Privacy Policy

Privacy Policy Introduction and Overview

We have written this privacy policy (version 10.03.2023-112328747) in order to explain to you, in accordance with the provisions of the [General Data Protection Regulation (EU) 2016/679](#) and applicable national laws, which personal data (data for short) we as the controller – and the processors commissioned by us (e.g. providers) – process, will process in the future and what legal options you have. The terms used are to be considered gender-neutral.
In short: We provide you with comprehensive information about any of your personal data we process.

Privacy policies usually sound very technical and use legal terminology. However, this privacy policy is intended to describe the most important things to you as simply and transparently as possible. So long as it aids transparency, technical **terms are explained in a reader-friendly manner, links** to further information are provided and **graphics** are used. We are thus informing in clear and simple language that we only process personal data in the context of our business activities if there is a legal basis for it. This is certainly not possible with brief, unclear and legal-technical statements, as is often standard on the internet when it comes to data protection. I hope you find the following explanations interesting and informative. Maybe you will also find some information that you have not been familiar with.
If you still have questions, we kindly ask you to contact the responsible body named below or in the imprint, follow the existing links and look at further information on third-party sites. You can of course also find our contact details in the imprint.

Scope

This privacy policy applies to all personal data processed by our company and to all personal data processed by companies commissioned by us (processors). With the term personal data, we refer to information within the meaning of Article 4 No. 1 GDPR, such as the name, email address and postal address of a person. The processing of personal data ensures that we can offer and invoice our services and products, be it online or offline. The scope of this privacy policy includes:

- all online presences (websites, online shops) that we operate
- Social media presences and email communication
- mobile apps for smartphones and other devices

In short: This privacy policy applies to all areas in which personal data is processed in a structured manner by the company via the channels mentioned. Should we enter into legal relations with you outside of these channels, we will inform you separately if necessary.

Legal bases

In the following privacy policy, we provide you with transparent information on the legal principles

and regulations, i.e. the legal bases of the General Data Protection Regulation, which enable us to process personal data.

Whenever EU law is concerned, we refer to REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 27, 2016. You can of course access the General Data Protection Regulation of the EU online at EUR-Lex, the gateway to EU law, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

We only process your data if at least one of the following conditions applies:

1. **Consent** (Article 6 Paragraph 1 lit. a GDPR): You have given us your consent to process data for a specific purpose. An example would be the storage of data you entered into a contact form.
2. **Contract** (Article 6 Paragraph 1 lit. b GDPR): We process your data in order to fulfill a contract or pre-contractual obligations with you. For example, if we conclude a sales contract with you, we need personal information in advance.
3. **Legal obligation** (Article 6 Paragraph 1 lit. c GDPR): If we are subject to a legal obligation, we will process your data. For example, we are legally required to keep invoices for our bookkeeping. These usually contain personal data.
4. **Legitimate interests** (Article 6 Paragraph 1 lit. f GDPR): In the case of legitimate interests that do not restrict your basic rights, we reserve the right to process personal data. For example, we have to process certain data in order to be able to operate our website securely and economically. Therefore, the processing is a legitimate interest.

Other conditions such as making recordings in the interest of the public, the exercise of official authority as well as the protection of vital interests do not usually occur with us. Should such a legal basis be relevant, it will be disclosed in the appropriate place.

In addition to the EU regulation, national laws also apply:

- In **Austria** this is the Austrian Data Protection Act (**Datenschutzgesetz**), in short **DSG**.
- In **Germany** this is the Federal Data Protection Act (**Bundesdatenschutzgesetz**), in short **BDSG**.

Should other regional or national laws apply, we will inform you about them in the following sections.

Contact details of the data protection controller

If you have any questions about data protection, you will find the contact details of the responsible person or controller below:

ondot solutions GmbH
Kaiser Franz-Ring 24
A-2500 Baden

E-Mail: sales[at]ondot.at
Phone: +43 2236 205866 0

Company details: https://www.ondot.at/impressum/

Storage Period

It is a general criterion for us to store personal data only for as long as is absolutely necessary for the provision of our services and products. This means that we delete personal data as soon as any reason for the data processing no longer exists. In some cases, we are legally obliged to keep certain data stored even after the original purpose no longer exists, such as for accounting purposes.

If you want your data to be deleted or if you want to revoke your consent to data processing, the data will be deleted as soon as possible, provided there is no obligation to continue its storage.

We will inform you below about the specific duration of the respective data processing, provided we have further information.

Rights in accordance with the General Data Protection Regulation

In accordance with Articles 13, 14 of the GDPR, we inform you about the following rights you have to ensure fair and transparent processing of data:

- According to Article 15 DSGVO, you have the right to information about whether we are processing data about you. If this is the case, you have the right to receive a copy of the data and to know the following information:
    - for what purpose we are processing;
    - the categories, i.e. the types of data that are processed;
    - who receives this data and if the data is transferred to third countries, how security can be guaranteed;
    - how long the data will be stored;
    - the existence of the right to rectification, erasure or restriction of processing and the right to object to processing;
    - that you can lodge a complaint with a supervisory authority (links to these authorities can be found below);
    - the origin of the data if we have not collected it from you;
    - Whether profiling is carried out, i.e. whether data is automatically evaluated to arrive at a personal profile of you.
- You have a right to rectification of data according to Article 16 GDPR, which means that we must correct data if you find errors.
- You have the right to erasure ("right to be forgotten") according to Article 17 GDPR, which specifically means that you may request the deletion of your data.
- According to Article 18 of the GDPR, you have the right to restriction of processing, which means that we may only store the data but not use it further.
- According to Article 20 of the GDPR, you have the right to data portability, which means that we will provide you with your data in a standard format upon request.

- According to Article 21 DSGVO, you have the right to object, which entails a change in processing after enforcement.
  - If the processing of your data is based on Article 6(1)(e) (public interest, exercise of official authority) or Article 6(1)(f) (legitimate interest), you may object to the processing. We will then check as soon as possible whether we can legally comply with this objection.
  - If data is used to conduct direct advertising, you may object to this type of data processing at any time. We may then no longer use your data for direct marketing.
  - If data is used to conduct profiling, you may object to this type of data processing at any time. We may no longer use your data for profiling thereafter.
- According to Article 22 of the GDPR, you may have the right not to be subject to a decision based solely on automated processing (for example, profiling).
- You have the right to lodge a complaint under Article 77 of the GDPR. This means that you can complain to the data protection authority at any time if you believe that the data processing of personal data violates the GDPR.

In short: you have rights – do not hesitate to contact the responsible party listed above with us!

If you believe that the processing of your data violates data protection law or your data protection rights have been violated in any other way, you can complain to the supervisory authority. For Austria, this is the data protection authority, whose website can be found at https://www.dsb.gv.at/. In Germany, there is a data protection officer for each federal state. For more information, you can contact the Federal Commissioner for Data Protection and Freedom of Information (BfDI). The following local data protection authority is responsible for our company:

Austria Data protection authority

Manager: Mag. Dr. Andrea Jelinek
Address: Barichgasse 40-42, 1030 Wien
Phone number.: +43 1 52 152-0
E-mail address: dsb@dsb.gv.at
Website: https://www.dsb.gv.at/

Security of data processing operations

In order to protect personal data, we have implemented both technical and organisational measures. We encrypt or pseudonymise personal data wherever this is possible. Thus, we make it as difficult as we can for third parties to extract personal information from our data.

Article 25 of the GDPR refers to "data protection by technical design and by data protection-friendly default" which means that both software (e.g. forms) and hardware (e.g. access to server rooms) appropriate safeguards and security measures shall always be placed. If applicable, we will outline the specific measures below.

TLS encryption with https

The terms TLS, encryption and https sound very technical, which they are indeed. We use HTTPS (Hypertext Transfer Protocol Secure) to securely transfer data on the Internet.
This means that the entire transmission of all data from your browser to our web server is secured – nobody can "listen in".

We have thus introduced an additional layer of security and meet privacy requirements through technology design Article 25 Section 1 GDPR). With the use of TLS (Transport Layer Security), which is an encryption protocol for safe data transfer on the internet, we can ensure the protection of confidential information.
You can recognise the use of this safeguarding tool by the little lock-symbol 🔒, which is situated in your browser's top left corner in the left of the internet address (e.g. examplepage.uk), as well as by the display of the letters https (instead of http) as a part of our web address.
If you want to know more about encryption, we recommend you to do a Google search for "Hypertext Transfer Protocol Secure wiki" to find good links to further information.

Cookies

> **Cookies Overview**
> Affected parties: visitors to the website
> Purpose: depending on the respective cookie. You can find out more details below or from the software manufacturer that sets the cookie.
> Processed data: depends on the cookie used. More details can be found below or from the manufacturer of the software that sets the cookie.
> Storage duration: can vary from hours to years, depending on the respective cookie
> Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What are cookies?

Our website uses HTTP-cookies to store user-specific data.
In the following we explain what cookies are and why they are used, so that you can better understand the following privacy policy.

Whenever you surf the Internet, you are using a browser. Common browsers are for example, Chrome, Safari, Firefox, Internet Explorer and Microsoft Edge. Most websites store small text-files in your browser. These files are called cookies.

It is important to note that cookies are very useful little helpers. Almost every website uses cookies. More precisely, these are HTTP cookies, as there are also other cookies for other uses. HTTP cookies are small files that our website stores on your computer. These cookie files are automatically placed into the cookie-folder, which is the "brain" of your browser. A cookie consists of a name and a value. Moreover, to define a cookie, one or multiple attributes must be specified.

Cookies store certain user data about you, such as language or personal page settings. When you re-open our website to visit again, your browser submits these "user-related" information back to

our site. Thanks to cookies, our website knows who you are and offers you the settings you are familiar to. In some browsers, each cookie has its own file, while in others, such as Firefox, all cookies are stored in one single file.

The following graphic shows a possible interaction between a web browser such as Chrome and the web server. The web browser requests a website and receives a cookie back from the server. The browser then uses this again as soon as another page is requested.
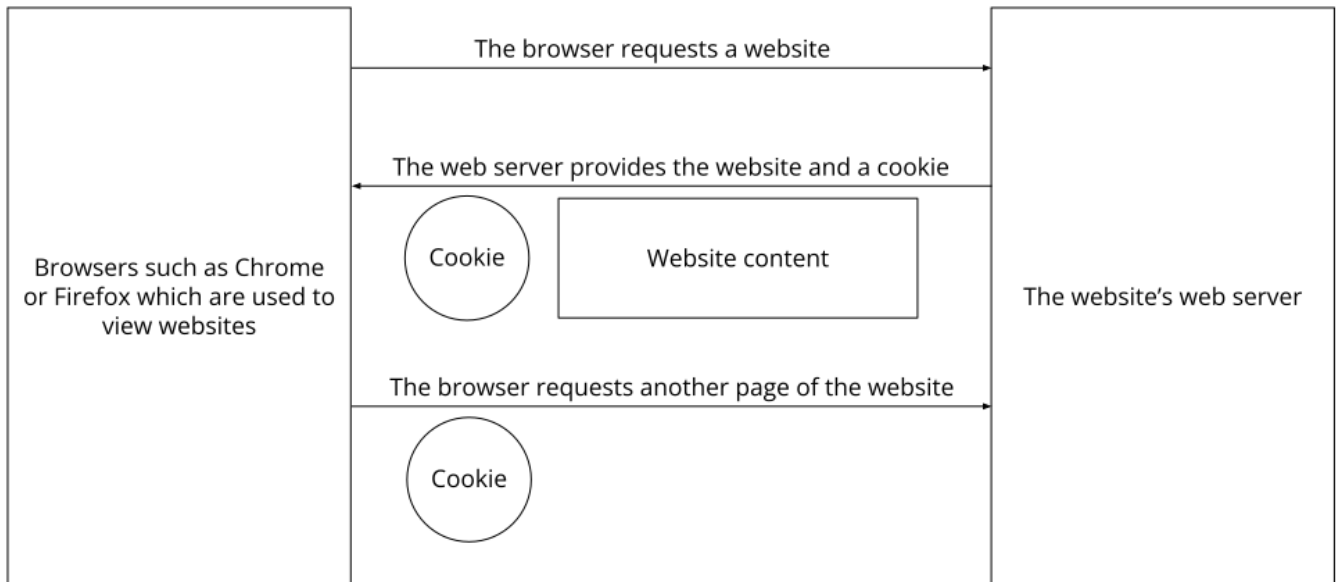
There are both first-party cookies and third-party cookies. First-party cookies are created directly by our site, while third-party cookies are created by partner-websites (e.g. Google Analytics). Each cookie must be evaluated individually, as each cookie stores different data. The expiry time of a cookie also varies from a few minutes to a few years. Cookies are not software programs and do not contain viruses, trojans or other malware. Cookies also cannot access your PC's information.

This is an example of how cookie-files can look:

Name: _ga
Value: GA1.2.1326744211.152112328747-9
Purpose: Differentiation between website visitors
Expiry date: after 2 years

A browser should support these minimum sizes:

- At least 4096 bytes per cookie
- At least 50 cookies per domain
- At least 3000 cookies in total

Which types of cookies are there?

The exact cookies that we use, depend on the used services, which will be outlined in the following sections of this privacy policy. Firstly, we will briefly focus on the different types of HTTP-cookies.

There are 4 different types of cookies:

Essential cookies
These cookies are necessary to ensure the basic functions of a website. They are needed when a user for example puts a product into their shopping cart, then continues surfing on different websites and comes back later in order to proceed to the checkout. These cookies ensure the shopping cart does not get deleted, even if the user closes their browser window.

Purposive cookies
These cookies collect information about user behaviour and whether the user receives any error messages. Furthermore, these cookies record the website's loading time as well as its behaviour in different browsers.

Target-orientated cookies
These cookies ensure better user-friendliness. Thus, information such as previously entered locations, fonts sizes or data in forms stay stored.

Advertising cookies
These cookies are also known as targeting cookies. They serve the purpose of delivering customised advertisements to the user. This can be very practical, but also rather annoying.

Upon your first visit to a website you are usually asked which of these cookie-types you want to accept. Furthermore, this decision will of course also be stored in a cookie.

If you want to learn more about cookies and do not mind technical documentation, we recommend https://tools.ietf.org/html/rfc6265, the Request for Comments of the Internet Engineering Task Force (IETF) called "HTTP State Management Mechanism".

Purpose of processing via cookies

The purpose ultimately depends on the respective cookie. You can find out more details below or from the software manufacturer that sets the cookie.

Which data are processed?

Cookies are little helpers for a wide variety of tasks. Unfortunately, it is not possible to tell which data is generally stored in cookies, but in the privacy policy below we will inform you on what data is processed or stored.

Storage period of cookies

The storage period depends on the respective cookie and is further specified below. Some cookies are erased after less than an hour, while others can remain on a computer for several years.

You can also influence the storage duration yourself. You can manually erase all cookies at any time in your browser (also see "Right of objection" below). Furthermore, the latest instance cookies based on consent will be erased is after you withdraw your consent. The legality of storage will

remain unaffected until then.

Right of objection – how can I erase cookies?

You can decide for yourself how and whether you want to use cookies. Regardless of which service or website the cookies originate from, you always have the option of erasing, deactivating or only partially accepting cookies. You can for example block third-party cookies but allow all other cookies.

If you want to find out which cookies have been stored in your browser, or if you want to change or erase cookie settings, you can find this option in your browser settings:

[Chrome: Clear, enable and manage cookies in Chrome](#)

[Safari: Manage cookies and website data in Safari](#)

[Firefox: Clear cookies and site data in Firefox](#)

[Internet Explorer: Delete and manage cookies](#)

[Microsoft Edge: Delete cookies in Microsoft Edge](#)

If you generally do not want cookies, you can set up your browser in a way to notify you whenever a cookie is about to be set. This gives you the opportunity to manually decide to either permit or deny the placement of every single cookie. This procedure varies depending on the browser. Therefore, it might be best for you to search for the instructions in Google. If you are using Chrome, you could for example put the search term "delete cookies Chrome" or "deactivate cookies Chrome" into Google.

Legal basis

The so-called "cookie directive" has existed since 2009. It states that the storage of cookies requires your **consent** (Article 6 Paragraph 1 lit. a GDPR). Within countries of the EU, however, the reactions to these guidelines still vary greatly. In Austria, however, this directive was implemented in Section 96 (3) of the Telecommunications Act (TKG). In Germany, the cookie guidelines have not been implemented as national law. Instead, this guideline was largely implemented in Section 15 (3) of the Telemedia Act (TMG).

For absolutely necessary cookies, even if no consent has been given, there are legitimate interests (Article 6 (1) (f) GDPR), which in most cases are of an economic nature. We want to offer our visitors a pleasant user experience on our website. For this, certain cookies often are absolutely necessary.

This is exclusively done with your consent, unless absolutely necessary cookies are used. The legal basis for this is Article 6 (1) (a) of the GDPR.

In the following sections you will find more detail on the use of cookies, provided the used software does use cookies.

Web hosting

```
Web hosting Overview
Affected parties: visitors to the website
Purpose: professional hosting of the website and security of operations
Processed data: IP address, time of website visit, browser used and other data. You can find
more details on this below or at the respective web hosting provider.
Storage period: dependent on the respective provider, but usually 2 weeks
Legal basis: Art. 6 para. 1 lit. f GDPR (legitimate interests)
```

What is web hosting?

Every time you visit a website nowadays, certain information – including personal data – is automatically created and stored, including on this website. This data should be processed as sparingly as possible, and only with good reason. By website, we mean the entirety of all websites on your domain, i.e. everything from the homepage to the very last subpage (like this one here). By domain we mean example.uk or examplepage.com.

When you want to view a website on a screen, you use a program called a web browser. You probably know the names of some web browsers: Google Chrome, Microsoft Edge, Mozilla Firefox, and Apple Safari.

The web browser has to connect to another computer which stores the website's code: the web server. Operating a web server is complicated and time-consuming, which is why this is usually done by professional providers. They offer web hosting and thus ensure the reliable and flawless storage of website data.

Whenever the browser on your computer establishes a connection (desktop, laptop, smartphone) and whenever data is being transferred to and from the web server, personal data may be processed. After all, your computer stores data, and the web server also has to retain the data for a period of time in order to ensure it can operate properly.

Illustration:

Why do we process personal data?

The purposes of data processing are:

1. Professional hosting of the website and operational security
2. To maintain the operational as well as IT security
3. Anonymous evaluation of access patterns to improve our offer, and if necessary, for prosecution or the pursuit of claims.li>

Which data are processed?

Even while you are visiting our website, our web server, that is the computer on which this website is saved, usually automatically saves data such as

- the full address (URL) of the accessed website (e. g. https://www.examplepage.uk/examplesubpage.html?tid=112328747)
- browser and browser version (e.g. Chrome 87)
- the operating system used (e.g. Windows 10)
- the address (URL) of the previously visited page (referrer URL) (e. g. https://www.examplepage.uk/icamefromhere.html/)
- the host name and the IP address of the device from the website is being accessed from (e.g. COMPUTERNAME and 194.23.43.121)
- date and time
- in so-called web server log files

How long is the data stored?

Generally, the data mentioned above are stored for two weeks and are then automatically deleted. We do not pass these data on to others, but we cannot rule out the possibility that this data may be viewed by the authorities in the event of illegal conduct.

In short: Your visit is logged by our provider (company that runs our website on special computers (servers)), but we do not pass on your data without your consent!

Legal basis

The lawfulness of processing personal data in the context of web hosting is justified in Art. 6 para. 1 lit. f GDPR (safeguarding of legitimate interests), as the use of professional hosting with a provider is necessary to present the company in a safe and user-friendly manner on the internet, as well as to have the ability to track any attacks and claims, if necessary.

ALL-INKL Privacy Policy

We use ALL-INKL for our website, which is a web hosting provider, among other things. The provider of this service is the German company ALL-INKL.COM – Neue Medien Münnich, Hauptstrasse 68, 02742 Friedersdorf, Germany. You can find out more about the data that is processed through the use of ALL-INKL in their Privacy Policy at https://all-inkl.com/datenschutzinformationen/.

Social Media

Social Media Privacy Policy Overview
Affected parties: website visitors
Purpose: Service presentation and optimisation, staying in contact with visitors, interested parties, etc. as well as advertising
Processed data: data such as telephone numbers, email addresses, contact data, data on user behaviour, information about your device and your IP address.
You can find more details on this directly at the respective social media tool used.
Storage period: depending on the social media platforms used
Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is Social Media?

In addition to our website, we are also active on various social media platforms. For us to be able to target interested users via social networks, user data may be processed. Additionally, elements of social media platforms may be embedded directly in our website. This is e.g. the case if you click a so-called social button on our website and are forwarded directly to our social media presence. So-called social media are websites and apps on which registered members can produce and exchange content with other members, be it openly or in certain groups and networks.

Why do we use Social Media?

For years, social media platforms have been the place where people communicate and get into contact online. With our social media presence, we can familiarise interested people better with our products and services. The social media elements integrated on our website help you switch to our social media content quickly and hassle free.

The data that is retained and processed when you use a social media channel is primarily used to conduct web analyses. The aim of these analyses is to be able to develop more precise and personal marketing and advertising strategies. The evaluated data on your behaviour on any social media platform can help to draw appropriate conclusions about your interests. Moreover, so-called user profiles can be created. Thus, the platforms may also to present you with customised advertisements. For this, cookies are usually placed in your browser, which store data on your user behaviour.

We generally assume that we will continue to be responsible under Data Protection Law, even when using the services of a social media platform. However, the European Court of Justice has ruled that, within the meaning of Art. 26 GDPR, in certain cases the operator of the social media platform can be jointly responsible with us. Should this be the case, we will point it out separately and work on the basis of a related agreement. You will then find the essence of the agreement for the concerned platform below.

Please note that when you use social media platforms or our built-in elements, your data may also be processed outside the European Union, as many social media channels, such as Facebook or Twitter, are American companies. As a result, you may no longer be able to easily claim or enforce

your rights regarding your personal data.

Which data are processed?

Exactly which data are stored and processed depends on the respective provider of the social media platform. But usually it is data such as telephone numbers, email addresses, data you enter in contact forms, user data such as which buttons you click, what you like or who you follow, when you visited which pages, as well as information about your device and IP address. Most of this data is stored in cookies. Should you have a profile on the social media channel you are visiting and are logged in, data may be linked to your profile.

All data that are collected via social media platforms are also stored on the providers' servers. This means that only the providers have access to the data and can provide you with appropriate information or make changes for you.

If you want to know exactly which data is stored and processed by social media providers and how you can object to the data processing, we recommend you to carefully read the privacy policy of the respective company. We also recommend you to contact the provider directly if you have any questions about data storage and data processing or if you want to assert any corresponding rights.

Duration of data processing

Provided we have any further information on this, we will inform you about the duration of the data processing below. The social media platform Facebook example stores data until they are no longer needed for the company's own purposes. However, customer data that is synchronised with your own user data is erased within two days. Generally, we only process personal data for as long as is absolutely necessary for the provision of our services and products. This storage period can also be exceeded however, if it is required by law, such as e.g. in the case of accounting.

Right to object

You also retain the right and the option to revoke your consent to the use of cookies or third-party providers such as embedded social media elements at any time. This can be done either via our cookie management tool or via other opt-out functions. You can e.g. also prevent data collection via cookies by managing, deactivating or erasing cookies in your browser.

Since cookies may be used with social media tools, we also recommend you to read our privacy policy on cookies. If you want to find out which of your data is stored and processed, we advise you to read the privacy policies of the respective tools.

Legal basis

If you have consented to the processing and storage of your data by integrated social media elements, this consent serves as the legal basis for data processing **(Art. 6 para. 1 lit. a GDPR)**. Generally, provided you have given your consent, your data will also be stored and processed on the basis of our legitimate interest **(Art. 6 para. 1 lit. f GDPR)** in maintaining fast and good

communication with you and other customers and business partners. Nevertheless, we only use the tools if you have consented. Most social media platforms also set cookies on your browser to store data. We therefore recommend you to read our privacy policy on cookies carefully and to take a look at the privacy policy or cookie policy of the respective service provider.

in the following section you can find information on special social media platforms – provided this information is available.

Facebook Privacy Policy

Facebook Privacy Policy Overview
Affected parties: website visitors
Purpose: service optimisation
Processed data: data such as customer data, data on user behaviour, device information and IP address.
You can find more details in the Privacy Policy below.
Storage period: until the data no longer serves Facebook's purposes
Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What are Facebook tools?

We use selected Facebook tools on our website. Facebook is a social media network of the company Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2 Ireland. With the aid of this tool we can provide the best possible offers to you and anyone interested in our products and services.

If your data is collected and forwarded via our embedded Facebook elements or via our Facebook page (fanpage), both we and Facebook Ireland Ltd. are responsible for this. However, should any further processing occur, then Facebook is solely responsible for this data. Our joint commitments were also set out in a publicly available agreement at [https://www.facebook. com / legal / controller_addendum](https://www.facebook.com/legal/controller_addendum) . It e.g. states that we must clearly inform you about the use of Facebook tools on our website. We are also responsible for ensuring that the tools are securely integrated into our website and are in accordance with the applicable privacy laws. Facebook, on the other hand, is e.g. responsible for the data security of Facebook's products. If you have any questions about Facebook's data collection and processing, you can contact the company directly. Should you direct the question to us, we are obliged to forward it to Facebook.

In the following we will give you an overview on the different Facebook tools, as well as on what data is sent to Facebook and how you can erase this data.

Along with many other products, Facebook also offers so called "Facebook Business Tools". This is Facebook's official name for its tools, but it is not very common. Therefore, we decided to merely call them "Facebook tools". They include the following:

- Facebook-Pixel
- Social Plugins (e.g. the "Like" or "Share" button)

- Facebook Login
- Account Kit
- APIs (application programming interface)
- SDKs (Softwart developmept kits)
- Plattform-integrations
- Plugins
- Codes
- Specifications
- Documentations
- Technologies and Services

With these tools Facebook can extend its services and is able to receive information on user activities outside of Facebook.

Why do we use Facebook tools on our website?

We only want to show our services and products to people who are genuinely interested in them. With the help of advertisements (Facebook Ads) we can reach exactly these people. However, to be able to show suitable adverts to users, Facebook requires additional information on people's needs and wishes. Therefore, information on the user behaviour (and contact details) on our website, are provided to Facebook. Consequently, Facebook can collect better user data and is able to display suitable adverts for our products or services. Thanks to the tools it is possible to create targeted, customised ad campaigns of Facebook.

Facebook calls data about your behaviour on our website "event data" and uses them for analytics services. That way, Facebook can create "campaign reports" about our ad campaigns' effectiveness on our behalf. Moreover, by analyses we can get a better insight in how you use our services, our website or our products. Therefore, some of these tools help us optimise your user experience on our website. With the social plugins for instance, you can share our site's contents directly on Facebook.

What data is stored by Facebook tools?

With the use of Facebook tools, personal data (customer data) may be sent to Facebook. Depending on the tools used, customer data such as name, address, telephone number and IP address may be transmitted.

Facebook uses this information to match the data with the data it has on you (if you are a Facebook member). However, before the customer data is transferred to Facebook, a so called "Hashing" takes place. This means, that a data record of any size is transformed into a string of characters, which also has the purpose of encrypting data.

Moreover, not only contact data, but also "event data" is transferred. These data are the information we receive about you on our website. To give an example, it allows us to see what subpages you visit or what products you buy from us. Facebook does not disclose the obtained information to third parties (such as advertisers), unless the company has an explicit permission or is legally obliged to do so. Also, "event data" can be linked to contact information, which helps

Facebook to offer improved, customised adverts. Finally, after the previously mentioned matching process, Facebook deletes the contact data.

To deliver optimised advertisements, Facebook only uses event data, if they have been combined with other data (that have been collected by Facebook in other ways). Facebook also uses event data for the purposes of security, protection, development and research. Many of these data are transmitted to Facebook via cookies. Cookies are little text files, that are used for storing data or information in browsers. Depending on the tools used, and on whether you are a Facebook member, a different number of cookies are placed in your browser. In the descriptions of the individual Facebook tools we will go into more detail on Facebook cookies. You can also find general information about the use of Facebook cookies at https://www.facebook.com/policies/cookies.

How long and where are the data stored?

Facebook fundamentally stores data, until they are no longer of use for their own services and products. Facebook has servers for storing their data all around the world. However, customer data is cleared within 48 hours after they have been matched with their own user data.

How can I erase my data or prevent data retention?

In accordance with the General Data Protection Regulation (GDPR) you have the right of information, rectification, transfer and deletion of your data.

The collected data is only fully deleted, when you delete your entire Facebook account. Deleting your Facebook account works as follows:

1) Click on settings in the top right side in Facebook.

2) Then, click "Your Facebook information" in the left column.

3) Now click on "Deactivation and deletion".

4) Choose "Permanently delete account" and then click on "Continue to account deletion".

5) Enter your password, click on "continue" and then on "Delete account".

The retention of data Facebook receives via our site is done via cookies (e.g. with social plugins), among others. You can deactivate, clear or manage both all and individual cookies in your browser. How this can be done differs depending on the browser you use. The following instructions show, how to manage cookies in your browser:

[Chrome: Clear, enable and manage cookies in Chrome](#)

[Safari: Manage cookies and website data in Safari](#)

[Firefox: Clear cookies and site data in Firefox](#)

[Internet Explorer: Delete and manage cookies](#)

[Microsoft Edge: Delete cookies in Microsoft Edge](#)

If you generally do not want to allow any cookies at all, you can set up your browser to notify you whenever a cookie is about to be set. This gives you the opportunity to decide upon the permission or deletion of every single cookie.

Legal basis

If you have consented to your data being processed and stored by integrated Facebook tools, this consent is the legal basis for data processing **(Art. 6 para. 1 lit. a GDPR)**. Generally, your data is also stored and processed on the basis of our legitimate interest **(Art. 6 para. 1 lit. f GDPR)** to maintain fast and good communication with you or other customers and business partners. Nevertheless, we only use these tools if you have given your consent. Most social media platforms also set cookies on your browser to store data. We therefore recommend you to read our privacy policy about cookies carefully and to take a look at the privacy policy or Facebook's cookie policy.

Facebook also processes data in the USA, among other countries. We would like to note, that according to the European Court of Justice, there is currently no adequate level of protection for data transfers to the USA. This can be associated with various risks to the legality and security of data processing.

Facebook uses standard contractual clauses approved by the EU Commission as basis for data processing by recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway and especially in the USA) or data transfer there (= Art. 46, paragraphs 2 and 3 of the GDPR). These clauses oblige Facebook to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses here: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847

We hope we could give you an understanding of the most important information about the use of Facebook tools and data processing. If you want to find out more on how Facebook use your data, we recommend reading the data policies at https://www.facebook.com/about/privacy/update.

Facebook Social Plugins Privacy Policy

We installed so-called social plugins from Facebook Inc. to our website. You can recognise these buttons by the classic Facebook logo, the "Like" button (hand with raised thumb) or by a "Facebook plugin" label. A social plugin is a small part of Facebook that is integrated into our page. Each plugin has its own function. The most used functions are the well-known "Like" and "Share" buttons.

Facebook offers the following social plugins:

- "Save" button
- "Like" button, Share, Send and Quote
- Page plugin
- Comments
- Messenger plugin

- Embedded posts and video player
- Group Plugin

At https://developers.facebook.com/docs/plugins you will find more information on how the individual plugins are used. On the one hand, we use the social plug-ins to offer you a better user experience on our site, and on the other hand because Facebook can optimise our advertisements with it.

If you have a Facebook account or have already visited facebook.com, Facebook has already placed at least one cookie in your browser. In this case, your browser sends information to Facebook via this cookie as soon as you visit our website or interact with social plugins (e.g. the "Like" button).

The received information will be deleted or anonymised within 90 days. According to Facebook, this data includes your IP address, the websites you have visited, the date, time and other information relating to your browser.

In order to prevent Facebook from collecting much data and matching it with your Facebook data during your visit to our website, you must log out of Facebook while you visit our website.

If you are not logged in to Facebook or do not have a Facebook account, your browser sends less information to Facebook because you have fewer Facebook cookies. Nevertheless, data such as your IP address or which website you are visiting can be transmitted to Facebook. We would like to explicitly point out that we do not know what exact data is collected. However, based on our current knowledge, we want to try informing you as best we can about data processing. You can also read about how Facebook uses the data in the company's data policy at https://www.facebook.com/about/privacy/update.

At least the following cookies are set in your browser when you visit a website with social plugins from Facebook:

Name: dpr
Value: no information
Purpose: This cookie is used to make the social plugins work on our website.
Expiry date: after end of session

Name: fr
Value: 0jieyh4112328747c2GnlufEJ9..Bde09j...1.0.Bde09j
Purpose: The cookie is also necessary for the plugins to function properly
Expiry date: after 3 months

Note: These cookies were set after our test and may be placed even if you are not a Facebook member.

If you are registered with Facebook, you can change your settings for advertisements yourself at https://www.facebook.com/ads/preferences/?entry_product=ad_settings_screen. If you are not a Facebook user, you can go to https://www.youronlinechoices.com/uk/your-ad-choices/ and manage your usage-based online advertising. There you have the option to deactivate or activate providers.

If you want to learn more about Facebook's data protection, we recommend the company's own data policies at https://www.facebook.com/policy.php.

Facebook Fanpage Privacy Policy

We also have a Facebook fan page for our website. The provider of this service is the American company Meta Platforms Inc. The responsible entity for the European area is the company Meta Platforms Ireland Limited (4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland).

Facebook also processes data in the USA, among other countries. We would like to note, that according to the European Court of Justice, there is currently no adequate level of protection for data transfers to the USA. This can be associated with various risks to the legality and security of data processing.

Facebook uses standard contractual clauses approved by the EU Commission as the basis for data processing by recipients based in third countries (i. e. outside the European Union, Iceland, Liechtenstein, Norway, and thus especially in the USA) or data transfer there (= Art. 46, paragraphs 2 and 3 of the GDPR). Standard Contractual Clauses (SCC) are legal templates provided by the EU Commission. Their purpose is to ensure that your data complies with European data privacy standards, even if your data is transferred to and stored in third countries (such as the USA). With these clauses, Facebook commits to comply with the EU's level of data protection when processing relevant data, even if it is stored, processed and managed in the USA. These clauses are based on an implementing order by the EU Commission. You can find the order and the standard contractual clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=en

Facebook's data processing terms, which correspond to the Standard Contractual Clauses, can be found at https://www.facebook.com/legal/terms/dataprocessing.

You can find out more about the data that is processed by using Facebook in their Privacy Policy at https://www.facebook.com/about/privacy.

Instagram Privacy Policy

Instagram Privacy Policy Overview
Affected parties: website visitors
Purpose: optimising our service
Processed data: includes data on user behaviour, information about your device and IP address.
More details can be found in the privacy policy below.
Storage period: until Instagram no longer needs the data for its purposes
Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is Instagram?

We have integrated functions of Instagram to our website. Instagram is a social media platform of the company Instagram LLC, 1601 Willow Rd, Menlo Park CA 94025, USA. Since 2012, Instagram is a

subsidiary company of Facebook Inc. and is a part of Facebook's products. The inclusion of Instagram's contents on our website is called embedding. With this, we can show you Instagram contents such as buttons, photos or videos directly on our website. If you open websites of our online presence, that have an integrated Instagram function, data gets transmitted to, as well as stored and processed by Instagram. Instagram uses the same systems and technologies as Facebook. Therefore, your data will be processed across all Facebook firms.

In the following, we want to give you a more detailed insight on why Instagram collects data, what data these are and how you can control data processing. As Instagram belongs to Facebook Inc., we have, on the one hand received this information from the Instagram guidelines, and on the other hand from Facebook's Data Policy.

Instagram is one of the most famous social media networks worldwide. Instagram combines the benefits of a blog with the benefits of audio-visual platforms such as YouTube or Vimeo. To "Insta" (how the platform is casually called by many users) you can upload photos and short videos, edit them with different filters and also share them to other social networks. Also, if you do not want to be active on Instagram yourself, you can just follow other interesting users.

Why do we use Instagram on our website?

Instagram is a social media platform whose success has skyrocketed within recent years. Naturally, we have also reacted to this boom. We want you to feel as comfortable as possible on our website. Therefore, we attach great importance to diversified contents. With the embedded Instagram features we can enrich our content with helpful, funny or exciting Instagram contents. Since Instagram is a subsidiary company of Facebook, the collected data can also serve us for customised advertising on Facebook. Hence, only persons who are genuinely interested in our products or services can see our ads.

Instagram also uses the collected data for tracking and analysis purposes. We receive summarised statistics and therefore more insight to your wishes and interests. It is important to mention that these reports do not identify you personally.

What data is stored by Instagram?

Whenever you land on one of our sites, which have Instagram functions (i.e. Instagram photos or plugins) integrated to them, your browser automatically connects with Instagram's servers. Thereby, data is sent to, as well as saved and processed by Instagram. This always happens, whether you have an Instagram account or not. Moreover, it includes information on our website, your computer, your purchases, the advertisements you see and on how you use our offer. The date and time of your interaction is also stored. If you have an Instagram account or are logged in, Instagram saves significantly more data on you.

Facebook distinguishes between customer data and event data. We assume this is also the case for Instagram. Customer data are for example names, addresses, phone numbers and IP addresses. These data are only transmitted to Instagram, if they have been "hashed" first. Thereby, a set of data is transformed into a string of characters, which encrypts any contact data. Moreover, the aforementioned "event data" (data on your user behaviour) is transmitted as well. It is also possible,

that contact data may get combined with event data. The collected data data is matched with any data Instagram already has on you.

Furthermore, the gathered data are transferred to Facebook via little text files (cookies) which usually get set in your browser. Depending on the Instagram function used, and whether you have an Instagram account yourself, the amount of data that gets stored varies.

We assume data processing on Instagram works the same way as on Facebook. Therefore, if you have an account on Instagram or have visited www.instagram.com, Instagram has set at least one cookie. If this is the case, your browser uses the cookie to send information to Instagram, as soon as you come across an Instagram function. No later than 90 days (after matching) the data is deleted or anonymised. Even though we have studied Instagram's data processing in-depth, we cannot tell for sure what exact data Instagram collects and retains.

In the following we will show you a list of the least cookies placed in your browser when click on an Instagram function (e.g. button or an Insta picture). In our test we assume you do not have an Instagram account, since if you would be logged in to your Instagram account, your browser would place significantly more cookies.

The following cookies were used in our test:

Name: csrftoken
Value: ""
Purpose: This cookie is most likely set for security reasons to prevent falsifications of requests. We could not find out more information on it.
Expiry date: after one year

Name: mid
Value: ""
Purpose: Instagram places this cookie to optimise its own offers and services in- and outside of Instagram. The cookie allocates a unique user ID.
Expiry date: after end of session

Name: fbsr_112328747124024
Value: no information
Purpose: This cookie stores the login request of Instagram app users.
Expiry date: after end of session

Name: rur
Value: ATN
Purpose: This is an Instagram cookie which guarantees functionality on Instagram.
Expiry date: after end of session

Name: urlgen
Value: "{"194.96.75.33": 1901}:1iEtYv:Y833k2_UjKvXgYe112328747"
Purpose: This cookie serves Instagram's marketing purposes.
Expiry date: after end of session

Note: We do not claim this list to be exhaustive. The cookies that are placed in each individual case, depend on the functions embedded as well as on your use of Instagram.

How long and where are these data stored?

Instagram shares the information obtained within the Facebook businesses with external partners and persons you are globally connected with. Data processing is done according to Facebook's internal data policy. Your data is distributed to Facebook's servers across the world, partially for security reasons. Most of these servers are in the USA.

How can I erase my data or prevent data retention?

Thanks to the General Data Protection Regulation (GDPR), you have the right of information, rectification, transfer and deletion of your data. Furthermore, you can manage your data in Instagram's settings. If you want to delete your data on Instagram completely, you will have to delete your Instagram account permanently.

And this is how an Instagram account can be deleted:

First, open the Instagram app. Then, navigate to your profile page, select the three bars in the top right, choose "Settings" and then click "Help". Now, you will be redirected to the company's website, where you must click on "Managing Your Account" and then "Delete Your Account".

When you delete your account completely, Instagram deletes posts such as your photos and status updates. Any information other people shared about you are not a part of your account and do therefore not get deleted.

As mentioned before, Instagram primarily stores your data via cookies. You can manage, deactivate or delete these cookies in your browser. Depending on your browser, managing them varies a bit. We will show you the instructions of the most relevant browsers here.

[Chrome: Clear, enable and manage cookies in Chrome](#)

[Safari: Manage cookies and website data in Safari](#)

[Firefox: Clear cookies and site data in Firefox](#)

[Internet Explorer: Delete and manage cookies](#)

[Microsoft Edge: Delete cookies in Microsoft Edge](#)

Generally, you can set your browser to notify you whenever a cookie is about to be set. Then you can individually decide upon the permission of every cookie.

Legal basis

If you have consented to the processing and storage of your data by integrated social media elements, this consent is the legal basis for data processing **(Art. 6 para. 1 lit. a GDPR)** . Generally,

your data is also stored and processed on the basis of our legitimate interest **(Art. 6 para. 1 lit. f GDPR)** to maintain fast and good communication with you or other customers and business partners. We only use the integrated social media elements if you have given your consent. Most social media platforms also place cookies in your browser to store data. We therefore recommend you to read our privacy policy about cookies carefully and to take a look at the privacy policy or the cookie policy of the respective service provider.

Instagram and Facebook also process data in the USA, among other countries. We would like to note, that according to the European Court of Justice, there is currently no adequate level of protection for data transfer to the USA. This can be associated with various risks to the legality and security of data processing.

As a basis for data processing by recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway and especially in the USA) or data transfers there, Facebook uses standard contractual clauses approved by the EU Commission (= Art. 46, paragraphs 2 and 3 of the GDPR). These clauses oblige Facebook to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses here:
https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847

We have tried to give you the most important information about data processing by Instagram. On https://help.instagram.com/519522125107875
you can take a closer look at Instagram's data guidelines.

LinkedIn Privacy Policy

LinkedIn Privacy Policy Overview
Affected parties: website visitors
Purpose: optimisation of our service
Processed data: includes data on user behaviour, information about your device and IP address.
More details can be found in the privacy policy below.
Storage period: the data is generally deleted within 30 days
Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is LinkedIn?

On our website we use social plugins from the social media network LinkedIn, of the LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA. Social plugins can be feeds, content sharing or a link to our LinkedIn page. Social plugins are clearly marked with the well-known LinkedIn logo and for example allow sharing interesting content directly via our website. Moreover, LinkedIn Ireland Unlimited Company Wilton Place in Dublin is responsible for data processing in the European Economic Area and Switzerland.

By embedding these plugins, data can be sent to, as well as stored and processed by LinkedIn. In this privacy policy we want to inform you what data this is, how the network uses this data and how

you can manage or prevent data retention.

LinkedIn is the largest social network for business contacts. In contrast to e.g. Facebook, LinkedIn focuses exclusively on establishing business connections. Therefore, companies can present services and products on the platform and establish business relationships. Many people also use LinkedIn to find a job or to find suitable employees for their own company. In Germany alone, the network has over 11 million members. In Austria there are about 1.3 million.

Why do we use LinkedIn on our website?

We know how busy you are. You just cannot keep up with following every single social media channel. Even if it would really be worth it, as it is with our channels, since we keep posting interesting news and articles worth spreading. Therefore, on our website we have created the opportunity to share interesting content directly on LinkedIn, or to refer directly to our LinkedIn page. We consider built-in social plugins as an extended service on our website. The data LinkedIn collects also help us to display potential advertising measures only to people who are interested in our offer.

What data are stored by LinkedIn?

LinkedIn stores no personal data due to the mere integration of social plugins. LinkedIn calls the data generated by plugins passive impressions. However, if you click on a social plugin to e.g. share our content, the platform stores personal data as so-called "active impressions". This happens regardless of whether you have a LinkedIn account or not. If you are logged in, the collected data will be assigned to your account.

When you interact with our plugins, your browser establishes a direct connection to LinkedIn's servers. Through that, the company logs various usage data. These may include your IP address, login data, device information or information about your internet or cellular provider. If you use LinkedIn services via your smartphone, your location may also be identified (after you have given permission). Moreover, LinkedIn can share these data with third-party advertisers in "hashed" form. Hashing means that a data set is transformed into a character string. This allows data to be encrypted, which prevents persons from getting identified.

Most data on of your user behaviour is stored in cookies. These are small text files that usually get placed in your browser. Furthermore, LinkedIn can also use web beacons, pixel tags, display tags and other device recognitions.

Various tests also show which cookies are set when a user interacts with a social plug-in. We do not claim for the information we found to be exhaustive, as it only serves as an example. The following cookies were set without being logged in to LinkedIn:

Name: bcookie
Value: =2&34aab2aa-2ae1-4d2a-8baf-c2e2d7235c16112328747-
Purpose: This cookie is a so-called "browser ID cookie" and stores your identification number (ID).
Expiry date: after 2 years

Name: lang
Value: v=2&lang=en-gb
Purpose: This cookie saves your default or preferred language.
Expiry date: after end of session

Name: lidc
Value: 1818367:t=1571904767:s=AQF6KNnJ0G112328747...
Purpose: This cookie is used for routing. Routing records how you found your way to LinkedIn and how you navigate through the website.
Expiry date: after 24 hours

Name: rtc
Value: kt0lrv3NF3x3t6xvDgGrZGDKkX
Purpose: No further information could be found about this cookie.
Expiry date: after 2 minutes

Name: JSESSIONID
Value: ajax:1123287472900777718326218137
Purpose: This is a session cookie that LinkedIn uses to maintain anonymous user sessions through the server.
Expiry date: after end of session

Name: bscookie
Value: "v=1&201910230812...
Purpose: This cookie is a security cookie. LinkedIn describes it as a secure browser ID cookie.
Expiry date: after 2 years

Name: fid
Value: AQHj7Ii23ZBcqAAAA...
Purpose: We could not find any further information about this cookie.
Expiry date: after 7 days

Note: LinkedIn also works with third parties. That is why we identified the Google Analytics cookies _ga and _gat in our test.

How long and where are the data stored?

In general, LinkedIn retains your personal data for as long as the company considers it necessary for providing its services. However, LinkedIn deletes your personal data when you delete your account. In some exceptional cases, LinkedIn keeps some summarised and anonymised data, even account deletions. As soon as you delete your account, it may take up to a day until other people can no longer see your data. LinkedIn generally deletes the data within 30 days. However, LinkedIn retains data if it is necessary for legal reasons. Also, data that can no longer be assigned to any person remains stored even after the account is closed. The data are stored on various servers in America and presumably also in Europe.

How can I delete my data or prevent data retention?

You have the right to access and delete your personal data at any time. In your LinkedIn account you can manage, change and delete your data. Moreover, you can request a copy of your personal data from LinkedIn.

How to access account data in your LinkedIn profile:

In LinkedIn, click on your profile icon and select the "Settings & Privacy" section. Now click on "Privacy" and then on the section "How LinkedIn uses your data on". Then, click "Change" in the row with "Manage your data and activity". There you can instantly view selected data on your web activity and your account history.

In your browser you also have the option of preventing data processing by LinkedIn. As mentioned above, LinkedIn stores most data via cookies that are placed in your browser. You can manage, deactivate or delete these cookies. Depending on which browser you have, these settings work a little different. You can find the instructions for the most common browsers here:

[Chrome: Clear, enable and manage cookies in Chrome](#)

[Safari: Manage cookies and website data in Safari](#)

[Firefox: Clear cookies and site data in Firefox](#)

[Internet Explorer: Delete and manage cookies](#)

[Microsoft Edge: Delete cookies in Microsoft Edge](#)

You can generally set your browser to always notify you when a cookie is about to be set. Then you can always decide individually whether you want to allow the cookie or not.

Legal basis

If you have consented to the processing and storage of your data by integrated social media elements, your consent is the legal basis for data processing **(Art. 6 para. 1 lit. a GDPR)**. Generally, your data is also stored and processed on the basis of our legitimate interest **(Art. 6 para. 1 lit. f GDPR)** to maintain fast and good communication with you or other customers and business partners. We only use the integrated social media elements if you have given your consent. Most social media platforms also place cookies in your browser to store data. We therefore recommend you to read our privacy policy about cookies carefully and take a look at the privacy policy or the cookie policy of the respective service provider.

LinkedIn also processes data in the USA, among other countries. We would like to note, that according to the European Court of Justice, there is currently no adequate level of protection for data transfers to the USA. This can be associated with various risks to the legality and security of data processing.

LinkedIn uses standard contractual clauses approved by the EU Commission as the basis for data

processing by recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, and especially in the USA) or data transfer there (= Art. 46, paragraph 2 and 3 of the GDPR). These clauses oblige LinkedIn to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses here: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847

We have tried to provide you with the most important information about data processing by LinkedIn. On https://www.linkedin.com/legal/privacy-policy you can find out more on data processing by the social media network LinkedIn.

Cookie Consent Management Platform

Cookie Consent Management Platform Overview
Affected parties: Website visitors
Purpose: Obtaining and managing consent to certain cookies and thus the use of certain tools
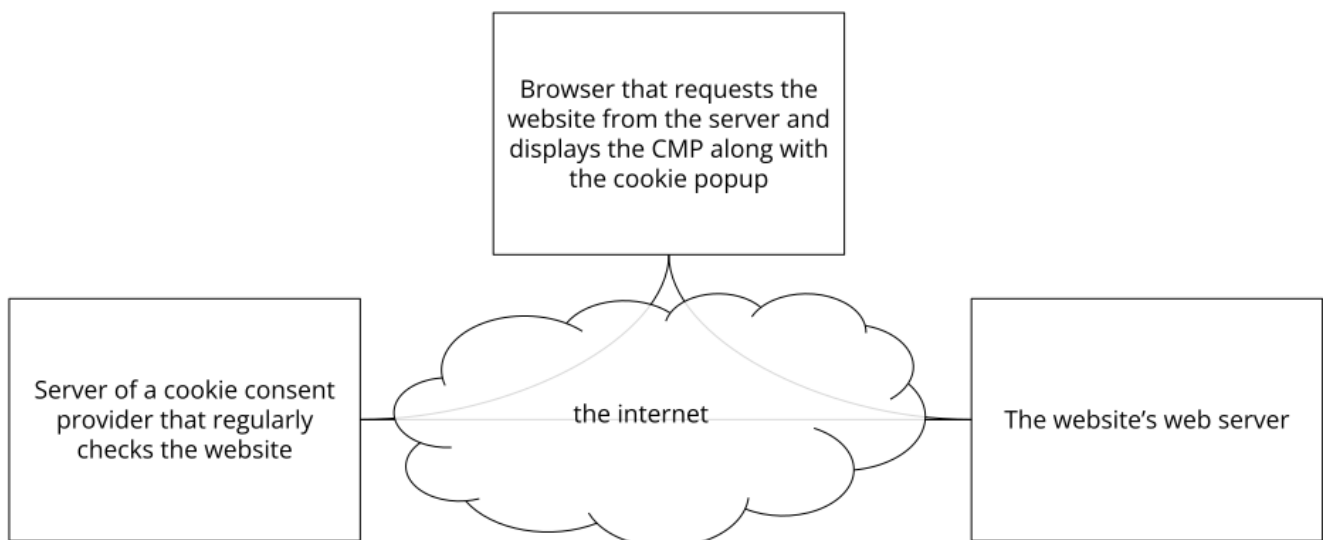Processed data: data for managing cookie settings such as IP address, time of consent, type of consent and individual consent. You can find more details on this directly with the tool that is being used.
Storage period: depends on the tool used, periods of several years can be assumed
Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is a cookie consent management platform?

We use a Consent Management Platform (CMP) software on our website that makes it easier for us and you to handle the scripts and cookies used correctly and securely. The software automatically creates a cookie pop-up, scans and controls all scripts and cookies, provides you with the cookie consent required under data protection law and helps you and us to keep track of all cookies. Most cookie consent management tools identify and categorize all existing cookies. As a website visitor, you then decide for yourself whether and which scripts and cookies you allow or not. The following graphic shows the relationship between browser, web server and CMP.

Browser that requests the website from the server and displays the CMP along with the cookie popup

Server of a cookie consent provider that regularly checks the website

the internet

The website's web server

Why do we use a cookie management tool?

Our goal is to offer you the best possible transparency in the area of data protection. We are also legally obliged to do so. We want to inform you as well as possible about all tools and all cookies that can save and process your data. It is also your right to decide for yourself which cookies you accept and which you do not. In order to grant you this right, we first need to know exactly which cookies actually landed on our website. Thanks to a cookie management tool, which regularly scans the website for all cookies present, we know about all cookies and can provide you with GDPR-compliant information. You can then use the consent system to accept or reject cookies.

Which data are processed?

As part of our cookie management tool, you can manage each individual cookie yourself and have complete control over the storage and processing of your data. The declaration of your consent is stored so that we do not have to ask you every time you visit our website and we can also prove your consent if required by law. This is saved either in an opt-in cookie or on a server. The storage time of your cookie consent varies depending on the provider of the cookie management tool. Usually this data (e.g. pseudonymous user ID, time of consent, detailed information on the cookie categories or tools, browser, device information) is stored for up to two years.

Duration of data processing

We will inform you below about the duration of the data processing if we have further information. In general, we only process personal data for as long as is absolutely necessary for the provision of our services and products. Data stored in cookies are stored for different lengths of time. Some cookies are deleted after you leave the website, others may be stored in your browser for a few years. The exact duration of the data processing depends on the tool used, in most cases you should be prepared for a storage period of several years. In the respective data protection declarations of the individual providers, you will usually receive precise information about the duration of the data processing.

Right of objection

You also have the right and the option to revoke your consent to the use of cookies at any time. This works either via our cookie management tool or via other opt-out functions. For example, you can also prevent data collection by cookies by managing, deactivating or deleting cookies in your browser.

Information on special cookie management tools can be found – if available – in the following sections.

Legal basis

If you agree to cookies, your personal data will be processed and stored via these cookies. If we are allowed to use cookies with your **consent** (Article 6 paragraph 1 lit. a GDPR), this consent is also the legal basis for the use of cookies and the processing of your data. In order to be able to manage the

consent to cookies and to enable you to give your consent, a cookie consent management platform software is used. The use of this software enables us to operate the website in an efficient and legally compliant manner, which is a **legitimate interest** (Article 6 paragraph 1 lit. f GDPR).

BorlabsCookie Privacy Policy

On our website we use BorlabsCookie, which is one of the tools that store your consent to cookies. The provider of this service is the German company Borlabs – Benjamin A. Bornschein, Rübenkamp 32, 22305 Hamburg, Germany. You can find out more about the data that is processed by the use of BorlabsCookie in their Privacy Policy at https://borlabs.io/privacy/.

Web Design Introduction

> **Web Design Privacy Policy Overview**
> Affected parties: website visitors
> Purpose: improvement of user experience
> Processed data: depends heavily on the services used. Usually, data such as IP address, technical data, language settings, browser version, screen resolution and browser name are processed. You can find more details directly with the respective web design tools.
> Storage duration: depends on the tools used
> Legal bases: Article 6 paragraph 1 lit. a GDPR (consent), Article 6 paragraph 1 lit. f GDPR (legitimate interests)

What is web design?

We use various tools on our website for the purpose of our web design. Contrary to common belief, web design is not just about making our website look nice, but rather also about functionality and performance. But of course, a good-looking website is also a major goal of professional web design. Web design is a part of media design and deals with the visual as well as the structural and functional design of a website. Our aim with our web design is to improve your experience on our site. In web design jargon, this is called User Experience (UX) and usability. User Experience entails all impressions and experiences that website visitors come across on a website. What is more, usability is part of the User Experience, as it determines how user-friendly a website is. This includes the clear structuring of content, subpages or products, along with how quickly and easily the website enables you to find what you are looking for. In order to offer you the best possible experience on our website, we also use so-called third-party web design tools. Therefore, all tools and services that help improve our website's design are classified under the category "web design". This may, for example, include fonts, various plugins or other integrated web design functions.

Why do we use web design tools?

The way you absorb information on a website depends very much on its structure, functionality and visual perception. Therefore, good and professional web design has become increasingly important for us. We are constantly working on improving our site as a way of further extending our services for you as a website visitor. Furthermore, a beautiful and functioning website also has

economic advantages for us. Needless to say, you will only visit it and take advantage of our offers if you feel completely at ease.

What data is stored by web design tools?

When you visit our website, any web design elements integrated into our pages may process your data. The exact data that is processed depends on the tools used. Below you can see exactly which tools we use for our website. For more information about data processing, we recommend you also read the respective privacy policy of the respective tools. There you can usually find out which data is processed, whether cookies are used and how long the data is stored. Moreover, fonts such as Google Fonts, for example, also automatically transmit information such as your language settings, IP address, browser version, browser screen resolution and browser name to Google's servers.

Duration of data processing

Data processing times are very individual and depend on the web design elements used. For example, when cookies are used, the retention period can be as little as a minute, but it may also be a few years. Please make yourself familiar with this topic. You may for example read our general section on cookies as well as the Privacy Policies of the tools used. There you can likely find out exactly which cookies are used and what information is stored there. For example, Google Font files are stored for one year, in order to improve the loading speed of a website. In principle, data is only kept for as long as is necessary to provide the service. But legal requirements may require data to be stored for longer.

Right to object

You also retain the right and the option to revoke your consent to the use of cookies or third-party providers at any time. You can do this either via our cookie management tool or via other opt-out functions. You can also prevent cookies from collecting your data by managing, deactivating or deleting the cookies in your browser. However, among web design elements (typically fonts) there is also data that cannot be erased easily. This is the case whenever data is automatically collected as soon as a page is accessed and then directly transmitted to a third party (e.g. Google). In these cases, please contact the support of the respective provider. In the case of Google, you can reach support at https://support.google.com/?hl=de.

Legal Basis

If you have consented to the use of web design tools, this consent serves as the legal basis for the relevant data processing. According to Article 6 (1) (a) GDPR (consent), your consent represents the legal basis for the processing of personal data, as it may occur when it is collected by web design tools. We also have a legitimate interest in web design to improve on our website. After all, only then can we provide you with a beautiful and professional web offer. The corresponding legal basis for this is Article 6 (1) (f) GDPR (legitimate interests). However, we strongly want to emphasise once more that we only use web design tools if you have given your consent.

You can find information on different web design tools – if available – in the following sections.

Google Fonts Local Privacy Policy

On our website we use Google Fonts, by the company Google Inc. The responsible entity for the European area is Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland). We have integrated Google fonts locally, i.e. on our web server and not on Google's servers. This means that no connection to Google's servers and therefore no data transfer or retention take place.

What are Google Fonts?

Google Fonts was previously called Google Web Fonts. It is an interactive list with over 800 fonts which [Google](#) offer for free use. With the use of Google Fonts, it is possible to utilise fonts without uploading them to your own server. In order to prevent any transfer of information to Google's servers, we downloaded the fonts to our own server. This way we can comply with data privacy and do not transmit any data to Google Fonts.

Online Map Services Introduction

> **Online Map Services Privacy Policy Overview**
> Affected parties: website visitors
> Purpose: Improvement of user experience
> Processed data: the data that is processed depends heavily on the services used. Usually, it is your IP address, location data, search queries and/or technical data. You can find more details on this under the respective tools used.
> Storage duration: depends on the tools used
> Legal bases: Article 6 paragraph 1 lit. a GDPR (consent), Article 6 paragraph 1 lit. f GDPR (legitimate interests)

What are Online Map Services?

We also use online map services for our website as an extended service. Google Maps is probably the service you are most familiar with. But there are also other providers out there that specialise in creating digital maps. These services allow the display of locations, route maps or other geographical information directly via our website. Thanks to an integrated map service, you no longer have to leave our website to e. g. view the route to a location. In order to ensure that the online map can run on our website, we have integrated map sections within our HTML code. This way the services can display street maps, the earth's surface, or aerial or satellite imagery. If you use the built-in map service, your data will be transferred to the tool used, where it will be retained. This may also include your personal data.

Why do we use Online Map Services on our website?

Generally speaking, it is imperative for us to offer you a pleasant time on our website. Of course, we know that you will most likely only enjoy your time here if you can easily find your way around and find all the information you need quickly and easily. Therefore, we decided that an online map system may be a significant optimisation of our website's service. After all, you can use the map system to easily view route descriptions, locations or any other points of interest – without leaving

our site. Needless to say, it is certainly also very practical that you can easily see where our company headquarters are so that you can find us quickly and safely. As you can see, there are just a lot of advantages – and we clearly consider online map services on our website to be part of our customer service.

What data is stored by Online Map Services?

If you open a page on our website with an online map function installed, your personal data may be transmitted to the relevant service, where it may be stored. This usually includes your IP address, which may also be used to determine your approximate location. In addition to your IP address, data such as the search terms you entered, as well as your longitude and latitude coordinates will be stored. If you e. g. enter an address for route planning, this data will also be stored. This data is not stored by us but instead on the servers of the integrated tools. You can think of it like this: You may be on our website, but when you interact with a mapping service, that interaction is actually happening on their website. Moreover, in order for the service to function properly, at least one cookie is usually set in your browser. As an example, Google Maps also uses cookies to record user behaviour, with which it can optimise its own service and offer personalised advertising. You can find out more about cookies in our "Cookies" section.

How long and where is the data stored?

Every online map service processes different user data. Provided we have further information, we will inform you about the duration of data processing in the corresponding sections on the individual tools below. Generally, personal data is only retained for as long as is necessary to provide the service. Google Maps e. g. stores certain data for a specified period of time, but you must erase other data yourself. At Mapbox, for example, your IP address is stored for 30 days after which it is deleted. As you can see, each tool stores data for different lengths of time. We thus recommend you take a closer look at the privacy policies of the tools used.

The providers may use cookies to store data on your user behaviour in relation to their map services. You can find more information about cookies in our "Cookies" section, but in the individual providers' privacy policies you can most probably also find out which cookies may be used. In most cases, however, this is only an indicative list and is not exhaustive.

Right to object

You always have the possibility and the right to access your personal data and to object to its use and processing. You can also revoke the consent you gave to us at any time. This is usually easiest through the cookie consent tool. However, there are other opt-out tools that you can use. You can also manage, erase or deactivate any cookies set by the used providers yourself with just a few mouse clicks. However, this may lead to some service functions stopping to work as usual. It also depends on your browser how you can manage cookies there. In our "Cookies" section you will find links to instructions of the most popular browsers.

Legal Basis

If you have agreed to the use of an online map service, the legal basis for the corresponding data processing is this consent. According to Article 6 Paragraph 1 lit. (consent) this consent is the legal basis for the processing of personal data as may occur when collected by an online map service.

We also have a legitimate interest in using an online map service to optimise our service on our website. The corresponding legal basis for this is Article 6 (1) (f) GDPR (legitimate interests). However, we only use an online map service if you have given your consent. We definitely wanted to stress this point once again.

You can find information on specific online map services – if available – in the following sections.

Google Maps Privacy Policy

Google Maps Privacy Policy Overview
Affected parties: website visitors
Purpose: service optimisation
Processed data: data such as entered search terms, IP address as well as latitude and longitude coordinates.
You can find more details on this in the Privacy Policy below.
Storage duration: depending on the retained data
Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is Google Maps?

On our website we use Google Maps of the company Google Inc. (1600 Amphitheatre Parkway Mountain View, CA 94043, USA). With the use of Google Maps, we can show you locations in a better way and can therefore adjust our service to your needs. Due to the utilisation of Google Maps, data gets transferred to Google and is saved on Google's servers. In the following, we want to explain in detail what Google Maps is, why we use this Google service, what data is stored and how you can prevent this.

Google Maps is an internet maps service of the company Google Inc. With Google Maps you can search for exact locations of cities, sights, accommodations or businesses online via a PC, a tablet or an app. If businesses are represented on Google My Business, the respective location as well as other information about the company are shown there. In order to show route directions, a location's map sections can be integrated in a website through a HTML-code. Google Maps depicts the earth's surface as either a road map or as air and satellite images. Due to the street view and high-quality satellite images, it is possible for exact representations to be made.

Why do we use Google Maps on our website?

The efforts we make on this page have the goal of giving you a useful and meaningful experience on our website. Through the integration of Google Maps, we can offer you essential information on various locations. Therefore, you can spot our office address with one glance. Furthermore, the

route directions always show you the best and fastest way to us. You can retrieve the route directions for traveling either by car, by public transport, on foot or by bike. The integration of Google Maps is a part of our customer service.

What data is stored by Google Maps?

For Google Maps to offer its full services, the company must collect and store your data. This includes your entered search terms, your IP-address as well as your longitude and latitude coordinates. When you use the route-planner function, the entered start address is stored also. However, this data retention happens on Google Maps' websites. We can only inform you about it but cannot influence it in any way. Since we have included Google Maps on our website, Google will set at least one cookie (Name: NID) into your browser. This cookie saves data on your user behaviour. Google primarily uses this data to optimise ist own services and to provide you with individual, personalised advertisements.

The following cookies are set in your browser due to the integration of Google Maps:

Name: NID
Value: 188=h26c1Ktha7fCQTx8rXgLyATyITJ112328747-5
Purpose: Google uses NID in order to adjust advertments to your Google searches. With the cookie's help Google "remembers" your most frequently entered search queries or your previous interaction with ads. That way you always receive customised adertisments. The cookie contains a unique ID, wich Google uses to collect your personal settings for advertising porposes.
Expiration date: after 6 months

Note: We cannot guarantee completeness of the information on saved data. This is, because especially concerning the use of cookies, changes can happen anytime. To identify the cookie NID, a test page was created, to which Google Maps was included.

How long and where is the data stored?

There are Google servers in data centres across the entire planet. However, most servers are in America. For this reason, your data is widely stored in the USA. Here you can read in detail about where the Google servers are located: https://www.google.com/about/datacenters/locations/?hl=en

Google distributes data to various data carriers. This makes it possible to retrieve the data faster and to better protect it from possible attempted manipulations. Every server has emergency programs. Thus, should for example a problem with Google's hardware occur or should a natural disaster impact the servers, any data will quite certainly stay protected.

Moreover, Google saves some data for a specified period. With some other data on the other hand, Google only offers the opportunity for deleting it manually. Furthermore, the company anonymises information (e.g. advertising data) in server logs, by deleting a part of the IP-address and cookie information after 9 to 18 months.

How can I erase my data, or prevent data retention?

Due to the automatic delete function for location and activity data, which was introduced in 2019, information that is used for determining your location and web or app activity is saved for either 3 or 18 months, depending on your preferred decision, and is deleted thereafter. Furthermore, it is possible to delete this data manually from your browser history via your Google account anytime. If you want to prevent the determination of your location altogether, you must pause the category "Web and app activity" in your Google account. Click on "Data and personalisation" and then choose the option "Activity controls". Here you can switch the activities on or off.

Moreover, in your browser you can deactivate, delete or manage individual cookies. This function can differ a little, depending on what browser you are using. The following instructions will show you how to manage cookies in your browser:

Chrome: Clear, enable and manage cookies in Chrome

Safari: Manage cookies and website data in Safari

Firefox: Clear cookies and site data in Firefox

Internet Explorer: Delete and manage cookies

Microsoft Edge: Delete cookies in Microsoft Edge

If you generally do not want to permit any cookies, you can set up your browser in a way that ensures you get informed whenever a cookie is about to be placed. That way you can decide to either permit or refuse every single cookie.

Please note, that when using this tool, your data may also be stored and processed outside the EU. Most third countries (including the USA) are not considered secure under current European data protection law. Data to insecure third countries must not simply be transferred to, stored and processed there unless there are suitable guarantees (such as EU Standard Contractual Clauses) between us and the non-European service provider.

Legal basis

If you have consented to the use of Google Maps, your consent is the legal basis for the corresponding data processing. According to **Art. 6 paragraph 1 lit. a GDPR (consent)** this consent is the legal basis for the processing of personal data, as can occur when processed by Google Maps.

We also have a legitimate interest in using Google Maps to optimise our online service. The corresponding legal basis for this is **Art. 6 para. 1 lit. f GDPR (legitimate interests)**. Nevertheless, we only use Google Maps if you have given your consent to it.

Google also processes data in the USA, among other countries. We would like to note, that according to the European Court of Justice, there is currently no adequate level of protection for data transfers to the USA. This can be associated with various risks to the legality and security of data processing.

Google uses standard contractual clauses approved by the EU Commission as basis for data processing by recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway and especially in the USA) or data transfer there (= Art. 46, paragraphs 2 and 3 of the GDPR). These clauses oblige Google to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses here: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847

The Google Ads Data Processing Terms, which reference the standard contractual clauses, can be found at https://business.safety.google/intl/en/adsprocessorterms/.

If you want to find out more about Google's data processing, we recommend you to read the company's own Privacy Policy at https://policies.google.com/privacy?hl=en-GB.

Explanation of the terminology used

We always strive to make our privacy policy as clear and comprehensible as possible. However, this is not always easy, especially when it comes to technical and legal matters. It is often sensible to use legal terms (such as 'personal data)' or certain technical terms (such as 'cookies' or 'IP address'). But we don't want to use such terms without any explanation. This is why you will find an alphabetical list of important terms used below. These are terms we may not yet have sufficiently explained in the privacy policy. In case we have adopted any of these terms from the GDPR which are definitions, we will also list the GDPR texts here and add our own further explanations if necessary.

Supervisory authority

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

> **"supervisory authority"** means an independent public authority which is established by a Member State pursuant to Article 51;

Explanation: "Supervisory authorities" are always independent government institutions that are also authorised to give instructions in certain cases. They serve to carry out the so-called state supervision and are located in ministries, special departments or other authorities. For data protection in Austria, there is an Austrian Data Protection Authority. For Germany, there is a separate supervisory authority for each federal state.

Processor

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

"processor" *means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*

Explanation: As a company and a website owner, we are responsible for all your data we process (i. e. the 'controller'). In addition to the controller, there may also be so-called processors. This includes any company or person who processes personal data on our behalf. In addition to service providers such as tax consultants, processors can also be hosting or cloud providers, payment or newsletter providers or large companies such as Google or Microsoft.

Supervisory authority concerned

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

"supervisory authority concerned" *means a supervisory authority which is concerned by the processing of personal data because:*

a)

the controller or processor is established on the territory of the Member State of that supervisory authority;

b)

data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

c)

a complaint has been lodged with that supervisory authority;

Explanation: In Germany, each federal state has its own supervisory authority for data protection. If your company headquarters (head office) is in Germany, your point of contact is the respective supervisory authority of the respective federal state. In Austria there is only one [Data Protection Authority](#) for the whole country.

Consent

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

> *"consent"* of the data subject means 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;

Explanation: With websites, such consent is usually given via a cookie consent tool. You've most certainly come across these. Whenever you visit a website for the first time, you will usually be asked via a banner whether you agree or consent to the data processing. You can usually also make individual settings and thus decide for yourself which level of data processing you want to allow. If you do not give your consent, no personal data may be processed. Consent can of course also be given in writing, i.e. not via a tool.

Personal Data

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

> *"personenal data"* means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Explanation: Personal data is all data that can identify you as a person. This is usually data such as:

- name
- address
- email address
- postal address
- phone number
- birthday
- identification numbers such as social security number, tax identification number, ID card number or matriculation number
- banking data such as account number, credit information, account balances and more.

According to the European Court of Justice (ECJ), your **IP address is also personal data**. IT experts can use your IP address to determine at least the approximate location of your device and subsequently your location as the connection owner. Therefore, storing an IP address also requires a legal basis within the scope of the GDPR. There are also so-called **"special categories"** of personal data, which are particularly worthy of protection. These include:

- racial and ethnic origin
- political opinions

- religious or ideological beliefs
- Union membership
- genetic data such as data obtained from blood or saliva samples
- biometric data (this is information about psychological, physical or behavioural characteristics that can identify an individual).
  health Data
- Data relating to sexual orientation or sex life

Profiling

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

> **"Profiling"** *means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;*

Explanation: Profiling collects various personal data about an individual in order to learn more about that individual. On the internet, profiling is often used for advertising purposes or for credit checks. Web and advertising analysis programs e. g. collect data about your behaviour and interests on a website. This results in a special user profile that can be used to target advertising to specific target groups.

Pseudonymisation

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

> **"Pseudonymisation"** *means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;*

Explanation: Our Privacy Policy often refers to pseudonymised data. Pseudonymised data means that this data can no longer be used to identify you as a person unless additional information is added. However, you should not confuse pseudonymisation with anonymisation. With

anonymisation, there is no personal reference whatsoever, and the only way to reconstruct it would require a disproportionate amount of technical effort.

Controller

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

> **"controller"** *means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*

Explanation: In our example, we are responsible for the processing of your personal data and are therefore the "controller". If we pass on collected data to other service providers for processing, they are considered "contract processors". For this, a "Data Processing Agreement (DPA)" must be concluded.

Processing

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

> **"processing"** *means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*

Note: When we talk about processing in our Privacy Policy, we talk about any type of data processing. As mentioned above in the original GDPR declaration, this includes not only the collection but also the storage and processing of data.

Closing Remarks

Congratulations! If you are reading these lines, you have most likely familiarised yourself with our entire Privacy Policy – or at least scrolled down here. As you can see from the scope of our Privacy Policy, we do not take the protection of your personal data lightly.

We find it important to inform you about the processing of your personal data to the best of our abilities. In doing so, we not only want to tell you which data is processed but also explain to you why we use various software programs. In general, Privacy Policies have very technical and legal jargon. However, since most of you are not web developers or solicitors, we wanted to take a different approach and explain the facts in simple and clear language. Of course, this is not always possible due to the subject matter. Therefore, you can also find a more detailed explanation of the most important terms at the end of the Privacy Policy.
If you have any questions about data protection on our website, please do not hesitate to contact us or the responsible body. We wish you all the best and hope to soon welcome you to our website again.

All texts are copyrighted.