What happens to my data? Why does data security matter?

What is data protection?

To some, data protection appears difficult, perhaps abstract and in any case technical. One may wonder whether it has any relevance to everyday life. But we protect our data in everyday life as a matter of utmost importance: we have curtains in front of our windows, close the door when we are discussing something sensitive, we only disclose some information to a few selected people and we prefer to keep other information to ourselves.

In a digital environment, protection of data is achieved by setting rules that determine who is authorised to access information. The difference with for example closing the curtains is that the person whose privacy is at stake is not always the one who protects the privacy; we are often reliant on others to protect our data from being accessed by others. In many cases we don’t even know whether ‘the curtains’ are open or not.

Why is data protection important?

The protection of our data as an aspect of our privacy is essential for our lives as human beings. A fundamental insight from psychology is that people behave differently under (potential) observation. Our privacy serves as a space of autonomy in which we can break through social norms and experiment with new behavior and thought. It is a place of rest and relaxation. In the private sphere, self-evaluation and free communication should be possible.[1] Data protection as part of the protection of privacy is supposed to safeguard this. Accordingly, data protection safeguards individual freedom by prohibiting the collection and processing of data and only allowing it under certain conditions.

Data protection also has a structural dimension.[2] Information relations are power relations; whoever has information – i.e. data – can exercise power. The individual has to be protected from asymmetrical power relations. Data protection is therefore more than a matter of protecting the individual.

How does data protection relate to apps?

Apps, short for applications, are the programs on our mobile phones and tablets. If we want to use an app, we usually have to provide a range of information, such as our name, an email address and our date of birth, sometimes a home address or payment details. In addition, apps often collect data without us actively giving the information to the app. When we install an app, we usually allow it to access a wide range of functions on our mobile device, such as location data, activity sensors, microphone or camera. The app then collects data while we use our device. This is very helpful for app providers because they can use the information to improve their product. However, it also means that an app provider can retrieve a lot of information: When do I use my smartphone, tablet etc? How do I use my device? Where am I located? This data can be used to draw a picture of the user.

How is our data protected?

Our data is protected by a range of laws. Data protection is fundamentally governed by Article 8 of the European Convention on Human Rights (ECHR), by Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union (CFR) at the European level, and by an array of rights in the German Federal Constitution. These fundamental rights are unpacked by the General Data Protection Regulation (GDPR) on the European Union level, in Germany by the Federal Data Protection Law and the country-specific data protection laws (e.g. Bavarian Data Protection Act). These laws are applicable when a public or non-public actor processes personal data. The term “processing” is to be understood broadly here. Effectively the term “processing” covers any data handling, including collection and deletion.[3]

The law assumes a fundamental prohibition of the processing of personal data. Processing is permitted in exceptional cases if one of the conditions specified in the law is fulfilled.

What do I agree to when I click „I agree“?

Under European law, any processing of personal data (such as health data) is in principle unlawful. It is only lawful in exceptional cases if certain conditions are met. Consent is one of six possible conditions according to which the processing of personal data is lawful, Art. 6(1) lit. a and Art. 9(2) lit. a GDPR.

Consent is defined in the GDPR as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;”, Art. 4 no. 11 GDPR.

When is consent given?

Consent can only be free and therefore valid if the data subject has a genuine choice and there is no risk of deception, intimidation, coercion or other negative consequences.[4] According to Art. 7 para. 2 GDPR the person responsible for collecting the data must ensure that the data subject can revoke his/her consent at any time and that the revoke is as simple as granting consent.

Data may only be passed on to third parties – for example in the context of data trading – if consent has been given. For this reason, consent to the data protection declaration must include the possibility of disclosure to third parties. If you do not agree to the data being passed on to third parties, you should not give your consent. However, this often means that the corresponding service, e.g. use of a social media platform or an online trade, is not possible.

Art. 9 GDPR provides a higher level of protection for particularly sensitive data, such as health data. Here, too, a fundamental prohibition on the processing of these particular personal data is accompanied by a number of admissibility facts, Art. 9 (2) GDPR. This means that under certain circumstances the processing of these particularly sensitive data may also be lawful.

Data as a currency?

Many online services, for example social media platforms such as Facebook or Instagram, are “free” at first glance because there is no charge for using them. However, these services are only seemingly “free” because the companies, which provide these platforms earn money with the users’ data, especially through advertising. Users regularly consent to the processing of their data when registering. Therefore, the use of such online services is not exactly free of charge, because the users pay with their data.

A particularly effective protective instrument in the GDPR is the prohibition of “coupling” or “tying”. In other words, companies cannot require that individuals who want to use the company’s services can only do so under the condition of providing personal data.[5] This means that if an individual voluntarily consents to the use of a particular service and a company tries to “couple” or “tie” them to also consent to the provision of personal data, then the contract cannot be considered valid and voluntary. The possibility of using data as currency is thus effectively hindered, because the processing of personal data is often not necessary for the fulfilment of the contract. A recent development is the so-called “pay or consent” model, mainly introduced by Facebook/Meta, where the user is given the choice to either consent to the collection and processing of personal data (mainly for targeted advertising) or to pay for a service without data collection and processing[6]

1. Trepte, 2012, Privatsphäre aus psychologischer Sicht, in Schimdt/Weichter (Hrsg.), Datenschutz, Bundeszentrale für politische Bildung, 62.↑
2. Lewinski, 2012, Zur Geschichte von Privatsphäre und Datenschutz, in Schimdt/Weichter (Hrsg.), Datenschutz, Bundeszentrale für politische Bildung, S. 32.↑
3. Tinnefeld/Buchner/Petri/Hansen, Einführung in das Datenschutzrecht, 2024, Kap. 2, Rn. 42 ff.↑
4. Datenschutzgruppe 29, WP259 rev.01 , S. 8.↑
5. Tinnefeld/Buchner/Petri/Hansen, Einführung in das Datenschutzrecht, 2024, Kap. 4 Rn. 41 ff.↑
6. D’Amico, A., Pelekis, D. ., Teixeira Santos, C., & Duivenvoorde, B. (2024). Meta’s Pay-or-Okay Model: An analysis

under EU Data Protection, Consumer and Competition Law. Technology and Regulation, 2024, 254-272. https://doi.org/10.71265/tkk29041 ff.↑