DATA PROTECTION AND SECURITY
MODULE SUMMARY

LIFE IS FOR SHARING.

PUBLICATION DETAILS

PUBLISHED BY

#DABEI-Geschichten – an initiative by Deutsche Telekom AG
Barbara Costanzo, Vice President Group Social Engagement
Friedrich-Ebert-Allee 140, 53113 Bonn, Germany

FURTHER INFORMATION	LAST REVISED	STATUS
https://dabei-geschichten.telekom.com/en/topics/data-protection-and-security/	Jan 9th, 2020	published

CONTACT

engagement-bonn@telekom.de

DATA PROTECTION AND SECURITY

Data Protection and Security?

Due to the large amounts of data that each of us leaves behind every day, it is becoming increasingly important to maintain control over our own data. In the following module you will learn how to do this.

What is Data Protection?

Address, date of birth, bank account data – a lot of information about you is stored as a matter of course. But what happens when your data is passed on to others? How can you protect your own data?
The term “data protection” does not mean the protection of data itself. “Data protection” wants to protect the people whose data is collected, stored and used. Data protection regulations are laid down in laws. They are designed to prevent people from losing control of their personal data. People should always be able to decide for themselves how their data is used. This is called informational self-determination.

International Differences

Internationally, there are different approaches to data protection.

- Germany
  In Germany, a central data protection law – the so-called “Bundesdatenschutzgesetz (BDSG)” (Federal Data Protection Act) – was previously in force. It was supplemented by sector-specific laws such as the “Telecommunications Act (TKG)”. Since 25 May 2018, the “Datenschutz-Grundverordnung (DSGVO)” or “General Data Protection Regulation (GDPR)” has been in force in Germany and the European Union, essentially replacing the previous data protection laws. The GDPR applies to all companies based in the European Union (EU), as well as companies providing services in the EU based outside of the EU.
- Russia
  In Russia, personal data belonging to Russian citizens may only be stored on Russian servers. This means that it is possible that websites not based in Russia may not store data belonging to Russian citizens.
- Japan
  Japan is very interested in data protection. The transfer of sensitive data is more likely to be avoided there. Therefore, authorities or companies can only use personal data to a very limited extent. Even in exceptional situations, such as after a train accident, hospitals sometimes do not pass on information about patients to their own families.
- Brazil
  In Brazil, the "Marco Civil da Internet" law applies – a kind of fundamental right for the Internet. The law is designed to protect the privacy of users online. However, this law also stipulates the storage of personal data. Companies and e-mail providers must store their customers' data for over a year and pass it on to government agencies if necessary. Critics see this as a violation of fundamental rights.
- USA
  Not many laws in the USA protect personal data. However, people in the USA have a different attitude towards data protection. Companies and authorities may actually use data there without consent. This is important, for example, when concluding an employment or rental contract. After checking a person’s personal data – e. g. income – a landlord may decide whether or not to conclude a contract for a house or apartment.

Data Breaches

In the past, there have been incidents where user data from various Internet services has been stolen and published. The aim of data protection is to prevent such incidents and to protect people.

- Yahoo!
  Names, e-mail addresses, birth dates, passwords – in 2013 these and other data were stolen from three billion “Yahoo!” user accounts. The data breach did not go public until three years later.
- iCloud-Leaks
  In 2014, a hacker managed to access hundreds of private celebrity photos. He sent a manipulated link by e-mail to those affected. Celebrities were supposed to log in with their iCloud ID as they were accustomed to. However, it was actually a fake site that stored users' iCloud IDs and forwarded them to the hacker. This procedure is also called "phishing". The, in some cases, very intimate photos were subsequently sold or published on the Internet.
- Ashley Madison
  In 2015, the online dating portal “Ashley Madison” came under fire. At that time, data from 32 million users – including names, addresses, searches, credit card information and sensitive information about privacy – was stolen. Subsequently, the hackers threatened to publish the data.
- Comdirect
  Two million customers of the direct bank "Comdirect" were able to access other customer accounts for several hours in July of 2016. This gave them access to other people's account balances. However, direct debits or bank transfers were not possible.
- Paradise Papers
  The so-called “Paradise Papers" have shown that many companies and individuals use loopholes when settling their taxes. The title refers to so-called "tax havens" – i. e. countries that are particularly attractive for taxpayers because of their low taxes. In November of 2017, the Süddeutsche Zeitung published information on a total of 13.4 million confidential documents.

DATA PROTECTION IN APPS AND SOCIAL MEDIA

What are Apps allowed to do?

Whether contacts, professional appointments, friends or reminder photos – your smartphone knows you and your personal data very well. But would you be willing to pass all of this data on to strangers? That is exactly what you are doing when you assign “App Permissions” in your smartphone settings. Of course, many apps only work if you share certain data, for example, you need to give a photo app access to your camera. A map service only makes sense if it knows your location. However, some apps also want access to data they do not need, such as phone numbers or contacts. Here, users themselves must become active and restrict this type of access.

Big Data – what's that?

Each day, billions of people use the Internet thus creating huge amounts of data. This is also called „Big Data“. If we search for something online or use digital navigation services each usage of the Internet leaves digital traces behind. Apart from personal data such as your address or phone

number, other data such as how long you remained on a certain website or which products you often look at also belongs to the category of Big Data.

Be Aware

Social networks or websites collect data – and you reveal a lot of this data yourself. Some platforms handle user data carelessly. It was only in March of 2018 that it became known that several million pieces of data from Facebook users, such as their age or place of residence, were passed on to third parties. As a user, you can prevent this by changing your privacy settings on the Facebook website.

Privacy Policy

Every time you click on a website you leave traces. Whether you are looking for new clothes or your next holiday destination, the website registers your interest and saves your entries. You can find out how companies handle this data, for example, in the data protection regulations.

Examples Privacy Policy

- Cookies
  When you visit a website, you are often informed that it stores cookies. Cookies are data that automatically back up websites to a user's end device. For example, if you place items in a shopping cart on a website, the content of the shopping cart is still available the next time you visit the page. Similar things can be observed with language settings. The language setting on a website only needs to be made once. This is, on the one hand, helpful. On the other hand, it allows companies to track your surfing behavior and thus place targeted advertising.
- Browser-Data
  Websites store data. As soon as you use the Internet with a browser, such as Mozilla Firefox, information is automatically passed on to the website operator. This includes, for example, the type of browser used, the IP address, the origin of the visitor or the time of the page request. Thus, websites always store information pertaining to when and where a user called up a page and how he or she moved around a page.
- Social Plug-Ins
  Imagine this: You have read an interesting article and would like to tell your friends about it. Instead of copying the link and sending it to each of your friends individually, you could use social plugins. Social plugins make it easier to share the article in question without leaving the website. A simple click on the small social network symbols is all it takes. However, from the perspective of German data protection, social plug-ins are not entirely harmless. They also make personal data, such as one's own surfing behavior, available to social networks.
- Tracking-Tools
  Many websites use tracking tools. They are used to collect and evaluate data about users with the permission of the website. This enables the website operator to recognize which information is of interest to the user or how long visitors stay on a site. This information is then used to adapt the website to the users' interests.
- Account Information
  Account information is the information you voluntarily provide on a website – for example, when you register as a user with your e-mail address. The website stores this information and creates a user account for you. Online shops in particular, often have to store bank data in addition to your name and e-mail address.

THE TRANSPARENT MAN

The Transparent Man

At first glance it is not always clear which data we leave behind on the Internet. However, we often disclose very personal data.

Flashlight and Contacts?

Anna-Lena (23) uses various apps on her smartphone in her free time. She often uses a flashlight app on her way home in the evening. The light makes her feel safer when she is alone. A flashlight app does not require any data such as location or contacts.

In 2013 it became known that the operator of a flashlight app was secretly collecting data from users. Users were not aware of which data was collected and when. After this became public knowledge, the operators of the app had to delete all of the user data they had collected.That is why you should always read exactly which data apps require before installing them. Also, a short search in an online search engine can often give you hints: Have other users already complained about the app? Is there any evidence that the app is dubious?

Advertising and Cold Calling

Anna-Lena was looking for a new smartphone when she came across a very interesting competition from a trustworthy source. All she had to do was enter her address and telephone number in order to participate. A few days later her phone rang. Anna-Lena was offered new smartphones and mobile phone contracts.

Data collected during competitions is often used for such purposes. Competitions in particular, often require data that is not necessary at first glance – e. g. your telephone number. The following wording is then often found in the conditions of participation: “By entering this competition, I agree to the commercial use of my data.” With your consent, the data and your telephone number may subsequently be passed on to third parties.

Viruses, Malware and Spam

In her free time, Anna-Lena likes to use social media – especially with new trends such as dating apps. She recently came across a new interesting app. After she downloaded it, an enormous amount of advertising suddenly appeared on her mobile phone. In addition to advertising for clothing and mobile phone contracts, a window with a virus warning also appeared. It asked for some information about her device and her person. The virus could only be removed after she entered the information it was asking for.

The messages were probably so-called “adware”. The term is composed of the English words “advertisement” and “software”. Adware often has a quite harmless reason – for example, a free program financed by advertising. Sometimes, however, a virus or malware is also the cause of the advertisement. If you suspect that your computer could be infected by a virus, you should react. An antivirus program for mobile devices provides protection against attacks like these.

Digital Surveillance

On the Internet we disclose – both intentionally and unintentionally – private data. But data about us is also collected at work or during leisure time. Security cameras are widely used in many public places (e. g. train stations). More and more places are being video-monitored for security reasons. Drones are also used and monitor, for example, demonstrations or crime scenes from above. This is one of the reasons why security measures such as these are being discussed in public: When do we truly feel safe? When do you feel your privacy is being violated or you are being watched?

DATA PROTECTION TIPS

Data Protection through Data Economy?

In the last chapter you already became acquainted with various problems. But you can't do entirely without data on the Internet. In other words, you have to enter your address for your order to be delivered. So the question is not: Which data do I want to disclose on the Internet? But rather: Which data is required at which point?

Safe Devices

Data protection starts with the device that is being used. Keep your smartphone, PC or tablet software up to date. You can prevent unauthorized access by using PINs, passwords or fingerprint or face scanners. Anti-virus programs on mobile devices also offer protection.

Secure Passwords

Virtually all Internet services are password protected against unlawful access. Therefore, it is important to choose a password that reliably protects your data.

Secure Networks

A quick e-mail check while you are underway? Public networks are a convenient way to connect to the Internet. However, there are a few things you should be aware of.

- Be careful when using open networks
  Open networks in cafés or train stations are fast and convenient, but can be unsafe. Personal data can be accessed via an unsecured connection. E-mails or services that you need to log in to can no longer be used securely.
- No Automatic Wi-Fi Connections
  Disable automatic Wi-Fi connections when you are out and about. Hackers can modify WLAN networks so that mobile devices can connect to them without your permission. This allows them to read your messages, for example.
- Secure Connections
  Only use public websites that encrypt communication with SSL connections. You can recognize this by the name "https" before the actual link. These connections prevent, for example, login data from being spied on.

- Disable File Sharing
  Windows and Mac OS allow you to connect computers in a network. This allows files to be exchanged between them. This is also called “file sharing”. In a public network, however, file sharing can allow strangers to gain access to your personal data. Disable file sharing in your device settings as soon as you browse publicly.

The Right to be Forgotten!

What if something gets on the Internet that you do not want there? Every citizen has the right to have private data removed from the public domain on the Internet. The so-called “right to be forgotten” allows users to prevent links to Google search queries or to report and delete content on Facebook, for example. In this way, private traces on the Internet can be removed.

Alternative Search Engines

In addition to the well-known search engines such as Google or Bing, there are also more and more alternative search engines.Some search engines like DuckDuckGo or StartPage want to offer their users more security. The connection is always encrypted and no user data (e.g. IP address) is stored. Other alternative search engines such as Ecosia or MetaGer operate their servers with renewable energy. These search engines are non-profit oriented. Their profits are donated, for example, to a rainforest project.

Data Protection Today!

Data protection will continue to affect many areas of our everyday lives in the future. By 2020, the “Internet of Things” will have connected up to fifty billion electronic devices – be it the refrigerator, the navigation device or the automatic vacuum cleaner. The manufacturers of these devices should, according to data protectors, pay attention to users’ privacy in the development and production of their products. This means that users should know exactly which data is collected when and how it is encrypted. The “Privacy by Design” requirement is already taken into account in the general data protection regulation of the EU (GDPR).

Protect Your Data

Stay in control and be proactive! You have learned about many possibilities in this module: change the privacy settings of your social networks or protect your devices. Data protection is your right – use it!