Commitment to data privacy and information protection 2023

Welcome

Welcome to your training 'Commitment to data privacy and information protection'

In this training, you will learn how to work safely in data privacy and information protection.

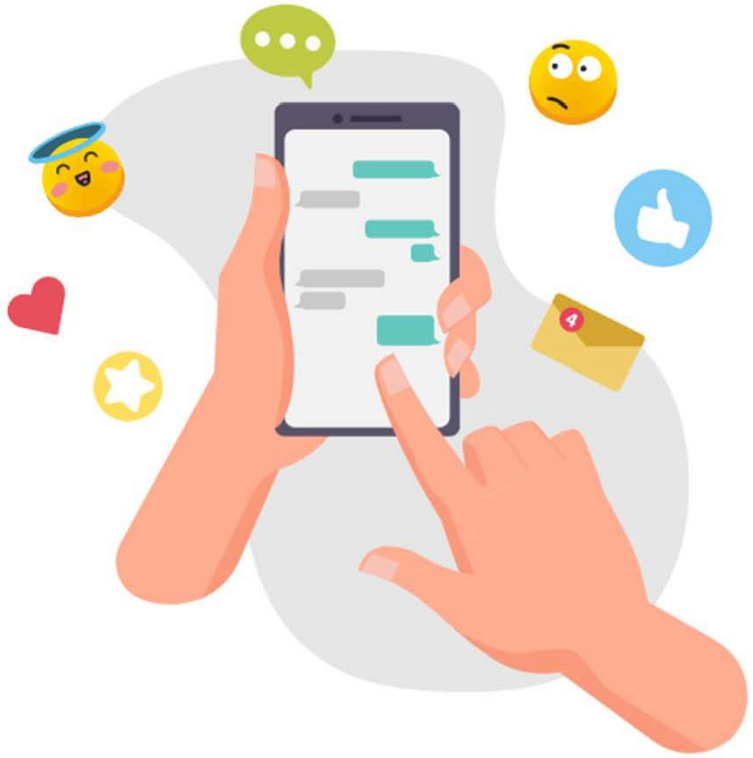
Dealing with data and information is not only the central content of Deutsche Telekom's business models, but also part of our daily work with each other. Therefore, as representatives and faces of Deutsche Telekom, we must all be particularly knowledgeable about what we need to pay special attention to when dealing with data and information. And we also need to keep ourselves regularly up to date on innovations in data and information protection!

Here we go...

You can pause your training at any time and continue it at a later time. You will receive a certificate for successful completion.

Chapter 1

Basics



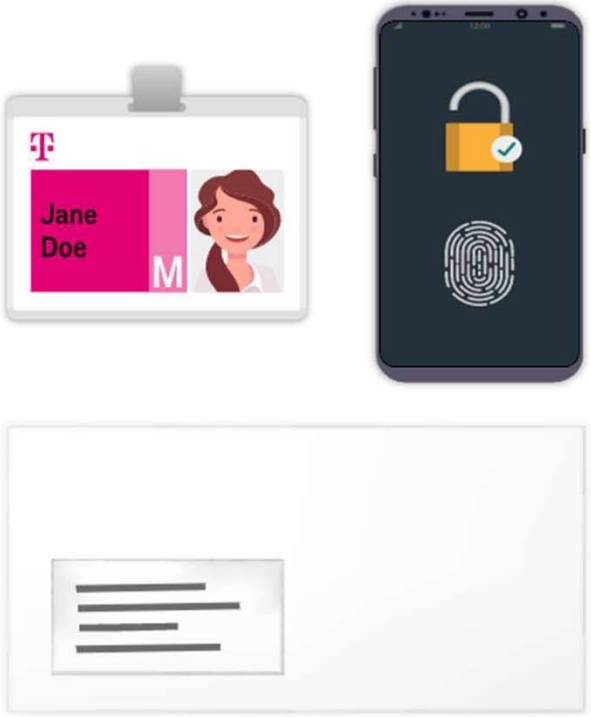
Data privacy and information protextion

In the general discussion, data privacy and information protection are often assumed to be identical, but in fact they have very different goals.

Data privacy regulates the handling of personal data - and thus protects the personal data of each individual. Data privacy essentially serves to build trust among customers and employees. Because data privacy creates an enviroment of trust!

Information protection protects our business information. This is information that we need to be able to carry out our business activities in the first place.

First, let's take a closer look at data privacy.



What is personal data?

Personal data includes all data that describe a person, make him or her identifiable or allow conclusions to be drawn about him or her; this includes, in particular, so-called individual data (such as name, address, biometric data, etc.).

Due to their close connection, personal data is part of the personality of our customers and ourselves. Just because they are our customers, we cannot simply help ourselves to their personal data when we feel like it.

More info on the info page

What is meant by permission requirement?

In principle, the processing of personal data is prohibited. However, there are - as always - exceptions to the rule:

For example, a law or legal regulation may permit data processing. Necessary data such as names, addresses or numbers may also be stored for the fulfilment of a contract, for example for a mobile phone contract or an employment contract.

The data subject himself/herself may allow data processing by giving consent (e.g. consent for a newsletter).

What is business information?

Business information includes, for example, how and why we do something, what results we achieve and, in particular, what decisions we want to make or have already made as a company.

All Telekom information that has not already been made public via the officially designated channels must be regarded as business information and protected.

A few pieces of business information can even be so important that the existence of the company can be at stake if they are 'lost', this is referred to as top trade secrets.

Information protection

Principles such as need-to-know, need-to-see or need-to-have must be observed.

Confidentiality means that information is not available or known to unauthorised persons. For this purpose, information is divided into the protection classes OPEN, INTERNAL and CONFIDENTIAL and protected accordingly.

Integrity means that information is unaltered and complete. For this purpose, information can be digitally signed.

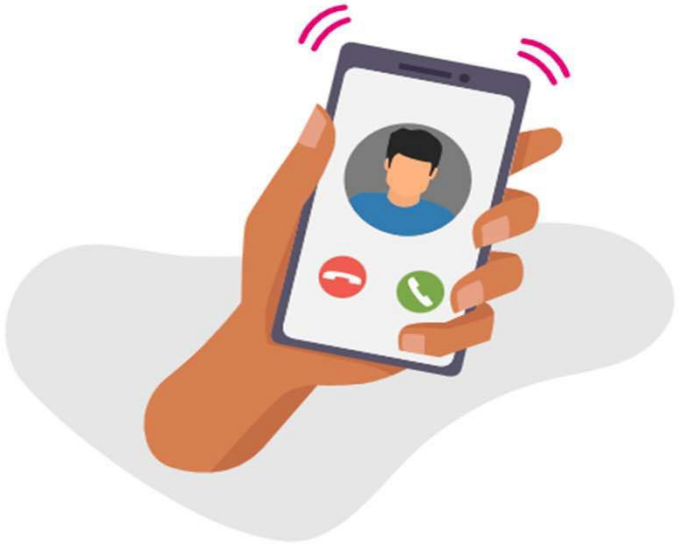
Availability means that information is accessible and usable on demand by the persons and systems authorised for it. Backups can be created for this purpose.

Principles such as need-to-know, need-to-see or need-to-have must be observed

More info on the info page

Chapter 2

Secrecy



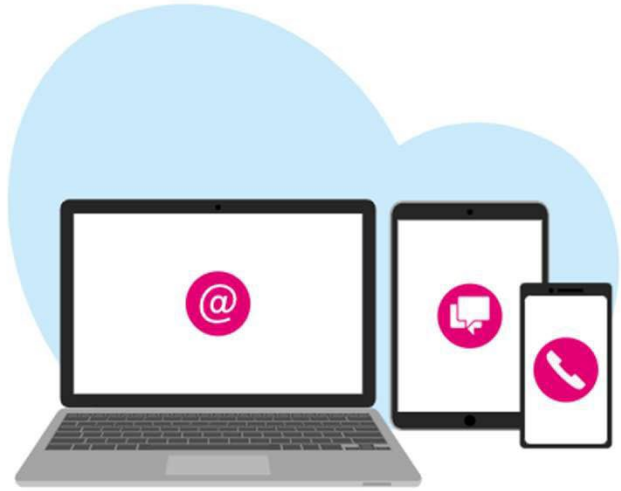
Secrecy of telecommunications

And off we go with this mysterious-sounding chapter.

As you can guess, it is first of all about the secrecy of telecommunications, which is of course a very important basis for us. Just like the right to informational self-determination, telecommunications secrecy is a fundamental right. And it functions as a comprehensive protection of all our communications. Because the secrecy of telecommunications not only protects information about the content of our conversations, but also the information that a conversation has taken place at all, i.e. who talks, writes, chats etc. with whom about what, and when.As you can guess, it is first of all about the secrecy of telecommunications, which is of course a very important basis for us. Just like the right to informational self-determination, telecommunications secrecy is a fundamental right. And it functions as a comprehensive protection of all our communications. Because the secrecy of telecommunications not only protects information about the content of our conversations, but also the information that a conversation has taken place at all, i.e. who talks, writes, chats etc. with whom about what, and when.

This is regulated by the Telecommunications Telemedia Data Protection Act.

More info on the info page



Secrecy of telecommunications

As a service provider, Deutsche Telekom has to respect the secrecy of telecommunications.

This also means that we, as employees, interns, temporary workers, consultants or other temporary contributors, are directly obliged to comply with the secrecy of telecommunications. With the obligation to maintain telecommunications secrecy, Deutsche Telekom makes this particularly clear to customers and employees.

A breach of telecommunications secrecy is punishable, not only for Telekom as a company, but also for you personally.

Therefore: Do not pass on any customer or employee data to outsiders. Never answer queries about this yourself, but forward them to privacy@telekom.de.

Business secret

And then there is the EU Business Secrets Act.

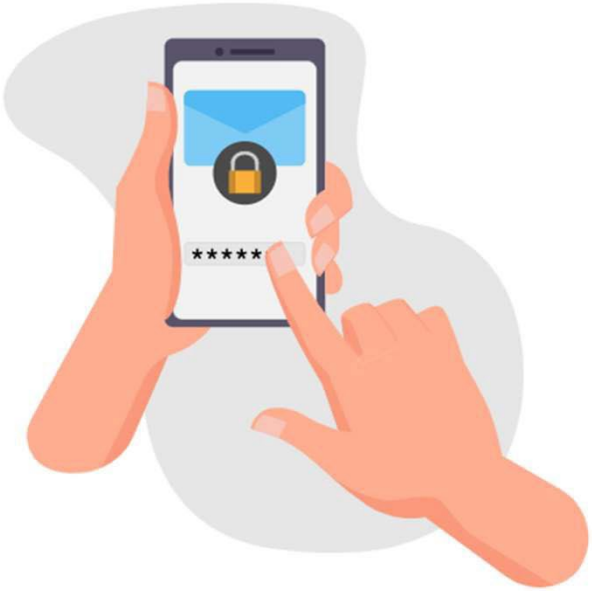
Accordingly, only business information that is also adequately protected is considered a business secret.

The law thus underlines how important it is that protective measures are observed and complied with.

Because information that is easily accessible is not covered by EU law and therefore we cannot claim protection rights for it.

If the competition can get hold of our business information quite easily and by legal means, they are also allowed to use it. In the event of a dispute, Telekom would then have to prove that there were sufficient protective measures.

More info on the info page



Business secret

And of course you are now interested in: What does that mean for me?

Business secrets can generally be classified as INTERNAL or CONFIDENTIAL; the 'Information Hub' tool helps you to classify them. The tool also tells you the protective measures to be applied.

However, protective measures should not only be applied, the application should also be appropriately documented in the case of particularly sensitive information.

For example, encrypted emails should be kept in order to be able to prove the encryption if needed.

Social secrecy

At Telekom, special sensitive data is also processed, which is subject to increased processing conditions and stricter legal requirements for permissible data processing.

Social data also falls under the concept of particularly sensitive data. Social data is often processed by Telekom for social insurance institutions, for example for pension insurance or statutory health insurance. In this context, social data is not only personal data, but also the trade and business secrets of social insurance institutions. This non-personal data is subject to data protection in the area of statutory social insurance.

This social data is particularly protected data which is subject to even stricter special data protection from the social security codes in addition to the protection provisions of the General Data Protection Regulation.

Everybody who is involved in the processing of social data in the course of their work must observe social secrecy. Otherwise they are liable to prosecution.

More info on the info page

Data of persons subjct to professional secrey

Information entrusted to 'persons subject to professional secrecy' (e.g. doctors, lawyers or auditors) in the course of their professional activities is also particularly protected data about which they must maintain confidentiality.

Any person who may come into contact with data belonging to persons subject to professional secrecy in the course of their activities is subject to the same obligation to maintain secrecy when handling this data as the persons subject to professional secrecy. If you breach this obligation, you can be prosecuted under Section 203 of the Criminal Code.
You can also be prosecuted if you do not oblige those service providers coming into contact with data of persons subject to professional secrecy in the course of their activities to maintain confidentiality.

If you handle the data of persons subject to professional secrecy, you must read the fact sheet in the information text. You can find further information in that fact sheet.

You can find further information here:

Question

You receive a request from a lawyer who wants to know whether his client used his mobile device to make a phone call to witness Y on day X. The request is answered in the following way.

Are you allowed to hand out the data?

Yes No

Question

You receive a request from a lawyer who wants to know whether his client used his mobile device to make a phone call to witness Y on day X. The request is answered in the following way.

Are you allowed to hand out the data?

No

The answer is correct:
You may not disclose this data. The data is subject to the secrecy of telecommunications, which is enshrined in Article 10 of the German Basic Law and Section 3 of the TTDSG. The secrecy of telecommunications protects who talks, writes or chats with whom and about what.

In addition, you never answer such requests yourself, but forward them to privacy@telekom.de.

Question

You have customer contact with a well-known pop star. Knowing that your daughter is a big fan and would love an autograph, you make a note of the star's address and phone number.

Is this behavior permitted?

Yes No

Question

You have customer contact with a well-known pop star. Knowing that your daughter is a big fan and would love an autograph, you make a note of the star's address and phone number.

Is this behavior permitted?

No

The answer is correct:
These data are so-called inventory data, which may only be used for the legally permitted purposes and in no case for private purposes.

Question

You can find a presentation by Telekom on the initial plans for the next mobile communications standard 6G on Facebook that is generally accessible. The presentation is marked CONFIDENTIAL and has been posted there by a Telekom employee.

Is the confidential Telekom presentation still a business secret?

Yes No

Question

You can find a presentation by Telekom on the initial plans for the next mobile communications standard 6G on Facebook that is generally accessible. The presentation is marked CONFIDENTIAL and has been posted there by a Telekom employee.

Is the confidential Telekom presentation still a business secret?

No

The answer is correct:
Since the confidential information is accessible to everyone, there can be no question of adequate protection. Thus, the information does not fall under the EU definition of a trade secret and there is no trade secret according to EU law. IMPORTANT: A presentation marked as CONFIDENTIAL may not be made public. This is an information protection incident that must be reported immediately.

Question

Do you have to maintain the secrecy of telecommunications even among colleagues?

Your colleague receives harassing calls on his smartphone. The phone number is suppressed. You know a colleague who could find it out and identify the caller. This would certainly be a valuable help for the person concerned, but is the colleague allowed to do this?

Yes No

Question

Do you have to maintain the secrecy of telecommunications even among colleagues?

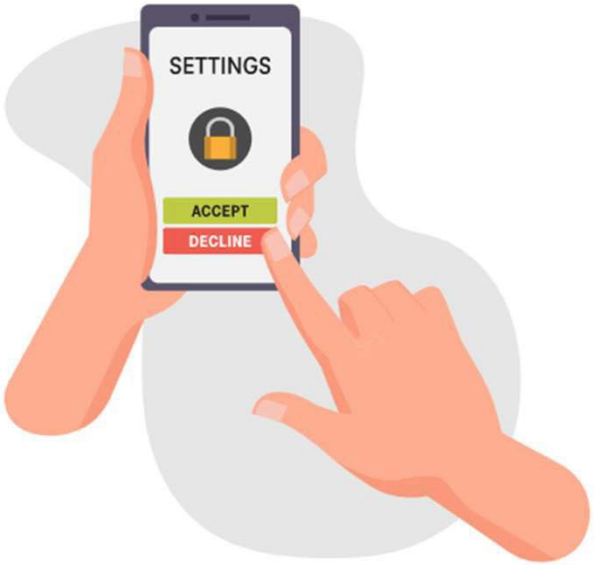
Your colleague receives harassing calls on his smartphone. The phone number is suppressed. You know a colleague who could find it out and identify the caller. This would certainly be a valuable help for the person concerned, but is the colleague allowed to do this?

No

The answer is correct:
Telecommunications secrecy is also violated if data subject to this are passed on within the group. Your colleague needs to contact the police. The criminal prosecution authorities may request information as part of the investigation.

Chapter 3

Rights and obligations

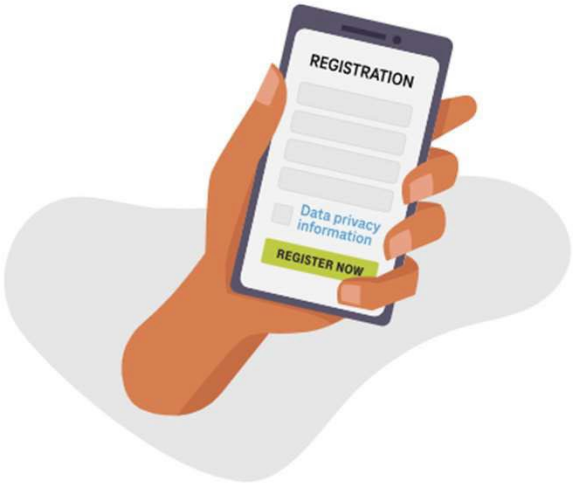


Rights of data subjects

Like our customers with us, we all have personal data stored with companies or institutions. For example, with our health insurance company or gym. And of course with our employer. And in the same way, we have some rights with regards to our data. The key words here are: informational self-determination.

And should you want to take a look at exactly what the whole thing looks like, you can find the rights of data subjects in the General Data Protection Regulation, Chapter 3, Articles 12 to 20.

Let's take a closer look at the individual rights.



Right to information

Even **before** the data is collected, for example, the customer has a right to information.

It stipulates that data subjects must be provided with information about the processing of their personal data. For example, the purpose for which the data is used, how it is stored and the rights to which the data subjects are entitled must be explained.

What is really important is that this information is provided **before** the first processing, the birth of the data, so to speak. All of this can be found in the privacy notices - which you are probably familiar with from apps or websites.

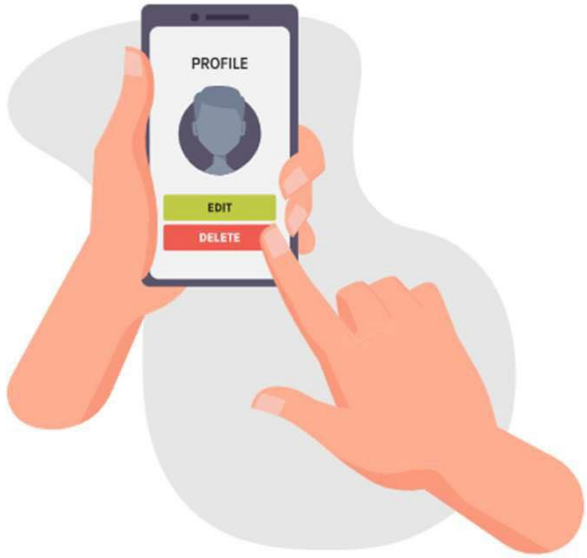
If you want to know more about the duty to inform, feel free to read on here.

More info on the info page

Right to demand information

Now the data is recorded and used in accordance with the agreed purpose - for example, as part of a mobile communications contract. Throughout the entire period of use, data subjects can ask at any time, free of charge, what personal data is stored.

Customer inquiries are answered by the team at privacy@telekom.de.



Right to erasure

If data is no longer needed for the agreed purpose, if data subjects have successfully objected to its use, or if unlawful use has come to light, then data subjects can demand that the data be deleted.

In this case, we have the obligation to delete the data.

Duties for information protection

Everyone is responsible for protecting information within their sphere of responsibility, influence or control.

For each piece of information there is a person responsible (so-called information owner). This is the person or entity that created the information or is responsible for its existence.

The information owner decides on the basis of the existing criticality whether the information is classified as INTERNAL or CONFIDENTIAL and whether any special measures should be applied to protect it.

Only tools, services and systems that have been approved by security management may be used to handle confidential information.

More info on the info page

Chapter 4

Reporting of incidents

Data protection incident

Mishaps or mistakes happen always and everywhere:

A customer accidentally receives an order confirmation that was intended for another customer, employees have access to customer data that they should not have, or customer data is stolen in a hacker attack.

These examples involve a data security incident, i.e., a data breach that results in a personal data breach.

Data protection incident

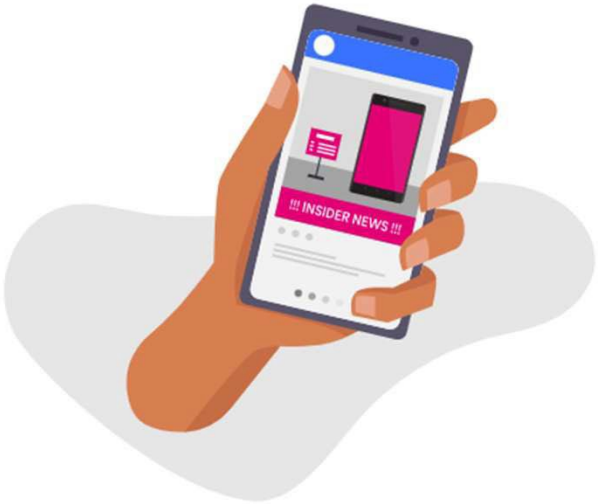
Failure to report can cause great damage to the company, because Telekom is legally obligated to report every data protection incident.

A data protection incident must be reported to the competent data protection supervisory authority within 24 (telecommunications) or 72 hours (GDPR).

Therefore: Please report all data protection incidents to the departmental mailbox at privacy@telekom.de.

Make a report even if you are not completely certain whether a data protection incident has occurred - better safe than sorry. Indeed, to minimize damage, it is important that potential incidents are reported promptly.

More information on this subject can be found in the information text.



Information Protection Incident

If you find that sensitive business information could be lost:

- because, for example, a Telekom presentation on network expansion was published on the internet with the label CONFIDENTIAL, or
- Detailed information about a Telekom product that is not yet on the market is already being posted on Facebook

please report it immediately.

The examples are information protection incidents. Please report it to the functional mailbox security@telekom.de.

More info on the info page

Question

You find the holiday list with private telephone numbers and e-mail addresses of a Telekom team in an Internet forum.

Do you need to take action here?

Yes No

More info on the info page

Question

You find the holiday list with private telephone numbers and e-mail addresses of a Telekom team in an Internet forum.

Do you need to take action here?

Yes

The answer is correct:
You must take action here, because this could be a data protection incident that must be reported to the competent supervisory authority within 72 hours. Telekom is legally obliged to report every data protection incident. Therefore: Please report all data protection incidents via the functional mailbox privacy@telekom.de.

More info on the info page

The rule here is: better once too much than once too little.

If you are not sure whether it is a data protection or information protection incident, simply report it to one of the mailboxes mentioned. The experts will check your report and then take all further steps.

te telephone
a Telekom team in

Yes

The answer is correct:
You must take action here, because this could be a data protection incident that must be reported to the competent supervisory authority within 72 hours. Telekom is legally obliged to report every data protection incident. Therefore: Please report all data protection incidents via the functional mailbox privacy@telekom.de.

More info on the info page

Question

In LinkedIn, you have shared a piece of information that, in retrospect, you are no longer sure you should have shared.

Do you have to do something?

Yes No

More info on the info page

Question

In LinkedIn, you have shared a piece of information that, in retrospect, you are no longer sure you should have shared.

Do you have to do something?

Yes

The answer is correct:
You must take action here, because this could be an information protection incident. Report it via the functional mailbox security@telekom.de.

More info on the info page

Question

You find a presentation of Telekom with the turnover of the Telekom Shops on the Internet.

Should you report this?

Yes No

More info on the info page

Question

You find a presentation of Telekom with the turnover of the Telekom Shops on the Internet.

Should you report this?

Yes

The answer is correct:
You must take action here, because this could be an information protection incident. Report it via the functional mailbox security@telekom.de.

More info on the info page

Chapter 5

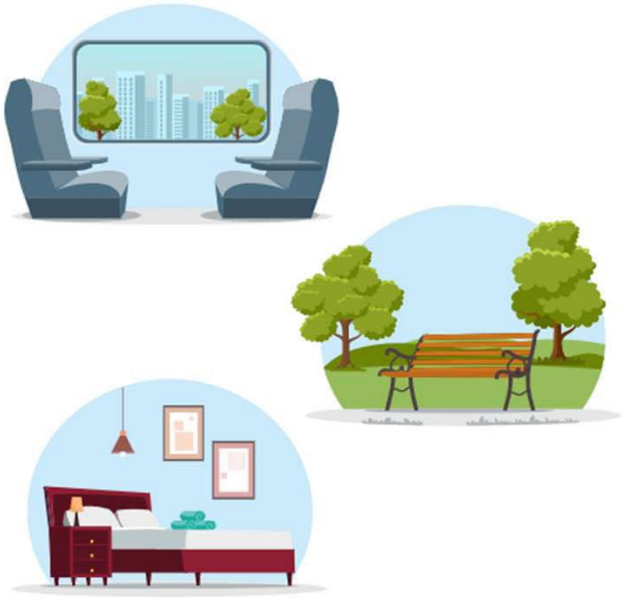
Practical cases on data and information protection

HomeOffice

Since 2020 at the latest, the home office has become the norm for all of us. This has a lot of advantages, but at this point we take a critical look at the challenges that working from home also brings.

Because the boundaries between office and home, between work and leisure, are becoming increasingly blurred.

Legal requirements and regulations of the company must also be complied with, otherwise there is a risk of violations of data protection or information protection! Especially in the home office, it is therefore all the more important that we behave correctly and security-consciously with regard to data and information protection.



Mobile working

When we work at home or on the road, we leave the 'protective umbrella' of our company.

Working on the train, in the park or in a hotel is no longer unusual. But of course, data and information are at greater risk here.

Conversations may be overheard, the laptop can be viewed, documents and data carriers may be forgotten.

Fortunately, we can work securely from anywhere with our business PC. A secure IT connection that our PC establishes and uses for this purpose makes this possible.

What we should know: No matter WHERE we work, whether in the home office, public space or in the office, the same rules for data and information protection apply. However, depending on the specific work situation, you need to be attentive wherever you are working.

More info on the info page

Clear desk

And of course - even in the office we pay attention to how we leave our office or a meeting room. We remove confidential content from flipcharts, check that no printouts or data carriers are left behind and don't simply throw business documents into the wastepaper basket.

Why should it be any different in the home office? The best thing to do there is to behave like we do in the office. That means putting notes, documents and printouts in the cupboard or drawer after work.

Devices and data carriers also need to be secured. So that third parties - including family members and friends - do not have easy access to them.

No mixing of official and private

Business is business and private is private, so we should always keep these two areas strictly separate. And that's how we should also act in the home office. And there are a few rules:

Private PCs, software and storage media - including cloud services used privately - may not be used for business purposes.

Finding your way through the app jungle

On your business smartphone, you naturally want to use apps that support you in your everyday work. But which ones are allowed? Can I use apps such as the weather app or navigation app from the public app store?

Simply run the guardrail-check and check whether the app meets the required criteria and may therefore be used.

Examples of apps that can be released by employees on their own initiative on the basis of the guardrails are navigation tools (route planners), travel tools (e.g. for travel information, check-in/check-out, delay tickers, etc.) and weather tools.

More info on the info page

Chapter 6

Question

Question

And finally, there are three questions that have to be answered correctly in order to complete the training successfully.

There is always only one correct answer. And off we go.

Question 1

I would like to download an app from the public app store on my business smartphone. What do I have to consider?

- [ ] As long as the app is available for free, I may use it on my smartphone.
- [ ] With the guardrail check, I check whether the app meets the criteria.
- [ ] Since some colleagues also use the app, this is allowed.

Senden

Question 1

I would like to download an app from the public app store on my business smartphone. What do I have to consider?

- [ ] As long as the app is available for free, I may use it on my smartphone.
- [x] With the guardrail check, I check whether the app meets the criteria.
- [ ] Since some colleagues also use the app, this is allowed.

Senden

Question 2

On the way to the canteen, I talk to a colleague on the phone and exchange confidential turnover figures with him. How do you judge that?

- [ ] That's totally ok, after all, the colleague is making the best use of his time.
- [ ] As we are making calls within a telecom building, this is allowed.
- [ ] In the case of telephone calls with confidential content, care must be taken to ensure that not everyone can hear the content of the call. This also applies within a telecom building or for web meetings.

Senden

Question 2

On the way to the canteen, I talk to a colleague on the phone and exchange confidential turnover figures with him. How do you judge that?

- [ ] That's totally ok, after all, the colleague is making the best use of his time.
- [ ] As we are making calls within a telecom building, this is allowed.
- [x] In the case of telephone calls with confidential content, care must be taken to ensure that not everyone can hear the content of the call. This also applies within a telecom building or for web meetings.

Senden

Question 3

You have booked yourself a desk in the open-plan office for the whole week. Therefore, you do not lock your keyboard, mouse and documents in the designated compartment after work because you will be using the desk again tomorrow.

- [ ] This is fine, because only authorised persons have access to the offices.
- [ ] That's fine because it saves working time, as everything doesn't have to be put up or taken down again every morning and evening.
- [ ] At the end of work, the desk must be tidied and everything either locked up or taken away.

Senden

Question 3

You have booked yourself a desk in the open-plan office for the whole week. Therefore, you do not lock your keyboard, mouse and documents in the designated compartment after work because you will be using the desk again tomorrow.

- [ ] This is fine, because only authorised persons have access to the offices.
- [ ] That's fine because it saves working time, as everything doesn't have to be put up or taken down again every morning and evening.
- [x] At the end of work, the desk must be tidied and everything either locked up or taken away.

Senden

Overview of tests

Here you can see the result of the test:

Downloading apps to the smartphone	✓
Phone call with colleagues on the way to the canteen	✓
Finishing work in the open plan office	✓

Chapter 7

Summary

What do I have to remember?

And if there are five things you should definitely take away from your training, they are the following:

What do I have to remember?

Basics

There is a clear line between data privacy and information protection

Data privacy regulates the handling of personal data and protects it from misuse by us, our company or other third parties.

Information protection, on the other hand, focuses primarily on the company: it is about protecting the information that we need to be able to carry out our business activities in the first place.

What do I have to remember?

Secrecy

The secrecy of telecommunications is a fundamental right. And it functions as a comprehensive protection of all our communications.

According to EU law, only business information that is also adequately protected is considered a trade secret.

What do I have to remember?

rights and obligations

Every person has rights in relation to their personal data.

The three most important are the right to information, the right to access and the right to erasure.

Everyone is responsible for the protection of information in their area of responsibility, influence or control.

What do I have to remember?

Reporting process

Report data privacy incidents to
datenschutz@telekom.de
and information protection incidents to
security@telekom.de.

If you are not sure whether it is a data protection or information protection incident, simply report it to one of the aforementioned mailboxes.

The experts will check your report and then take all further steps.

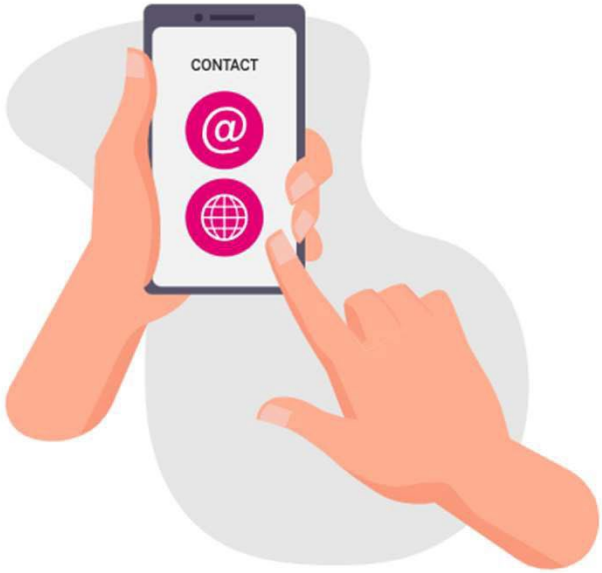
What do I have to remember?

Cases from practice

No matter where we work, the same rules on data and information protection apply. However, depending on the specific work situation, we have to be more or less attentive in how we work.

Therefore, the strict separation of official and private software and hardware is important.

We can use apps from the public app store if they pass the guardrail check.



Contact

Thank you for participating in our data and information protection training!

Would you like to learn more about data or information privacy? Are you looking for a contact person in data or information protection?

Here you can inform:

Or you send us a mail to: privacy@telekom.de