded or processed beyond the required extent.
- If you have to send sensitive data by email, use a password to encrypt the document.

- Only ever use passwords once for a service. The use of work passwords for private purposes (e.g. email account, apps, websites, social media) is strictly forbidden.
- Protect yourself from being observed by others when you enter your password.
- Always accompany non-employees to the desired place or person.

4. How can I protect
personal data while travelling?

In the modern world of work, professional activities are increasingly transferring from your own desk in a protected office to more public areas. This increases the risk of unauthorised non-employees obtaining personal information. Special care must therefore be taken!

The following situations are especially risky:

- **Working on a laptop in public areas:**
  Whether you are preparing documents for an upcoming appointment while using public transport, or spending your waiting time at an appointment or before the departure of your next bus going through your emails of a coffee shop, there is a risk of strangers obtaining personal information by looking at your laptop.

- **Phone calls in public places:**
  When making phone calls on public transport, in a supermarket or restaurant, there is a risk of strangers overhearing the content of the call and therefore obtaining personal data.

- **Carrying documents or data media:**
  Sometimes, the job may require you to carry documents or data media with you (e.g. because the documents are needed for or come from an outside appointment, or because they are absolutely necessary for the finalisation of work assignments). In hectic situations, especially, there is a risk of leaving these documents on the train or in the restaurant, for example.

- **Conversations/discussions with colleagues in public places:**
  You meet a colleague on public transport while on the way to work, join a colleague on the way to an appointment or spend the waiting time between two appointments in a coffee shop and would like briefly to run through the key points for the day. Here too, care is needed to prevent strangers from listening in.

Don´ts:

- If possible, do not make confidential phone calls in public places.
- Do not discuss personal or confidential information in public. This applies to phone calls as well as to conversations with your colleagues.
- If possible, avoid having confidential discussions in public places.

Do´s:

- Choose a suitable place or, if possible, use a privacy screen to protect your laptop from prying eyes.
- Before you leave public transport or other places, always check that you have not left any documents, files or data media behind.
- When making phone calls in public places, avoid mentioning personal and/or confidential information.
- Also protect printed documents from prying eyes when working in public places.
- When holding critical discussions outside company premises, always choose areas away from other people and avoid mentioning personal and/or confidential information.

Note:
All tips for conduct in the office or when travelling apply not only to personal data but **also to** all other **company-related information**. This must also be protected from unauthorised, external dissemination.

5. What do I do with documents I no longer need?

As data controllers, we are subject to the basic principles of data protection and therefore also to the principle of storage limitation.

Personal data must therefore only be stored for as long as absolutely necessary to complete the specific purpose of the processing. Furthermore, we store personal data only as long as needed to fulfil our statutory retention obligations. This may be, for example, the seven-year tax assessment retention period under the Federal Fiscal Code (BAO).

Note:
Not only the unlawful processing but also the loss of personal data can be an infringement of data protection regulations.

Don´ts:

- Never simply dispose of paper documents or data media containing personal data by placing them in the waste-paper bin.
- Never randomly delete documents from shared drives.
- Never randomly destroy letter or email correspondence.

Do´s:

- Regularly check to determine which data or documents are no longer needed, and destroy or archive them.
- Use the containers provided to dispose of documents. These will be securely destroyed later by a specialist disposal company.
- Alternatively, a shredder with an adequate level of security (cross-cut at least) can be used to destroy paper documents.
- If data media are not longer needed, please contact the IT department.

6. To whom can I forward personal data?

The forwarding of personal data to third parties also qualifies as processing under data protection legislation. Forwarding is governed by the applicable data protection provisions and may in particular only take place if there are legal grounds for the transmission. Data may only be forwarded outside the EEA if special conditions are met.

The contract with the customer generally serves as the legal basis for this. The question of the need to forward data for the fulfilment of a specific contract is of great importance.

Special case - application documents:
Care is also required in connection with job application documents. Applicant details must only be used for the purpose of the hiring process. Any additional record-keeping requires the consent of the applicant.

Don´ts:

- Do not forward personal data from customers or your colleagues to people outside the company unless this is absolutely necessary for the performance of your job.
- Also, only share internally with your colleagues those personal data which are absolutely necessary for the performance of your job or are needed for efficient collaboration within the team.

Do´s:

- Always store documents containing personal data only in the storage locations provided for that purpose and with restricted access rights.
- At the end of the application process, delete application documents sent to you for review, and do not file these on shared drives during the application process either. If the applicant has agreed to a record being kept, you can, if necessary, request the documents again from the HR department.
- If in doubt, ask your line manager whether the personal data for particular people (groups) may be made accessible. This applies especially if the recipient is located outside the EU.

7. How do I deal
with an inquiry from **a data subject**?

The person affected by the processing of personal data has a number of data subject rights. As data controllers, we have to answer questions regarding the assertion of data subject rights in accordance with the applicable data protection regulations and, if the conditions are met, to comply with the wishes of the data subject.

The data subject may assert the following rights:

- Right to **information** about their personal data
- Right to **correction** of their data, if incorrect or incomplete
- Right to **erasure** of their data if the processing was inadmissible or the data are no longer needed for the purpose collected
- Right to **data portability**
- Right to **revoke** previously granted **consent**
- Right to **object** to processing under certain conditions
- Right to **restrict processing**

Notwithstanding these rights, the data controller must provide the data subject with information, especially about the extent, purpose and legal basis for the processing. We comply with our information obligations by means of comprehensive data protection explanations (e.g. on the website), and by relevant data protection notices at relevant locations.

Data subjects may also **lodge complaints with the data protection authorities**.

If we receive a request from a data subject to assert their data protection rights, we must respond to this within one month. Here, the data subject is usually informed of receipt of their request, followed by the request being checked for legality by our data protection experts, and subsequently processed and answered in collaboration with our IT experts.

Don´ts:

- Never ignore a data protection request from a customer.
- Never answer written inquiries on data protection matters or data subject rights yourself but forward these as quickly as possible to our central data protection mailbox (datenschutz@welser.com). Leave the acknowledgement of receipt of the inquiry and the answer to our experts.

Do´s:

- Forward inquiries on data protection topics to our central data protection mailbox (datenschutz@welser.com). Only in this way can a timely decision be made on which further steps are needed, and these implemented within the statutory time limit.
- It is irrelevant here whether the inquiry relates to general questions on data protection at Welser or to the assertion of data subject rights such as a request for information.
- If you receive an inquiry by phone, advise the inquirer to send a written request to the central data protection mailbox (datenschutz@welser.com).

6. What is the procedure in the event of an infringement of **data protection regulations**?

If there is an infringement (data breach) of data protection regulations, it is important to respond quickly, objectively and correctly to the occurrence and to take the necessary action. This is the only way to minimise the risk to the rights of the data subject and so comply with the relevant statutory reporting deadlines.

A data breach has occurred, for example, if

- a file of documents containing personal data has been accidentally left on a train
- a USB stick containing personal data has been lost
- the company mobile or laptop of an employee has been stolen
- a phishing email has obtained access to employee accounts
- an email with personal content has been sent to the wrong recipient

Don´ts:

- Never conceal a data protection incident, no matter how insignificant it seems to you. Only our data protection experts can judge the severity of the incident and the associated risks. They can proficiently assess whether a report to the supervisory authorities and/or the data subject is needed and what further action should be taken.

Do´s:

- Report any data protection incident promptly to our data protection contact people
- Describe the incident truthfully and in detail
- For your own protection, carefully document the incident and your reporting of it
- Also encourage your colleagues to disclose data protection incidents

welser profile

We take responsibility
for our employees

Imprint: © Welser Profile GmbH
Prochenberg 24 • A-3341 Ybbsitz / Österreich
Layout and Outwork: Welser Profile
1st edition-DE-06.2019

www.welser.com