Content Unit

[Personal data protection]

Project: B-SAFE
Number: 2018-1CZ01-KA204-048148
Name of author: bit schulungscenter
Last processing date: 14.8.2020

Funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

Personal Data Protection

First introduction

Data is valuable and the possibilities of data collection and processing have increased rapidly in the digital age. Therefore, data privacy is an issue that affects us all. Did you know that Europe's data protection regulators have received more than 95,000 complaints about possible data breaches since the adoption of a landmark EU privacy law in May 2018?

Would you also like to be able to assert your data protection rights if necessary? Then basic knowledge of the protection of personal data is an important prerequisite! Furthermore, data breaches can have existentially threatening consequences for companies, which is why you as an employee need to have basic knowledge of data protection.

Practical relevance – This is what you will need the knowledge and skills for

After completing this content unit you will have a basic understanding of data privacy and data security so that you be able to comply with data protection regulations in your professional life and, as a private individual, gain more control over your own data.

Overview of learning objectives and competences

In LO_Personal data protection_01 you will learn about the purpose of data privacy and the legal basis of data protection in Europe. In LO_Personal data protection_02 you will receive information about the material scope of application of the GDPP. In LO_Personal data protection_03 you will learn under which conditions the collection and processing of personal data is legally permitted and which principles must be observed. In LO_Personal data protection_04 you will become familiar with the duties of the data controller and processor in the event of a data breach. In LO_Personal data protection_05 you will learn about the rights of data subjects. In LO_Personal data protection_06 you will receive information about important protection goals and measures to protect data in practice. In LO_Personal data protection_07 you will learn how you can contribute to improve data protection in your company.

Learning objectives	Fine objectives

LO_Personal data protection_01: You know the purpose of data privacy and the European legal basis	FO_Personal data protection_01_01: You can give a definition for the term data privacy. FO_Personal data protection_01_02: You can explain the purpose of data privacy. FO_Personal data protection_01_03: You can explain what the GDPR is about and what its territorial scope is. FO_Personal data protection_01_04: You can define the difference between the terms data controller and data processor FO_Personal data protection_01_05: You can explain what the one-stop-shop mechanism is about and what consequences data protection violations can have.
LO_Personal data protection_02: You know the material scope of application of the GDPR	FO_Persoanl data protection_02_01: You can explain what is covered by the term data processing according to the GDPR and give examples of when the GDPR does not apply despite the personal nature of the data processed. FO_Persoanl data protection_02_02: You can explain what is meant by personal data and what is sensitive data.
LO_Personal data protection _03: You know the principles and conditions for data processing	FO_Personal data protection _03_01: You can name important principles of data processing according to the GDPR and the consequences of violation of these principles. FO_Personal data protection _03_02: You can give examples of lawful basis that allow data processing of non-sensitive personal data. FO_Personal data protection _03_03: You can explain what has to be considered if the consent of the data subject is used as the legal basis for data processing. FO_Personal data protection _03_04: You can use examples to explain when the processing of sensitive data is allowed.
LO_ Personal data protection _04: You know the duties of data processors and controllers in the event of data protection violations.	FO_ Personal data protection _04_01: You can explain what is meant by data breach. FO_ Personal data protection _04_02: You can explain what data processors and data controllers must do in the event of a data breach.
LO_Personal data protection_05: You know the rights of data subjects	FO_Personal data protection_05_01: You can name rights of data subjects. FO_Personal data protection_05_02: You can explain what the right to be informed and the right of access mean and describe how to proceed with a request for data protection in general. FO_Personal data protection_05_03: You can give a basic explanation of what the right of rectification, the right of deletion or to be forgotten, the right to restrict processing and the

	right to data transferability mean, who is entitled to exercise these rights and what to consider in terms of costs and consequences.
LO_Personal data protection_06: You know data protection measures that have to be undertaken by the data controller and processor.	FO_Personal data protection_06_01: You can explain the meanings of the terms privacy by design and privacy by default. FO_Personal data protection_06_02: You can name important data protection objectives. FO_Personal data protection_06_03: You can explain what the term TOMs stands for, who is responsible for their implementation according to the GDPR and give examples of TOMs. FO_Personal data protection_06_04: You can give practical examples of data protection measures.
LO_Personal data protection_07: You know how you can contribute to data protection in your company	FO_Personal data protection_07_01: You can explain how to put a clear desk / clear screen policy into practice. FO_Personal data protection_07_02: You can give some criteria for a secure use and handling of passwords.

1.Build knowledge - Purpose of data privacy and European legal basis

In times of increasing digitalization and with the rise of the data economy, the protection of personal data is one of the key issues. It is therefore all the more crucial for everyone to know what the term **data privacy** actually stands for.

Definition
Data privacy, also known as information privacy, is an aspect of data security that deals with the proper handling of **personal data**. It refers primarily to the protection of individuals' personal data against misuse.

Data privacy can thus be interpreted as the right to decide for yourself,

- who
- at what time and
- to what extent

has access to your personal data.

The purpose of data privacy is therefore to ensure the **privacy of individuals**.

Did you know that the protection of personal data has been a **fundamental right** in Europe for years? In recent years, however, data protection has become even more important in practical terms. Technical developments and global networking facilitate the collection, processing, storage, dissemination and analysis of data.

Example
In the USA, there are already some very successful companies that specialize in collecting personal data. The records include, for example, name, gender, political affiliation, income and much more. Banks, insurance companies or other businesses buy this data to get background information, make credit decisions or optimize marketing activities.

You may be familiar with the scandal surrounding Camebridge Analytics, which is said to have used such data to significantly influence the elections of US President Trump?

Examples such as these clearly show that data privacy is important so that people **stay in control** of their personal information. Therefore, the main objective of the **General Data Protection Regulation (GDPR)** is the protection of **personal data.**

Since 25 May 2018, the GDPR has been in force.

As a European regulation, it is directly - i.e. mandatory - applicable in **every European member state**. National laws are therefore only of a supplementary nature. However, the GDPR also contains certain opening clauses (e.g. age limits can be shifted by national laws).

What is GDPR exactly? It is a legally binding regulation on the protection of individuals regarding the processing of **personal data**. The protection of company data only plays a role if it is personally identifiable (e.g. the data of employees, customers, suppliers).

GDPR aims to strengthen the rights of individuals, harmonise data protection law in the EU and improve the enforceability of data protection by uniform enforcement and high fines.

In order to give individuals more control over their personal data, the GDPR applies not only to all processing of personal data carried out **by organisation within the EU, but also to organisations outside the EU** offering goods and services to citizens of the EU. So if you are wondering whether the EU's strict data protection guidelines also apply to, for example, US-based search engine operators offering their services to European citizens or social networks such as Facebook, the answer is yes.

It is important that you are familiar with some important terms introduced in GDPR. Let's take a closer look at them now:

Definition
A **data controller** is the person (or business) who decides on the purposes and ways of processing personal data, whereas a **data processor** processes personal data on behalf of the controller (excluding the data controller's own employees).

There can be differences in certain regulations, depending on whether a data processor or a data controller is involved (e.g. if data subjects want to exercise their rights).

The GDPR also stipulates that there must be at least **one independent data protection supervisory authority** in each member state responsible for monitoring the application of data protection law.

Important
In the case of cross-border data processing, the one-stop-shop mechanism applies. This means that EU citizens can always complain to the **data protection authority of their Member State**, regardless of the Member State in which the data was misused.

Do you believe that your privacy rights have been violated? Then you can file a complaint with your national data processing authority, which is empowered to impose a number of **sanction.**

Important
It is important to note that the GDPR has **significantly increased the fines** for those who break the rules. In extreme cases, these fines can now amount to up to 20 million euros or, in the case of companies, up to 4% of the worldwide turnover of the previous financial year.

With these figures, you can imagine how much more important data protection compliance has become for businesses.

1.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_01_01

Situation: What is the term data privacy about?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **Data privacy is also known as information privacy.**
- Data privacy is primarily dealing with the proper handling of confidential company data and its protection against misuse.
- **Data privacy can be interpreted as the right of any person to decide for him/herself who has access to personal data, when and to what extent.**
- Data privacy has nothing to do with data security.

Exercise SINGLE CHOICE

Associated fine objective: FO_01_02

Situation: Data privacy is important for which of the following purposes?
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- Data privacy is important so that banks can make better credit decision.

- **Data privacy is important so that people stay in control of their personal information.**
- Data privacy is important so that companies can optimize their marketing activities.
- Data protection is important so that companies are no longer allowed to process personal data at all.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_01_03

Situation: What is the GDPR and under which conditions does it apply?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **The GDPR is a European regulation which is directly applicable in every European member state.**
- The GDPR is a European regulation that member states that do not have their own national data protection law can voluntarily comply with.
- The GDPR applies to all confidential company data such as company secrets or price and cost calculations.
- The GDPR applies only to companies based in a European member state and therefore is not applicable to Facebook, Google or other large corporations based in the USA.
- **The GDPR aims to strengthen the rights of individuals and harmonise data protection law in the EU.**

Exercise MULTIPLE CHOICE

Associated fine objective: FO_01_04

Situation: What is understood by a data processor and what is meant by a data controller according to GDPR?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **A data controller decides on the purpose and ways of processing personal data.**
- A data processor decides on the purpose and ways of processing personal data.
- **A data processor processes data on behalf of the data controller.**
- The employees of a data controller are usually considered as data processor.
- A data controller processes data on behalf of the data processor.

Exercise SINGLE CHOICE

Associated fine objective: FO_01_05

Situation: The Austrian Josefa H. is convinced that her data protection rights have been violated by the German company Easyshop. Which of the following statements are correct?
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

- Josefa H. has to contact the data supervisory authority in Germany in order to claim her data protection rights, as Easyshop is based in Germany.
- **The data protection authority can impose high penalties of up to 20 million euros for serious data protection violations.**
- Due to the different legal situation in the area of data protection in Austria and Germany, Ms. Josefa H. should first find out in which of the two countries her data protection complaint could be more successful.

- Ms Josefa H. should definitely look for a lawyer, because as a private individual you unfortunately cannot turn to data supervisory authorities.

2.Build knowledge - Material scope of application of the GDPR

You already know that the **GDPR** applies as soon as **personal data of natural persons** are processed. The term **processing** is interpreted quite broadly.

Definition
According to the GDPR, you "**process**" personal data as soon as you collect, record, organize, arrange, store, adapt, change, read out, query, use, disclose, compare, link, restrict, delete or destroy it by transmission, processing or any other form of provision.

In this context, it does not matter whether such processing is **wholly or partially automated**. The GDPR may even apply to **non-automatic processing** of personal data (e.g. in paper form). This is the case if the data is stored or **is to be stored in a structured file system**.

Are you wondering what is considered a file system by the GDPR? In accordance with the GDPR any collection of personal data organized according to certain criteria already represents a **file system.**

Example
The scope of application of the GDPR includes, for example, questionnaires, catei cards or files which are sorted according to the names of persons. Whereas a bunch of disordered notepads with personal data is only recorded by the GDPR if it is intended to be filed in a structured manner at some point.

The background to these regulations is to ensure that the level of protection should not depend on the data processing techniques used.

If you are considering whether your private notepad with the phone numbers of friends and family is subject to the GDPR - don't worry. The data protection law **does not apply** in areas of data processing within the scope of **exclusively personal or family activities**, nor does it come into force in certain special cases such as activities in the field of national security.

As you already know, the GDPR deals with the protection of personal data. But what exactly does **personal data** stand for?

Definition
Personal data is any information relating to an identified or identifiable natural person ("data subject").

If you take a look at the following examples, you will quickly notice that in practical terms **personal data** simply covers anything that in **any way allows a reference to a natural person**.

Example
Examples of personal data: • a name • family status • date of birth and age • a home adress, a telephone number, an email address • account or credit card number

However, it makes a big difference under data protection law whether it's about protecting your e-mail address or your medical history, for example. So-called **sensitive data** receive increased protection.

Definition
Sensitive data is a **special category** of personal data that reveals - racial and ethnic origin, - political opinion, - religious or philosophical beliefs or - union membership. This also includes the processing of genetic or biometric data or data on the health or sexual life of a natural person.

Example
Examples of sensitive data are medical records, fingerprints and iris scans or religious credentials.

This data is particularly worth protecting. Therefore, the processing rules for sensitive data are **extremely strict**.

2.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_02_01

Situation: In which of the following cases does the GDPR apply?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **A marketing company collects names and e-mail addresses by telephone call and stores them electronically.**
- **A small craft business keeps a customer list (names and telephone numbers) in paper form.**
- The civil servant Lisa S. is a member of a national security authority. In the course of her work she evaluates telephone logs.
- **Peter P. has recently been promoted to managing director of a long-standing family business. He wants to concentrate on new business areas and therefore deletes numerous entries from the existing customer database.**
- The student Sarah K. notes down the contact details of several fellow students.
- **The employee Maria S. evaluates the results of a written customer survey. The survey was conducted by means of questionnaires in paper form. The customers were asked to give their postal code, but giving their name was optional.**

Exercise MULTIPLE CHOICE

Associated fine objective: FO_02_02

Situation: Which of the following data are personal data?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- Name of a person
- Date of birth
- Address of a person
- Company location
- Income
- Sales figures
- Employee photo on company homepage
- E-mail addresses of a person
- E-mail address of a company

Exercise MULTIPLE CHOICE

Associated fine objective: FO_02_02

Situation: Which of the following data is sensitive data?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- Fingerprint
- Medical history
- Age
- Account details
- sexual orientation
- Union Membership

3.Build knowledge - Principles and conditions for data processing

The GDPR defines **seven key principles** that must be strictly complied with in data processing:

1. Data must be processed **lawfully, fairly and in a transparently.**
2. Data may only be processed for **specified, explicit and legitimate purposes.**
3. The processing of data must be **limited to what is strictly necessary.**
4. Data must be **accurate** and up to date.
5. Personal data must be kept in a form which permits identification of the data subjects **only for as long as is necessary for the purposes** for which they are processed.
6. Personal data must be protected against **unauthorised processing** and **against accidental loss or damage** by suitable technical (e.g. backups) and organisational measures (e.g. access authorisations). .
7. The **controller** must **be able to prove compliance** with the data protection principles.

Important
Violations of these principles are likely to result in **maximum penalties.**

Did you know that the **processing of personal data is prohibited in general**, unless specific conditions are met? For non-sensitive personal data the GDPR has **a total of six available lawful basis for processing**:

1. **Processing is necessary to fulfil a contract** – e.g. processing of customer address data for online purchases

2. **Processing is necessary to satisfy a legal obligation** – e.g. employer's duty to record working time
3. **Processing is needed to protect someone's life** – e.g. in the event of epidemics or natural disasters
4. **Personal data are processed to carry out specific tasks in the interst of the public** or in the exercise of offical authority which are laid down by law – e.g. in the context of police queries
5. **Processing is necessary for your legitimate interests** or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests – e.g. video surveillance of the company premises to protect against burglary
6. **Consent of the individual concerned** – e.g. by signing or ticking a box on a website.

Important
Declarations of consent can be **revoked** by the persons concerned **at any time**!

If consent is to be used as the lawful basis, certain requirements must be met and the **age of the data subject** must also be taken into account.

Important
In the case of persons who have not yet reached the age of **16**, the consent of their parent or legal guardian is required. A lower age treshold for obtaining parental consent may be estabilshed by EU member states but this will not be below the age of 13.

Special requirements apply to the processing of **sensitive data**. Data processing is only permitted in **very specific exceptional cases**, e.g. in the event of an accident due to vital interests or if the personal data have obviously been published by the data subject.

3.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_03_01

Situation: As an employee of a consulting firm you process various customer data. What should you be aware of?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **the processing of personal data must be limited to what is strictly necessary**
- existing personal data must not be updated
- **personal data may not be stored for an unlimited period of time**
- **the data must be protected against unauthorised processing**
- **maximum penalties are likely to be imposed in the event of a breach of fundamental data protection principles**

Exercise MULTIPLE CHOICE

Associated fine objective: FO_03_02

Situation: In which of the following cases is the processing of personal non-sensitive data covered by one of the six legal bases and therefore permitted?

Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **A customer buys a new kitchen and wants it delivered to his home. The salesperson notes the customer's address and stores it in the customer database.**
- **In a company, the working hours of all employees are recorded and processed.**
- **A customer agrees to the processing of his personal data and signs a declaration of consent.**
- A sports club publishes the birth dates of its members' newborns and their wedding dates in a club newspaper.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_03_03

Situation: Imagine that you want to process personal data. Due to the lack of other legal bases, you will need the declaration of consent of the persons concerned. What should you take into account?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **Consent may be withdrawn by the data subject at any time.**
- **For persons who have not yet reached the age of 16, the consent of a parent or guardian is required for valid consent.**
- EU member states may set a higher age limit for obtaining parental consent.
- **EU member states may set a lower age limit for obtaining parental consent.**

Exercise MULTIPLE CHOICE

Associated fine objective: FO_03_04

Situation: In which of the following cases is the processing of sensitive data allowed?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **An unconscious person is taken to hospital following an accident. Data such as blood group, age or allergies are processed.**
- **A homosexual person speaks openly about his or her sexual orientation in a television interview.**
- In none of the cases, since the processing of sensitive data is strictly prohibited without exception.
- The processing of sensitive data is only allowed in one case, namely if the data subject gives his/her consent.

4.Build knowledge - Duty to notify of data breaches

Suppose you start your working day as usual, but are suddenly confronted with the following events:

- there has been a hacker attack on your company server, allowing unauthorized persons to gain access to personal data or
- there was a break-in into a company car - notebooks with personal data were stolen.

These events pose a threat to the protection of personal data.

Definition
Incidents that could lead to accidental or unlawful destruction, loss, change or unauthorized access to personal data are referred to as **data breaches**.

It is the duty of each **data processor** to inform the data controller immediately of any data breach.

Important
If a data breach occurs, data controller must fulfil a **reporting and notification obligation.** This means: • The **data protection authority** must be informed within **72 hours** of becoming aware of the violation if this is likely to pose a risk to the rights and freedoms of the data subjects. • The **additional notification of the data subjects** is always necessary if there is likely to be a **high risk** for the rights and freedoms of the data subjects - e.g. if sensitive data were affected by the data breach.

4.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_04_01

Situation: What is considered a data breach in terms of the GDPR?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **Unauthorized persons have gained access to personal data due to a hacker attack.**
- **An employee has deleted numerous customer data by mistake.**
- A laptop containing important statements about the company's new marketing strategy was stolen.
- **An employee of a recruitment agency lost a USB stick, on which, among other things, numerous CVs and notes on the personal situation of customers were stored.**

Exercise MULTIPLE CHOICE

Associated fine objective: FO_04_02

Situation: A cyber attack occurred at a health insurance company. Hackers have gained access to numerous health data of the insured. What is the procedure according to the GDPR?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **There is a high risk to the rights and freedoms of the persons concerned, so the data controller must also notify the person concerned of this incident.**
- **The data controller must inform the data protection authority within 72 hours.**
- The data processor shall notify the data controller within 72 hours.
- The data processor must notify the data protection authority within 72 hours.
- This is not sensitive data, so it is sufficient to notify the data protection authority. The data controller may waive the notification of the data subject.

5.Build knowledge - Rights of data subjects

The GDPR expands **the rights of data subjects**. You should be aware of these rights so that you can exercise your rights and react in accordance with the law in the event of data protection queries to your company. As you can see form the graphic, the GDPR provides the following rights for individuals:

But what do these rights actually mean in practice? Let us have a closer look:

Let's start with the **right to be informed**. If your personal data are processed, **at the time of collection of your data** the data controller is obliged to provide you with **certain information**, including in particular:

- **who** is processing your data (name and contact details)
- **what data** they are processing,
- **why** they are porcessing it and
- for **how long** the data will be kept

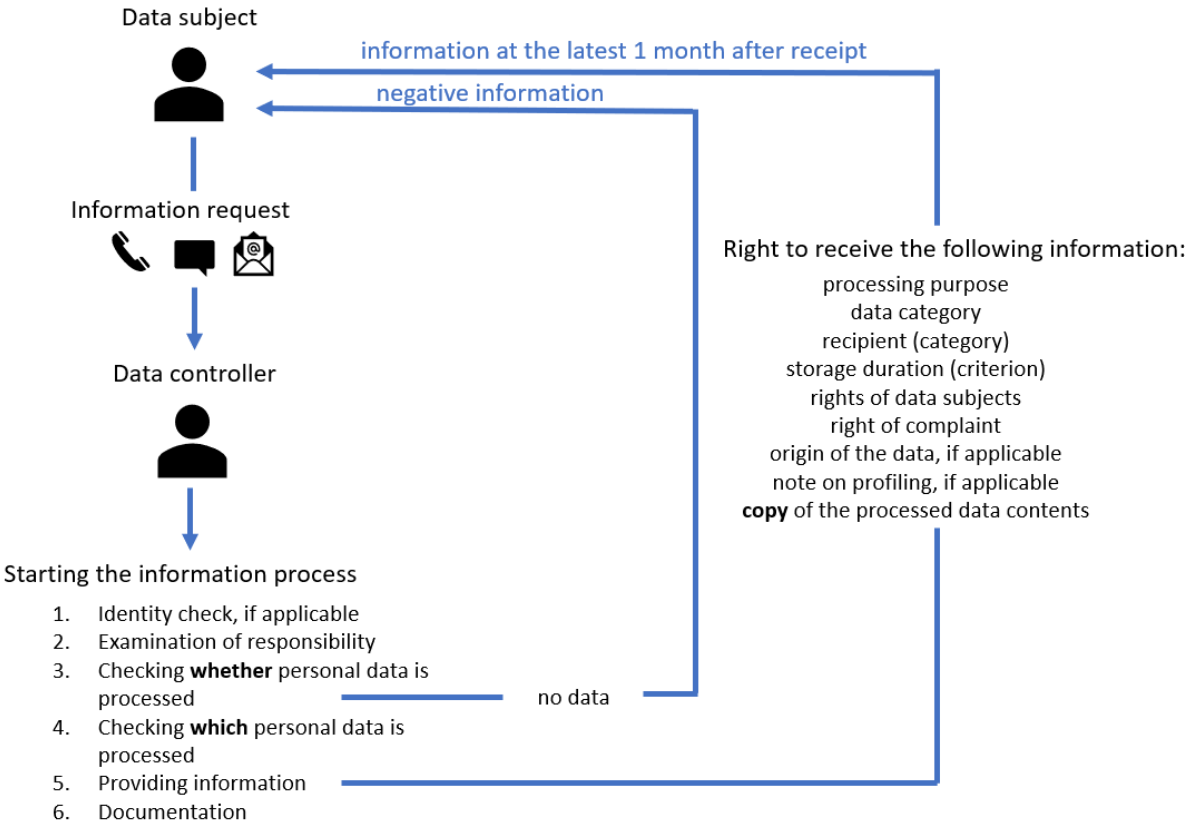
Furthermore, the GDPR requires that **the information** is provided to you

- in a precise, transparent and easily accessible form

- in clear and simple language and
- free of charge

In order to fulfil the right to information, data controllers must **actively** provide individuals with certain information. In contrast, the **right of access** entitles any data subject to obtain a copy of their personal data and other complementary information regarding data processing.

The following graphic shows the correct response when a data subject wishes to exercise his/her right of access:



As you can see form the graphic, the request for information can be made in person, in written or by telephone. It is important to clarify the **identity** of the person making the request beyond all doubt.

The next step is the **examination of responsibility**.

Important
Data subject rights can only be asserted with **data controller**! However, as the data processor has **a support obligation ,** the data protection request should be forwared directly to the **data controller.** Without express instructions, you as an employee are **not authorized to provide information about personal data**!

As you may have already noticed from the graphic, the data controller must respond to the request to exercise the right of access if no personal data is processed (**negative information**). However, if personal data are actually processed, individuals have the **right to access that data**, be provided with a copy of the personal data being processed and get any relevant additional information.

Important
In case of a data protection request the time limit for providing information is in principle **only one month** after receipt of the request.

Note
The regulations that have been learned so far with regard to - form of data protection request (written, electronic, personal, telephone) - obligation to verify the identity of the data subject in case of doubt - responsibility of the data protection request (only the data controller) - deadline for the data protection response (1 month) apply equally to ALL rights of the data subjects!

The **right to rectification** gives individuals the right to ask for incorrect, inaccurtate or incomplete personal data to be corrected.

Individuales can request **the deletion of personal data** if, for example, the data processed by the company is no longer needed or if the data has been used unlawfully. This right also applies **online** and is often referred to as the **'right to be forgotten'.** This right obliges data controller to take all reasonable steps to remove publicly disclosed personal data.

The **right to restrict processing** is a right which can only be exercised under **certain conditions**. Examples include an objection by a data subject to data processing wherby the decision on the objection is still pending or a dispute as to the accuracy of the data.

The **right to data portability** is intended to ensure that individuals can request the transmission of the personal data they have made available to a data controller in a structured, common and machine-readable format. The right only applies when the data are processed on the basis of consent or a contract. You can also ask for personal information to be transferred directly to another data controller, when it's technically feasible.

Example
Suppose you want to change your email provider. The **right to data transferability** allows you to request your current email provider to send your list of contacts to a new email provider.

In principle, data subjects have the **right to object to the processing** of personal data. Wheter the right applies depends on the purpose and the lawful basis for processing. For example you always have the right to object to processing for the purpose of direct marketing. However, if data are processed, for instance, for scientific or historical research or statistical purposes, the right to object is more limited.

The GDPR provides individuals with **the right not to be subject to a decision based solely on automated processing**, including profiling.

Important
Only **natural persons** are entitled to excerise data protection rights! The exercise of data subjects' rights must be **free of charge**. Non-compliance with these rights could lead to high financial penalties.

5.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_05_01

Situation: With the GDPR, the rights of individuals are strengthened. What rights can individuals now invoke?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- Right to object
- Right to be informed
- Right to publication
- Right to data portability
- Right to rectification
- Right to access
- Right to fair payment for data

Exercise MULTIPLE CHOICE

Associated fine objective: FO_05_02

Situation: Which of the following statements concerning the right to be informed and the right to access are correct?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- The right of access entitles data subjects to receive a copy of their personal data processed.
- The right to information is exactly the same as the right to be informed.
- The right of access means that the person requesting information also has the right to be informed that no personal data concerning him/her is processed (negative information).
- The right to be informed means that the data controller must actively inform the data subjects about specific points of the data processing.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_05_02

Situation: A training company collects and processes names and contact details of course participants when they register for a course using the registration form. Which points must be observed to comply with the right to be informed?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- Participants must be informed about certain data processing issues (e.g. name and contact details of the data controller) as soon as the data is collected.
- There is no obligation to provide information, as this is not sensitive data.
- No later than 1 month after obtaining the personal data, the person responsible must fulfil his or her obligation to inform the course participants.
- In this case no declaration of consent is required. Therefore, the duty to inform is also not obligatory.
- The information must be provided to the course participants in clear and simple language and free of charge.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_05_02

Situation: A customer contacts you by phone. He wants to know what data is being processed by him in your company. How do you react?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- I answer his inquiry immediately.

- I will answer his enquiry if I know the customer and no sensitive data are processed by him.
- I will answer his inquiry if I know the customer.
- **I inform him that I personally as an employee are not allowed to provide information without explicit instructions and ask him to address his request in writing to the person responsible for data processing.**

Exercise MULTIPLE CHOICE

Associated fine objective: FO_05_02

Situation: According to the DSGVO, who is responsible for answering data protection queries from affected individuals?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- Data processor
- **Data controller**
- Employees, if they can identify the person concerned beyond doubt
- Only the data protection authority

Exercise MULTIPLE CHOICE

Associated fine objective: FO_05_02

Situation: Mr. P. has been receiving mailings for a few weeks now from a company that he is not familiar with. He therefore decides to ask this company by telephone for information about what personal data the company has about him and where the company got this data from.
Which of the following statements is correct?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **The company may ask Mr. P. for proof of identity before responding to his request for information.**
- **If Mr. P. does not receive any answer or information from the company within one month, he can lodge a complaint with the data protection authority.**
- Mr. P. can only assert his right to information in person on site, on presentation of an identity card.
- The company is entitled to claim a fee for the transmission of information in paper form. Only the transmission in electronic form must be free of charge for the person requesting information.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_05_03

Situation: Which of the following statements on the right to data portability are correct?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **Individuals can request the transmission of the personal data they have made available to a data controller.**
- **The right only applies when the data are processed on the basis of consent or a contract.**
- Companies can also claim the right to data portability.

- The right to data transferability allows you to request your current email provider to send your list of contacts to a new email provider. The costs of the data transfer are to be borne by the new email provider.
- **Non-compliance with this right could lead to high financial penalties.**

Exercise MULTIPLE CHOICE

Associated fine objective: FO_05_03

Situation: Klaus married last year and agreed that the photographer may publish wedding photos for advertising purposes on his company website. Today, Klaus is divorced and he is annoyed that by entering his name on Google, his wedding photos are visible to everyone. Which of the following statements are correct?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **He has the right to revoke his consent to the data processing by the wedding photographer.**
- **He also has the right to demand that his photos published on the Internet be deleted.**
- **Klaus ex-wife Lisa has moved out. She is entitled to demand a correction of her customer data (new address).**
- The right to restrict processing allows the wedding photographers to continue using the photos for advertising purposes.

6.Build knowledge - Data security measures

In order to ensure the protection of personal data, the issue of **data security** certainly plays a central role. Important keywords in this context **are privacy by design** and **privacy by default**.

Definition
The term **privacy by design** refers to data protection through **technology design**. This means that when developing new technologies, appropriate solutions conforming to data protection must be ensured. For example, important data protection principles, such as data minimization, must not be ignored when developing new software programs and devices. **Privacy by default** stands for privacy through appropriate **default settings.** The person responsible must ensure by appropriate default settings that only those personal data are processed, which are absolutely necessary.

Are you still not sure what data protection by design and default actually means? Let's have a look at a few examples:

Example
Privacy by design: Integration of deletion concepts in software for data processing or the use of pseudonymisation (replacing personally identifiable material with artificial identifiers) and encryption (encrypting messages so that only those authorised can read them). **Privacy by default:** For example, a provider of a social network must ensure that personal data of users are not published from the start by presetting its app. Persons who use the app should not first have to change the settings from "public" to "private".

But what can be done concretely to improve data security? You will now get to know some suitable measures at a glance:

- Definition of data protection objectives
- TOMs – technical and organizational measures

Let us now take a look at the individual measures a little closer:

Essential data protection objectives are considered to be

- **Integrity:** Data is true to the original and has not been damaged or changed by unauthorized parties.
- **Availability:** Data is available to authorized persons when and where they need it. The data processing systemis to a certain extent tolerant of malfunctions and errors.
- **Confindentiality:** The data is only accessible to authorized persons.

The GDPR requieres that the controller and the processor must implement **appropriate technical and organisational measures** (TOMS) in data processing to ensure a level of protection adapted to the risk.

As you already know, the GDPR obligates to **privacy by design and default**.

However, the precise measures to be taken to protect personal data are ultimately the responsibility of the data controller and the processor. **Examples of TOMs** are pseudonymisation and encryption of data, information and training of staff or automatic back-ups.

The following example shows how data protection measures can be put into practice.

Example
Suppose you are employed by a company that uses a **customer database.** This customer database is located on a server. In order to ensure an adequate level of protection for the personal data of customers, the following data protection measures, for example, would be conceivable: • Access to all customer data is only possible with **password and user name.** • The room in which the server is located is locked with a **key.** • Every use is **logged,** both log in and log out as well as changes to data records. A person is assigned to each login. • **Read and write rights** are only distributed as required. • If possible, customers are not recorded under a real name, but under a **user ID.** • Regular **back-ups** are made, which are also tested for integrity at certain time intervals. • All **TOMs are reviewed** on a quarterly basis. • Employees receive **clear instructions** on how to handle personal data, **basic training on data protection** and regular **specific data protection notices** by e-mail.

6.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_06_01

Situation: What is meant by the terms privacy for design and privacy by default?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- Privacy by design stands for privacy through appropriate pre-settings.
- **Privacy by default stands for privacy through suitable pre-settings.**
- **Privacy by design stands for data protection through technology development.**
- **An app is preset in such a way that personal data cannot be viewed by other users. This is an example for privacy by default.**
- In a software program, all data that is not absolutely necessary is stored anonymously. This is an example for privacy by default.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_06_02

Situation: What are the important protection goals in data protection?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **Integrity**
- **Data availability**
- Open data access
- **Confidentiality**
- High storage duration
- Data Transparency

Exercise MULTIPLE CHOICE

Associated fine objective: FO_06_03

Situation: What is meant by the term TOM and who is responsible for their implementation according to the GDPR?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **The abbreviation TOMs stands for technical and organizational measures for data protection.**
- The abbreviation TOMs stands for technically obligatory measures for data protection.
- **The data controller and the data processor are responsible for implementing suitable TOMs.**
- The data controller is responsible for the implementation of suitable TOMs.
- The data protection authority is responsible for the exact measures that must be taken to protect personal data.
- **The training of employees is an example of TOMs.**
- **Automatic back-ups or pseudonymization are examples of TOMs.**

Exercise MULTIPLE CHOICE

Associated fine objective: FO_06_04

Situation: Which of the following measures can be used in practice for data protection?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **Regular back-ups.**
- **Basic training on data protection for all employees.**
- **To get access to customer data you need a password and a user name.**
- If possible, customers are recorded under their real name and not under a user ID.
- As much data as possible is stored for as long as technically possible.

7.Data security measures – what can YOU do?

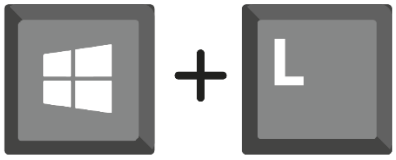
In addition to the technical component, **the personnel component** is also particularly important. Find out now how **you** can contribute to better data protection in your company:

An important data protection measure is the so-called **Clear Desk/Clear Screen Policy.**

Definition
Clear Desk Policy refers to the instruction that employees lock all confidential documents when absent and do not leave them open at the workplace. This is to prevent unauthorised persons (such as visitors, customers, cleaning staff) from having access to them.

Furthermore, all employees should be encouraged to adopt a **clear screen policy**. This means that all users are obliged to log off from the PC when leaving the workplace or to lock the PC if there are only brief interruptions.

Tip
For a quick locking of the PC in Windows operating systems it is sufficient to press the "Windows" + "L" key together.



In addition, it makes sense to configure an **automatic PC lock with password protected screen saver** for minutes of non-use.

Important
Never store your password notes directly at your workstation, e.g. under the desk pad or as post-It on the screen!

This takes us to the next important issue in relation to data protection measures: The correct use and secure handling of **passwords:**

Example
The following passwords are very negative examples, but unfortunately still very popular: • Password1 • Firstname_lastname_Date of Birth • Number chains like 123456 You should never use these passwords. They are easy to hack and therefore very insecure.

Worried that your password strength is weak? You may be right. The following aspects have to be kept in mind to create a strong password:

Note
• Length of the password (at least 10 characters) • A mix of letters and numbers, special characters, uppercase and lowercase letters • No use of first or last names, dates of birth or trival passwords like 123456 or qwertz • Change your password at reasonable intervals • Keep your password secret at all times and do not send it unencrypted by e-mail • Do not use private login passwords (e.g. for Facebook, online customer accounts) for professional purposes.

7.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_07_01

Situation: The company you work for requires a clear desk/clear screen policy. What does this mean?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **You should lock all confidential documents when you are not at your work desk.**
- **You should log out of your PC when you leave your workspace.**
- You should not save anything unnecessary on the desktop of your PC.
- **For a quick lockout of a PC with Windows operating system it is enough to press the key combination "Windows key" and "L".**
- You should not store private things on your work desk.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_07_02

Situation: What should you consider when choosing a password?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- If you are likely to forget your password, make a password note that you can always easily access (post-it at work for example).
- Try not to use any special characters.
- **Do not use the same password for private and professional purposes.**
- **Make sure to choose a password that is long enough.**
- Your last name in combination with your family name or your date of birth are relatively secure passwords.

Co-funded by the
Erasmus+ Programme
of the European Union

Sources

jusline.at: https://www.jusline.at/gesetz/dsgvo

wko.at: https://www.wko.at/site/it-safe/mitarbeiter-handbuch.pdf

wko.at: https://www.wko.at/site/it-safe/kmu-handbuch.pdf

arbeiterkammer.at: https://www.arbeiterkammer.at/beratung/konsument/Datenschutz/FAQ_DSGVO.pdf

dsb.gv.at: https://www.dsb.gv.at/documents/22758/116802/dsgvo_leitfaden.pdf/640015cb-eb90-4702-bf29-ca4fa2d32aca

wko.at: https://media.wko.at/epaper/Leitfaden-Sicherheitsmassnahmen-DSGVO/#20

wko.at: https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/datenschutz-grundverordnung-fragen-und-antworten.html#heading_1__Bin_ich_von_der_DSGVO_betroffen_

wko.at: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-oesterreichisches-datenschutzgesetz.html

bmf.gv.at: https://www.bmf.gv.at/en/data-protection.html

gdpr.eu: https://gdpr.eu/eu-gdpr-personal-data/

gdpr-info.eu: https://gdpr-info.eu/

ico.org.uk: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf)

ec.euorpa.eu: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en

cyberthreatportal.com: https://cyberthreatportal.com/types-of-data-security-measures/

Save knowledge

Summary

The term **data protection** refers to the **protection of people** against the misuse of their personal data.

The protection of personal data of natural persons is also the main objective of the European General Data Protection Regulation (GDPR). Since 25 May 2018, the GDPR has applied directly in every member state of the EU and national data protection regulations are only of a supplementary nature.

In addition to **new definitions**, the GDPR entails an **extension of data subjects' rights**, an increase in data processing obligations and stricter penalties for data protection violations. The implementation of the GDPR is monitored by independent supervisory authorities in each Member State.

The objective scope of application of the GDPR is limited to the processing of **data with personal reference**. The GDPR applies not only to data processed automatically, but also to data processed manually, insofar as this data is (or is to be) stored in a file system.

Co-funded by the
Erasmus+ Programme
of the European Union

According to the GDPR, personal data is all information relating to an **identified or identifiable natural person**. So-called **sensitive data** such as data on health status or religious or political orientation are treated as special data categories. In addition to the consent of the data subject, there are other conditions for the lawful processing of non-sensitive data as well. The processing of **sensitive data** is only permitted in exceptional cases.

A **valid declaration of consent** must be made voluntarily, for the specific processing purpose and in an informed and unambiguous manner and can be revoked at any time.

The **principles for GDPR-compliant data processing** are legality and transparency, purpose limitation, data minimization and correctness, storage limitation, integrity and confidentiality.

As soon as personal data are to be processed, the data subject must **be informed** of certain aspects of the data processing. The information must be provided to data subjects in a transparent and easily accessible form, in clear and simple language and free of charge.

The GDPR requires data protection through default settings (**privacy by default**) and data protection-friendly technology design (**privacy by desgin**).

In the case of a **data breach**, the data controller is obliged to notify the data protection authority within 72 hours if a risk to the rights and freedoms of the data subjects cannot be excluded.

The **rights of the data subjects** have been strengthened within the framework of the GDPR. So, requests for access, rectification, erasure, data portability or objection to the processing must be given attention. Only the data controller is responsible and authorized to answer data protection requests and to deal with data protection concerns of data subjects, However, the data processors have a so-called support obligation.

In order to protect data sufficiently, a **data protection concept** and the involvement **of trained personnel** are necessary. Based on this, various measures can be taken to prevent breaches of data protection laws and their serious consequences.