

Privacy policy

Introduction and overview

This privacy policy (version 11/30/2022-112344008) explains, in accordance with the requirements of the [General Data Protection Regulation \(EU\) 2016/679](#) and applicable national laws, which personal data (data in short) we as the responsible person - and the processors (e.g. providers) engaged by us - process, will process in the future, and what legal options you have. The terms used are to be understood as gender-neutral.

In short, it provides comprehensive information on the data we process about you.

Privacy policies usually are very technical and use legal jargon. This privacy policy, on the other hand, is intended to describe the most important things as simply and transparently as possible. In the interest of transparency, technical terms are explained in a reader-friendly manner; links to additional information are provided, and explanatory diagrams are included. Thus, we inform you in clear and simple language that we only process personal data in the course of our business activities if there is a corresponding legal basis.

I hope you find the following explanations interesting and informative and that you find some information that you did not already know.

If you still have questions, we would ask you to contact the responsible party named below or in the imprint, or to follow the available links and look at additional information on third-party sites. Our contact details can also be found in the imprint.

Scope of application

This privacy policy applies to all personal data processed by Kat&Carmel OG and to all personal data processed by companies commissioned by us (processors). By personal data we mean information in the sense of Article 4 No. 1 GDPR such as a person's name, e-mail address, and postal address. The processing of personal data ensures that we can offer and bill our services and products, whether online or offline. The scope of this privacy policy includes:

- All online presences (websites, online shops) that we operate
- Social media appearances and e-mail 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 Kat&Carmel OG via the aforementioned channels. If we enter into legal relationships with you outside of these channels, we will inform you separately if necessary.

Legal basis

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.

As far as EU law is concerned, we refer to REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016. You can read this EU General Data Protection Regulation online on EUR-Lex, the access to EU law, at <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32016R0679>

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

1. **Consent** (Article 6(1)(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(1) lit. b GDPR): In order to fulfill a contract or pre-contractual obligation with you, we process your data. For example, if we conclude a purchase contract with you, we need personal information in advance.
3. **Legal obligation** (Article 6(1)(c) GDPR): If we are subject to a legal obligation, we process your data. For example, we are legally obliged to keep invoices for accounting purposes. These usually contain personal data.
4. **Legitimate interests** (Article 6(1)(f) GDPR): In case of legitimate interests that do not restrict your fundamental rights, we reserve the right to process personal data. For example, we need to process certain data in order to operate our website in a secure and economically efficient manner. This processing is therefore a legitimate interest.

Further conditions such as making recordings in the public interest and the exercise of official authority as well as the protection of vital interests do not generally occur with us. If such a legal basis should be relevant, it will be indicated in the appropriate place.

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

- In **Austria**, this is the Federal Act on the Protection of Individuals with regard to the Processing of Personal Data (**Data Protection Act; DSG**).
- In **Germany**, the Federal **Data Protection Act; BDSG**).

If other regional or national laws apply, they will be mentioned in the following sections.

Contact details of the responsible person

If you have any questions regarding data protection or the processing of personal data, please find below the contact details of the responsible person:

Kat&Carmel OG
Nußdorfer Straße 53/12
A - 1080 Vienna
Authorized to represent: Kathryn Nenning
e-mail: kathryn@katandcarmel.com
Phone: +43 (0) 664 436 3568
Imprint: <https://www.katandcarmel.com/impressum>

Storage period

Generally, we only store personal data for as long as is necessary for the provision of our services and products. This means that we delete personal data as soon as the reason for processing the data no longer exists. In some cases, we are required by law to store certain data even after the original purpose has ceased to exist, for example for accounting purposes.

Should you wish your data to be deleted or revoke your consent to data processing, the data will be deleted as soon as possible and insofar as there is no obligation to store it.

The specific duration of the respective data processing is explained below, provided this information is available to us.

Rights according to the General Data Protection Regulation

Pursuant to Article 13, 14 of the GDPR, in order to ensure fair and transparent processing of data you have the following rights:

- According to Article 15 of the GDPR, you have the right to know 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 be informed of the following:
 - the purpose for which we are processing it;
 - the categories, i.e. types of data that are processed;
 - who receives these data and if the data are 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 complain to 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 are automatically evaluated to arrive at a personal profile of you.
- You have the right to rectification of data according to Article 16 of the 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 of the 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 for any other purposes.
- 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 of the GDPR, 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 carry out 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 person listed above!

If you believe that the processing of your data violates data protection law or that 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 Kat&Carmel OG:

Austria Data Protection Authority

Head: Mag. Dr. Andrea Jelinek

Address: Barichgasse 40-42, 1030 Vienna

Tel. number: +43 1 52 152-0

E-mail address: dsb@dsb.gv.at

Website: <https://www.dsb.gv.at/>

Data processing security

To protect personal data, we have implemented both technical and organizational measures. Where possible, we encrypt or pseudonymize personal data. In this way, we make it as difficult as possible, as far as possible, for third parties to infer personal information from our data.

Article 25 of the GDPR refers to "data protection by technical design and by data protection-friendly default settings" and thus means that both software (e.g., forms) and hardware (e.g., access to the server room) should always be designed with security in mind and that appropriate measures taken. In the following sections, we will go into more detail on specific measures, if necessary.

TLS encryption with HTTPS

TLS, encryption, and https sound very technical and they are. We use HTTPS (Hypertext Transfer Protocol Secure stands for "secure hypertext transfer protocol") to transfer data via the internet in a tap-proof manner.

This means that the complete transmission of all data from your browser to our web server is secured - no one can "listen in".

This way, we have introduced an additional layer of security and comply with data protection by design of technology (Article 25(1) GDPR). By using TLS (Transport Layer Security), an encryption protocol for secure data transmission on the Internet, we ensure the protection of confidential data.

Data transmission protection is indicated by the small lock symbol at the top left of the browser, to the left of the internet address (e.g., example.de), and the use of https (instead of http) as part of our internet address.

Communication

Communication summary

-  Data subjects: All those who communicate with us by telephone, e-mail, or online form.
-  Data processed: e.g. telephone number, name, e-mail address, form data entered. Further details are provided in the contact type used.
-  Purpose: Handling communication with customers, business partners, etc.
-  Storage period: Duration of the business case and legal requirements.
-  Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. b GDPR (contract), Art. 6 para. 1 lit. f GDPR (legitimate interests)

Personal data may be processed when you contact us and communicate by phone, e-mail, or online form.

The data are processed for the handling and processing of your question and the related business transaction. The data are stored for as long as required by law.

Persons concerned

All those who seek contact with us via phone, e-mail or online form are affected by the aforementioned processes.

Telephone

When you call us, the call data are stored pseudonymously on the terminal device and with the telecommunications provider used. In addition, data such as name and telephone number may subsequently be sent by e-mail and stored for the purpose of responding to your inquiry. The data is deleted as soon as the business case has been closed and legal requirements permit.

E-mail

If you communicate with us by e-mail, data may be stored on the end device (computer, laptop, smart phone...) and data are stored on the e-mail server. The data will be deleted as soon as the business case has been closed and legal requirements allow it.

Online forms

If you communicate with us using online forms, data are stored on our web server and may be forwarded to an e-mail address of ours. The data are deleted as soon as the business case has been terminated and legal requirements permit.

Legal basis

The processing of data is based on the following:

- Art. 6 para. 1 lit. a GDPR (Consent): You give us your consent to store and further use your data for purposes related to the business case;
- Art. 6 para. 1 lit. b GDPR (Contract): It is necessary to fulfill a contract with you or a processor such as a telephone provider, or we need to process the data for pre-contractual activities, such as preparing an offer;
- Art. 6 para. 1 lit. f GDPR (Legitimate Interests): We wish to conduct customer inquiries and business communications in a professional manner. For this purpose, certain technical facilities such as e-mail programs, exchange servers, and mobile operators are necessary in order to be able to operate communication efficiently.

Cookies

Cookies summary

 Data subjects: visitors to the website.

 Purpose: depends on the cookie in question. Further details are provided below or are available by the manufacturer of the software that sets the cookie.

 Data processed: Depending on the cookie used. Further details are provided below or are available by the manufacturer of the software that sets the cookie.

 Storage duration: Depending on the cookie, can range from hours to years.

 Legal basis: Art. 6 para. 1 lit. a GDPR (Consent), Art. 6 para. 1 lit.f GDPR (Legitimate Interests).

What are cookies?

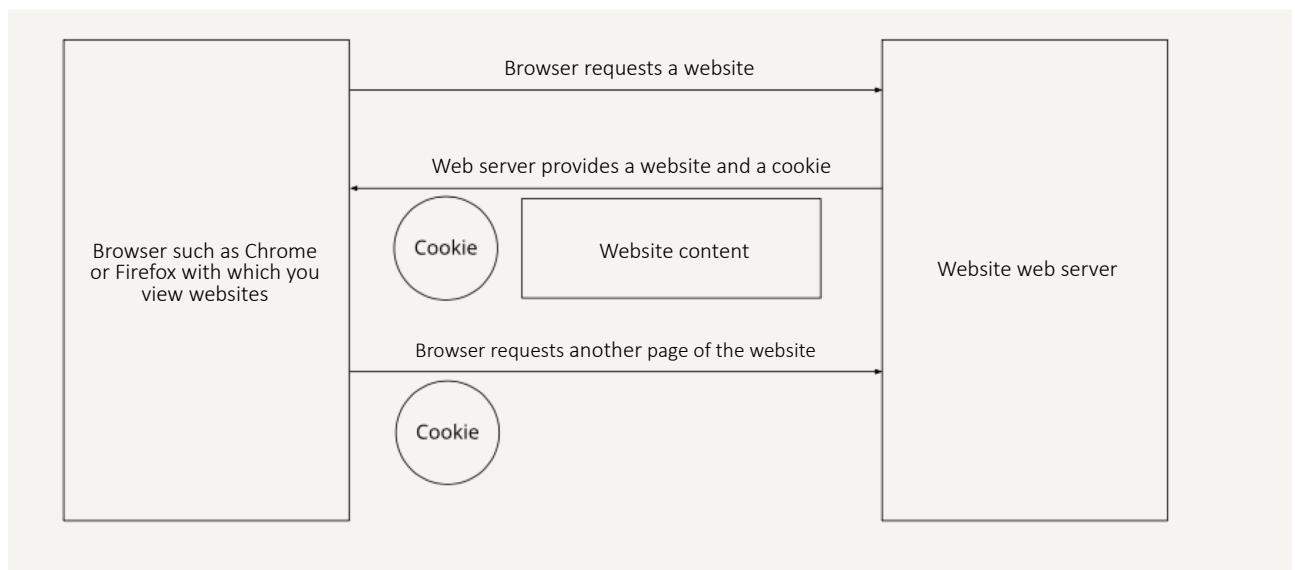
Our website uses HTTP cookies to store user-specific data. Below we explain what cookies are and why they are used so that you can better understand this privacy policy.

Whenever you browse the internet, you use a browser. Popular browsers include Chrome, Safari, Firefox, Internet Explorer, and Microsoft Edge. Most websites store small text files in your browser. These files are called cookies.

Cookies are useful little helpers. Almost all websites use cookies, namely, HTTP cookies, as other cookies exist for other applications. HTTP cookies are small files that are stored on your computer by our website. These cookie files are automatically placed in the cookie folder, effectively the "brain" of your browser. A cookie consists of a name and a value. When defining a cookie, one or more attributes must also be specified.

Cookies store certain user data, such as language or personal page settings. When you return to our site, your browser transmits the "user-related" information back to our site. Thanks to cookies, our site knows who you are and offers you the setting you are familiar with. In some browsers each cookie has its own file, in others, such as Firefox, all cookies are stored in a single file.

The following figure shows a possible interaction between a web browser, such as Chrome, and the web server. Here, the web browser requests a website and receives a cookie back from the server, which the browser uses 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, third-party cookies are created by partner websites (e.g. Google Analytics). Each cookie must be evaluated individually, as each cookie stores different data. Also, the expiration time of a cookie ranges from a few minutes to a few years. Cookies are not software programs and do not contain viruses, Trojans, or other "pests". Cookies also cannot access information on your PC.

For example, cookie data may look like this

Name: _ga

Value: GA1.2.1326744211.152112344008-9

Purpose: to distinguish website visitors

Expiration date: after 2 years

A browser should be able to support these minimum sizes

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

What types of cookies are there?

The particular cookies we use depend on the services used and are explained in the following sections. Here, we would like to briefly discuss the different types of HTTP cookies.

There are 4 types of cookies:

Essential cookies

These cookies are necessary to ensure the basic functions of the website. For example, these cookies are needed when a user adds a product to the shopping cart, then continues browsing on other pages, and only later goes to the checkout. These cookies do not delete the shopping cart even when the user closes his browser window.

Purpose cookies

These cookies collect information about user behavior and whether the user receives any error messages. In addition, these cookies are also used to measure the loading time and the behavior of the website with different browsers.

Target-oriented cookies

These cookies provide a better user experience. For example, entered locations, font sizes, or form data are saved.

Advertising cookies

These cookies are also called targeting cookies. They are used to deliver customized advertising to the user. This can be very convenient, but also very annoying.

Usually, when you visit a website for the first time, you are asked which of these cookie types you want to allow. And of course, this decision is also stored in a cookie.

If you want to know more about cookies and are not averse to technical documentation, we recommend <https://datatracker.ietf.org/doc/html/rfc6265>, the Request for Comments from the Internet Engineering Task Force (IETF) called "HTTP State Management Mechanism".

Purpose of processing via cookies

The purpose ultimately depends on the cookie in question. Further details are provided below or available by the manufacturer of the software that sets the cookie.

Which data are processed?

Cookies are little helpers for many different tasks. Unfortunately, it is not possible to generalize which data are stored in cookies, but this privacy policy provides information about processed or stored data.

Storage duration of cookies

The storage duration depends on the cookie in question and is specified further below. Some cookies are deleted after less than an hour, others remain stored on a computer for several years.

You can also influence the storage period yourself. You can manually delete all cookies at any time via your browser (see also "Right to object" below). Furthermore, cookies based on

consent are deleted at the latest after revocation of your consent, whereby the legality of the storage remains unaffected until then.

Right to object - how can I delete cookies?

You decide how and whether you want to use cookies. Regardless of the service or website from which the cookies come, you can always delete, disable or only partially allow cookies. For example, you can block third-party cookies but allow all other cookies.

To find out which cookies have been stored in your browser, or if you want to change or delete cookie settings, check your browser settings:

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

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

[Firefox: Delete cookies to remove data that websites have placed on your computer](#)

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

[Microsoft Edge: delete and manage cookies](#)

If you don't want to allow cookies, you can set your browser to notify you whenever a cookie is about to be set. This way, you can decide whether or not to allow each cookie. The procedure varies according to the browser. It is best to search for the instructions in Google using the search term "delete cookies Chrome" or "disable cookies Chrome" for a Chrome browser.

Legal basis

The so-called "Cookie Guidelines" have been in place since 2009. These state that the storage of cookies requires your **consent** (Article 6 (1) a GDPR). Within the EU countries, however, there are very different responses to these directives. In Austria, this directive was implemented in Section 96 (3) of the Telecommunications Act (TKG). In Germany, the Cookie Directives were not implemented as national law. Instead, the implementation of this directive took place largely in § 15 para.3 of the Telemedia Act (TMG).

For strictly necessary cookies, even in the absence of consent, there are legitimate interests (Article 6 para. 1 lit. f GDPR), which in most cases are of an economic nature. We want to provide visitors to the website with a pleasant user experience and for this purpose certain cookies are often absolutely necessary.

Insofar as cookies that are not strictly necessary are used, this is only done with your consent. The legal basis for this is Art. 6 para. 1 lit. a GDPR.

The following sections provide further details on the use of cookies, insofar as the software used uses cookies.

Web hosting summary

Web hosting summary

- 👤 Concerned parties: visitors of the website.
- 🤝 Purpose: professional hosting of the website and safeguarding operations.
- 💻 Processed data: IP address, time of website visit, browser used, and other data. Further details can be found below or with the web hosting provider used.
- 📅 Storage period: depends on the provider, but usually 2 weeks.
- ⚖️ Legal basis: Art. 6 para. 1 lit.f GDPR (Legitimate Interests).

What is web hosting?

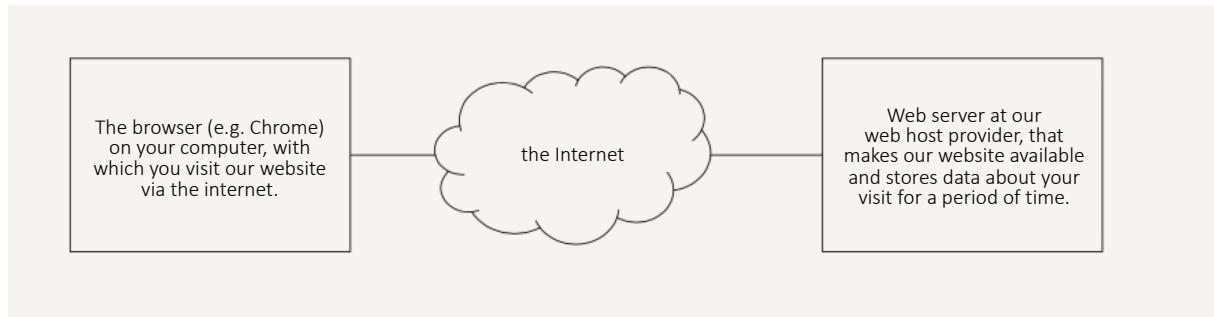
Nowadays, when you visit websites, certain information - including personal data - is automatically created and stored, including on this website. These data should be processed as sparingly as possible and only with justification. By website, we mean the entirety of all web pages on a domain, i.e. everything from the home page (homepage) to the very last subpage (like this one). By domain, we mean, for example, example.de or sampleexample.com.

When you want to view a website on a computer, tablet, or smartphone, you use a program called a web browser. You probably have heard of some web browsers: Google Chrome, Microsoft Edge, Mozilla Firefox, and Apple Safari. We call these browsers or web browsers.

To display the website, the browser needs to connect to another computer where the website's code is stored: the web server. Running a web server is a complicated and costly task, which is why this is usually done by professional providers. These offer web hosting and thus ensure reliable and error-free storage of website data.

When the browser on your computer (desktop, laptop, tablet or smartphone) connects, as well as during data transfer to and from the web server, personal data may be processed. While your computer stores data, the web server must also store data for a while to ensure proper operation.

The following figure illustrates the interaction between the browser, the internet, and the hosting provider.



Why do we process personal data?

The purposes of data processing are:

1. Professional hosting of the website and safeguarding operations,
2. Maintenance of operational and IT security,
3. Anonymous evaluation of access behavior to improve our offer and, if necessary, for law enforcement or prosecution of claims.

Which data are processed?

Even now while you are visiting our website, our web server, which is the computer on which this website is stored, usually automatically stores data such as

- the complete internet address (URL) of the website you are visiting
- browser and browser version (e.g. Chrome 87)
- operating system used (e.g. Windows 10)
- address (URL) of the previously visited page (referrer URL) (e.g. <https://www.beispielquellsite.de/vonabinichgekommen/>)
- host name and IP address of the device accessed (e.g. COMPUTERNAME and 194.23.43.121)
- date and time
- as files, the so-called web server log files

For how long are data stored?

As a rule, the above-mentioned data are stored for two weeks and then automatically deleted. We do not share these data, but we cannot exclude the possibility that they may be viewed by authorities in the event of unlawful behavior.

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

Legal basis

The lawfulness of the processing of personal data in the context of web hosting results from Art. 6 (1) lit. f GDPR (protection of legitimate interests), because the use of professional hosting is necessary to present Kat&Carmel OG on the internet in a secure and user-friendly manner and to be able to pursue attacks and claims if necessary.

A contract usually exists between us and the hosting provider on commissioned processing pursuant to Art. 28 f. GDPR, which ensures compliance with data protection and guarantees data security.

Cookie Consent Management Platform Introduction

Cookie Consent Management Platform Summary

👤 Data subjects: website visitors

🤝 Purpose: Obtaining and managing consent for certain cookies and thus the use of certain tools.

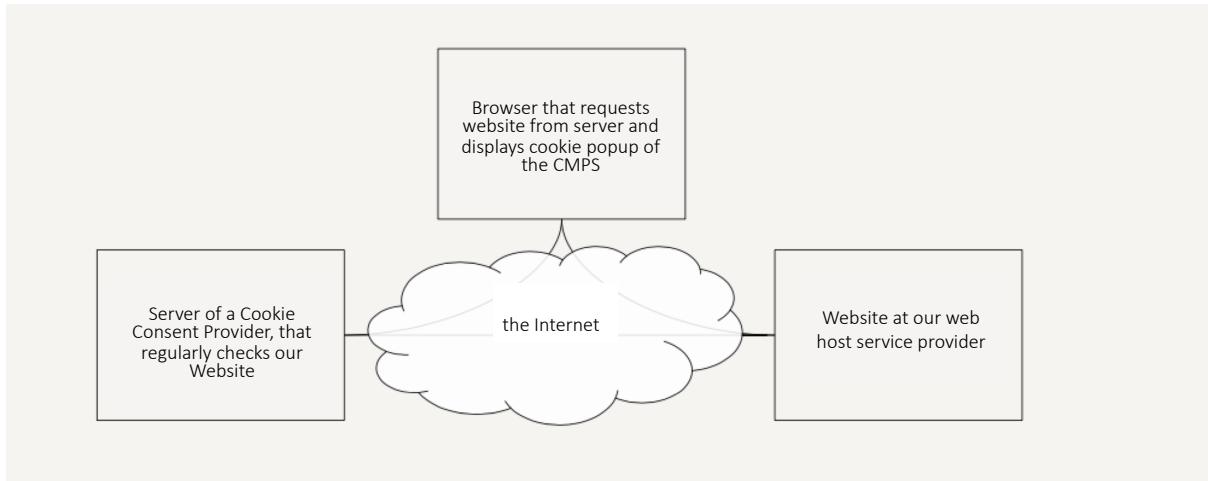
📅 Data processed: Data used to manage the cookie settings set, such as IP address, time of consent, type of consent, and individual consent. Further details can be found by examining the policies of the tool used.

📅 Storage period: Depending on tool used, up to several years.

⚖️ Legal basis: 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 Consent Management Platform (CMP) software on our website, which helps us and you to handle used scripts and cookies correctly and safely. The software automatically creates a cookie popup, scans and controls all scripts and cookies, provides cookie consent for you as required by data protection laws, and helps us and you keep track of all cookies. With most cookie consent management tools, all existing cookies are identified and categorized. You as a website visitor then decide which scripts and cookies to allow. The following figure illustrates the relationship between the browser, web server, and CMP.



Why do we use a cookie management tool?

Our goal is to make data protection as transparent as possible. We are also legally obligated to do so. We want you to know as much as possible about all tools and cookies that can store and process your data. You also have the right to decide which cookies to accept and which to reject. To offer you this right, we first need to know exactly which cookies ended up on our website in the first place. Thanks to a cookie management tool that regularly scans the website for all existing cookies, we know about all cookies and can provide you with GDPR-compliant information. You can then accept or reject cookies via the consent system.

Which data are processed?

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

Duration of data processing

The duration of data processing is described below, provided that such information is available to us. In general, we only process personal data for as long as is strictly necessary to provide our services and products. Data that are stored in cookies are stored for different periods of time. Some cookies are deleted as soon as you leave the website, while others may be stored in your browser for several years. The exact duration of data processing depends on the tool used; in most cases, data are stored for several years. Precise information on the duration of data processing is provided in the privacy policies of the individual tool providers.

Right to object

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

Information on specific cookie management tools, if available, is provided in the following sections.

Legal basis

If you consent to cookies, your personal data will be processed and stored via these cookies. If by your **consent** (Article 6 (1) lit. a GDPR), we are allowed to use cookies, this consent is also the legal basis for the use of cookies or the processing of your data. In order to be able to manage consent to cookies and to enable you to give your consent, cookie consent management platform software is used. The use of this software enables us to operate the website in an efficient manner in compliance with the law, which constitutes a legitimate interest (Article 6(1)(f) GDPR).

Explanation of terms used

Our privacy policy is intended to be as clear and understandable as possible. However, it is often necessary to use legal terms (such as personal data) or certain technical terms (such as cookies, IP address). To explain terms that we may not have sufficiently addressed in the previous sections, please find below an alphabetical list of important terms. Where these terms are taken from the GDPR, we also list the GDPR definitions, adding our own explanations where necessary.

Consent

Definition according to Article 4 of the GDPR

For the purposes of this regulation, the term:

“Consent” is defined as any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

As a rule, such consent is given on websites via a cookie consent tool. Whenever you visit a website for the first time, you are usually asked via a banner whether you agree or consent to the data processing. In most cases, you can also make individual settings and thus decide which data processing you allow and which you do not. If you do not consent, no personal data of yours may be processed. In principle, 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 this regulation, the term:

"Personal data" is information that relates to an identified or identifiable individual. ("data subject"); an identifiable individual 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

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

- Name
- Address
- E-mail address
- Postal address
- Phone number
- Date of birth
- Identification numbers such as social security number, tax identification number, identity card number, or matriculation number
- Bank data such as account number, credit information, account balances, and more.

According to the European Court of Justice (ECJ), your **IP address is also considered as personal data**. IT experts can use your IP address to determine at least the approximate location of your device and, subsequently, you as the connection owner. Therefore, the storage of an IP address also requires a legal basis as defined by the GDPR. There are also still so-called "**special categories**" of personal data that also require special protection. These include:

- racial and ethnic origin
- political opinions
- religious or ideological convictions
- trade union membership
- genetic data, such as data taken from blood or saliva samples
- biometric data (information regarding mental, physical, or behavioral characteristics that can identify an individual).
- health data
- data regarding sexual orientation or sexual life

Profiling

Definition according to Article 4 of the GDPR.

For the purposes of this regulation, the term:

"Profiling" means any form of automated processing of personal data which consists of using such personal data to evaluate certain personal aspects relating to an individual, in particular, to analyze or predict aspects relating to the individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or change of location;

Profiling involves gathering various pieces of information about an individual in order to learn more about them. On the web, profiling is often used for advertising purposes or even for credit checks. Web or advertising analysis programs, for example, collect data about your

behavior and interests on a website. This results in a specific user profile, which can be used to target advertising to a specific group.

All texts are protected by copyright.