

## Introduction and Overview

We have written this privacy statement (version 06.02.2022-111940724) in order to explain to you, in accordance with the requirements 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 (e.g. providers) commissioned by us - process, will process in the future and what lawful options you have. The terms used are to be understood as gender-neutral.

In short, we inform you comprehensively about data we process about you.

Privacy statements usually sound very technical and use legal terminology. This privacy statement, on the other hand, is intended to describe the most important things to you as simply and transparently as possible. To the extent that it is conducive to transparency, technical terms are explained in a reader-friendly manner, links to further information are provided and graphics are used. In this way, 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. This is certainly not possible by providing the most concise, unclear and legalistic explanations possible, as is often standard practice on the Internet when it comes to data protection. I hope you find the following explanations interesting and informative, and perhaps there is one or two pieces of information that you did not yet know.

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

## Scope of application

This data protection declaration applies to all personal data processed by us in the company and to all personal data processed by companies commissioned by us (order processors). By personal data, we mean information within the meaning of Art. 4 No. 1 DSGVO, such as a person's name, e-mail address and postal address. The processing of personal data ensures that we can offer and invoice our services and products, whether online or offline. The scope of this privacy policy includes:

- all online presences (websites, online stores) that we operate
- social media presences and email communications
- mobile apps for smartphones and other devices

In short, the data protection declaration applies to all areas in which personal data is processed in the company via the aforementioned channels in a structured manner. 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 statement, 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, which you can of course read online on EUR-Lex, the access to EU law, at <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679>.

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

Consent (Article 6(1)(a) DSGVO): You have given us your consent to process data for a specific purpose. An example would be the storage of your entered data of a contact form.

Contract (Article 6(1) lit. b) DSGVO): In order to fulfill a contract or pre-contractual obligations with you, we process your data. For example, if we conclude a purchase contract with you, we need personal information in advance.

Legal obligation (Article 6(1)(c) DSGVO): 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.

Legitimate interests (Article 6(1)(f) DSGVO): In the 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.

Other conditions, such as the performance of recordings in the public interest and the exercise of official authority, as well as the protection of vital interests, do not generally arise for us. If such a legal basis should nevertheless be relevant, it will be indicated at 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), or DSG for short.
- In Germany, the Federal Data Protection Act, or BDSG for short, applies.
- If other regional or national laws apply, we will inform you about them in the following sections.

#### Storage period

It is our general policy 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 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.

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

#### Rights according to the General Data Protection Regulation

According to Article 13 of the GDPR, you have the following rights to ensure fair and transparent processing of data:

According to Article 15 DSGVO, you have the right to be informed 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 19 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).

In short, you have rights - do not hesitate to contact the controller 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

Head: Mag. Dr. Andrea Jelinek

Address: Barichgasse 40-42, 1030 Vienna

Telephone number: +43 1 52 152-0

E-mail address: [dsb@dsb.gv.at](mailto:dsb@dsb.gv.at)

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

### Security of data processing

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, within the scope of our possibilities, for third parties to infer personal information from our data.

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

### 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 over the internet in a tap-proof way.

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

Thus, we have implemented an additional layer of security and fulfill data protection by design of technology Article 25(1) DSGVO). By using TLS (Transport Layer Security), an encryption protocol for secure data transmission on the Internet, we can ensure the protection of confidential data.

You can recognize the use of this protection of data transmission by the small lock symbol at the top left of the browser, to the left of the Internet address (e.g., beispieleseite.de) and the use of the scheme https (instead of http) as part of our Internet address.

If you want to know more about encryption, we recommend a Google search for "Hypertext Transfer Protocol Secure wiki" to get good links to further information.

## Communication

### Communication summary



Affected parties: anyone who communicates with us by phone, email, or online form.



Data processed: e.g. telephone number, name, e-mail address, form data entered. You can find more details on this in the respective contact type used.



Purpose: Handling of communication with customers, business partners, etc.



Storage period: Duration of the business case and legal requirements.



Legal basis: Art. 6 para. 1 lit. a DSGVO (consent), Art. 6 para. 1 lit. b DSGVO (contract), Art. 6 para. 1 lit. f DSGVO (legitimate interests).

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

The data is processed for the handling and processing of your question and the related business transaction. The data will be stored for the same period of time or as long as required by law.

### Persons concerned

All those who seek contact with us via the communication channels provided by us are affected by the aforementioned processes.

### Telephone

When you call us, the call data is stored pseudonymously on the respective 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 respective end device (computer, laptop, smartphone,...) and data is 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 is stored on our web server and may be forwarded to an e-mail address of ours. The data will be 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 legal bases:

Art. 6 para. 1 lit. a DSGVO (consent): you give us your consent to store your data and to further use it for purposes related to the business case;

Art. 6 (1) lit. b DSGVO (contract): there is a need for the performance of a contract with you or a processor such as the telephone provider or we need to process the data for pre-contractual activities, such as the preparation of an offer;

Art. 6 para. 1 lit. f DSGVO (Legitimate Interests): we want to operate customer inquiries and business communication in a professional framework. 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 the communication efficiently.

## Cookies

### Cookies Summary



Data subjects: Visitors to the website.



Purpose: depending on the respective cookie. More details can be found below or from the manufacturer of the software that sets the cookie.



Data processed: Depending on the cookie used in each case. More details can be found below or from the manufacturer of the software that sets the cookie.



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



Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit.f DSGVO (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 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.

One thing can't be denied: Cookies are really useful little helpers. Almost all websites use cookies. More precisely, they are HTTP cookies, as there are other cookies 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 about you, 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 used to. In some browsers each cookie has its own file, in others, such as Firefox, all cookies are stored in a single file.

The following graphic 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 once another page is requested.

HTTP cookie interaction between browser and web server

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 varies 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`

Wert: `GA1.2.1326744211.152111940724-9`

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 question of which cookies we use in particular depends on the services we use and is clarified in the following sections of the privacy policy. At this point, we would like to briefly discuss the different types of HTTP cookies.

We can distinguish 4 types of cookies:

Essential cookies.

These cookies are necessary to ensure 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 if 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 stored.

### 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 afraid of technical documentation, we recommend <https://datatracker.ietf.org/doc/html/rfc6265>, the Internet Engineering Task Force (IETF) Request for Comments called "HTTP State Management Mechanism".

### Purpose of processing via cookies

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

### What data is processed?

Cookies are little helpers for a lot of different tasks. Unfortunately, it is not possible to generalize what data is stored in cookies, but we will inform you about the processed or stored data in the following privacy policy.

### Storage duration of cookies

The storage duration depends on the respective cookie and is specified further below. Some cookies are deleted after less than an hour, others can 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 that are based on consent will be deleted at the latest after revocation of your consent, whereby the legality of the storage remains unaffected until then.

### Right of objection - how can I delete cookies?



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

If you want to find out which cookies have been stored in your browser, if you want to change or delete cookie settings, you can find it in 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 generally don't want cookies, you can set your browser to notify you whenever a cookie is about to be set. This way, you can decide for each cookie whether to allow it or not. The procedure varies depending on the browser. It is best to search for the instructions in Google using the search term "delete cookies Chrome" or "disable cookies Chrome" in the case of a Chrome browser.

#### Legal basis

Since 2009, there are the so-called "Cookie Guidelines". This states that saving cookies requires your consent (Article 6 (1) a DSGVO). Within the EU countries, however, there are still very different reactions to these directives. In Austria, however, 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 absolutely necessary cookies, even if there is no consent. there are legitimate interests (Article 6 para. 1 lit. f DSGVO), 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 absolutely necessary are used, this is only done in the case of your consent. The legal basis in this respect is Art. 6 para. 1 lit. a DSGVO.


In the following sections, you will be informed in more detail about the use of cookies, insofar as software used uses cookies.


Web hosting introduction

Web hosting summary

 Data subject: Visitors to the website.

 Purpose: professional hosting of the website and safeguarding its operation.

 Processed data: IP address, time of website visit, browser used and other data. More details can be found below or with the respective web hosting provider used.

 Storage period: depending on the respective provider, but usually 2 weeks.

 Legal basis: Art. 6 para. 1 lit.f DSGVO (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. This data should be processed as sparingly as possible and only with justification. By website, by the way, 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.

If you want to view a website on a screen, you use a program called a web browser to do it. You probably know some web browsers by name: Google Chrome, Microsoft Edge, Mozilla Firefox, and Apple Safari.

This web 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, the providers. These offer web hosting and thus ensure reliable and error-free storage of website data.

When the browser on your computer (desktop, laptop, smartphone) connects and during data transfer to and from the web server, personal data may be processed. On the one hand, your computer stores data, and on the other hand, the web server also needs to store data for a while to ensure proper operation.

To illustrate:

Browser and web server

Why do we process personal data?

The purposes of data processing are:

Professional hosting of the website and securing its operation.

To maintain operational and IT security

Anonymous evaluation of access behavior to improve our offer and, if necessary, to prosecute or pursue claims

What data is processed?

Even while you are visiting our website right now, 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)

the operating system used (e.g. Windows 10)

the address (URL) of the previously visited page (referrer URL) (e.g. <https://www.beispielquellseite.de/vondabinichgekommen.html/>)

the host name and IP address of the device being accessed (e.g. COMPUTERNAME and 194.23.43.121)

date and time

in files, the so-called web server log files

How long is data stored?

As a rule, the above data is stored for two weeks and then automatically deleted. We do not pass on this data, but we cannot rule out the possibility that this data may be viewed by the authorities in the event of unlawful conduct.

In short, your visit is logged by our provider (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 DSGVO (protection of legitimate interests), because the use of professional hosting with a provider is necessary to present the company on the Internet in a secure and user-friendly manner and to be able to pursue attacks and claims from this if necessary.


Between us and the hosting provider there is usually a contract on commissioned processing pursuant to Art. 28 f. DSGVO, which ensures compliance with data protection and guarantees data security.

## Website Building Block Systems Introduction

### Website Building Block Systems Privacy Policy Summary

 Data subjects: Visitors to the website

 Purpose: Optimization of our service performance.

 Processed data: Data such as technical usage information like browser activity, clickstream activity, session heatmaps, as well as contact details, IP address or your geographical location. More details can be found below in this privacy policy and in the privacy policy of the providers.

 Storage duration: depends on the provider.

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

## What are Website Building Block Systems?

We use a website building block system for our website. Modular systems are special forms of a content management system (CMS). With a building block system, website owners can create a website very easily and without programming knowledge. In many cases, web hosts also offer building block systems. By using a modular system, personal data of you may also be collected, stored and processed. In this data protection text, we provide you with general information about data processing by modular systems. You can find more detailed information in the provider's data protection statements.

## Why do we use website building block systems for our website?

The biggest advantage of a modular system is its ease of use. We want to provide you with a clear, simple and concise website that we can easily operate and maintain ourselves - without external support. A modular system now offers many helpful functions that we can use even without programming knowledge. This allows us to design our web presence according to our wishes and to offer you an informative and pleasant time on our website.

## What data is stored by a modular system?

Exactly what data is stored depends, of course, on the website construction kit system used. Each provider processes and collects different data of the website visitor. However, technical usage information such as operating system, browser, screen resolution, language and keyboard settings, hosting provider and the date of your website visit are usually collected. Furthermore, tracking data (e.g. browser activity, clickstream activity, session heatmaps, etc.) may also be processed. In addition, personal data may also be collected and stored. This is mostly contact data such as e-mail

address, telephone number (if you have provided it), IP address and geographical location data. You can find out exactly what data is stored in the provider's privacy policy.

How long and where is the data stored?

We will inform you about the duration of data processing below in connection with the website construction kit system used, provided we have further information on this. You can find detailed information about this in the provider's privacy policy. In general, we only process personal data for as long as is absolutely necessary for the provision of our services and products. It may be that the provider stores data from you according to its own specifications, over which we have no control.

Right of objection

You always have the right to information, correction and deletion of your personal data. If you have any questions, you can also contact the person responsible for the website construction system used at any time. Contact details can be found either in our privacy policy or on the website of the relevant provider.

You can delete, deactivate or manage cookies that providers use for their functions in your browser. Depending on which browser you use, this works in different ways. Please note, however, that all functions may then no longer work as usual.

Legal basis

We have a legitimate interest in using a website construction kit to optimize our online service and present it efficiently and in a user-friendly manner for you. The corresponding legal basis for this is Art. 6 para. 1 lit. f DSGVO (Legitimate Interests). Nevertheless, we only use the construction kit insofar as you have given your consent.

Insofar as the processing of data is not absolutely necessary for the operation of the website, the data will only be processed on the basis of your consent. This applies in particular to tracking activities. The legal basis in this respect is Art. 6 para. 1 lit. a DSGVO.

With this privacy policy, we have brought you closer to the most important general information around data processing. If you would like more detailed information in this regard, you will find further information - if available - in the following section or in the provider's privacy policy.

WordPress.com Privacy Policy

We use WordPress.com, a website building system, for our website. The service provider is the American company Automattic Inc, 60 29th Street #343, San Francisco, CA 94110, USA.

WordPress also processes data from you in the USA, among other places. We would like to point out that according to the opinion of the European Court of Justice, there is currently no adequate level of protection for the transfer of data to the USA. This may be associated with various risks for the legality and security of data processing.

As a basis for data processing with recipients located in third countries (outside the European Union, Iceland, Liechtenstein, Norway, so in particular in the USA) or a data transfer there, WordPress uses so-called standard contractual clauses (= Art. 46. para. 2 and 3 DSGVO). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through these clauses, WordPress undertakes to comply with the European level of data protection when processing your relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the decision and the corresponding standard contractual clauses here, among other places: [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?locale=de](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de)


The Data Processing Agreements, which correspond to the standard contractual clauses, can be found at <https://wordpress.com/support/data-processing-agreements/>.


To learn more about the data processed through the use of WordPress.com, please see the Privacy Policy at <https://automattic.com/de/privacy/>.

## Facebook Privacy Policy

### Facebook Privacy Policy Summary


 Data subjects: Visitors to the website.

 Purpose: Optimization of our service performance.

 Processed data: Data such as customer data, user behavior data, information about your device and your IP address.

More details can be found below in the privacy policy.

 Storage period: until the data is no longer useful for Facebook's purposes.

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

### What are Facebook tools?

We use selected tools from Facebook 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 help of these tools we can offer you and people who are interested in our products and services the best possible offer.

If data is collected from you and forwarded via our embedded Facebook elements or via our Facebook page (Fanpage), both we and Facebook Ireland Ltd. are responsible for this. Facebook is solely responsible for the further processing of this data. Our joint obligations have also been set out in a publicly available agreement at [https://www.facebook.com/legal/controller\\_addendum](https://www.facebook.com/legal/controller_addendum). This states, for example, that we must clearly inform you about the use of Facebook tools on our site. Furthermore, we are also responsible for ensuring that the tools are securely integrated into our website in accordance with data protection law. Facebook, on the other hand, is responsible for the data security of Facebook products, for example. If you have any questions about data collection and data processing by Facebook, you can contact the company directly. If you direct the question to us, we are obliged to forward it to Facebook.

Below we provide an overview of the various Facebook tools, what data is sent to Facebook and how you can delete this data.

Among many other products, Facebook also offers the so-called "Facebook Business Tools". This is the official name of Facebook. However, since the term is hardly known, we have decided to simply call them Facebook Tools. Among them are:

Facebook Pixel

Social plug-ins (such as the "Like" or "Share" button).

Facebook Login

account kit

APIs (programming interface)

SDKs (collection of programming tools)

Platform integrations

Plugins

Codes

Specifications

Documentations

Technologies and services

Through these tools, Facebook extends services and has the ability to obtain information about user activity outside of Facebook.

We only want to show our services and products to people who are really interested in them. With the help of advertisements (Facebook ads), we can reach precisely these people. However, in order to show users suitable ads, Facebook needs information about people's wishes and needs. Thus, information about user behavior (and contact data) on our website is made available to the company. As a result, Facebook collects better user data and can show interested people the

appropriate advertising about our products or services. The tools thus enable customized advertising campaigns on Facebook.

Data about your behavior on our website is called "event data" by Facebook. This is also used for measurement and analysis services. Facebook can thus create "campaign reports" on our behalf about the impact of our advertising campaigns. Furthermore, analytics give us better insight into how you use our services, website or products. As a result, we use some of these tools to optimize your user experience on our website. For example, social plug-ins allow you to share content on our site directly on Facebook.

What data is stored by Facebook tools?

By using individual Facebook tools, personal data (customer data) may be sent to Facebook. Depending on the tools used, customer data such as name, address, phone number and IP address may be sent.

Facebook uses this information to match the data with the data it itself has from you (if you are a Facebook member). Before customer data is sent to Facebook, a process called "hashing" takes place. This means that a data record of any size is transformed into a character string. This also serves to encrypt data.

In addition to contact data, "event data" is also transmitted. Event data" refers to the information that we receive about you on our website. For example, which subpages you visit or which products you buy from us. Facebook does not share the information it receives with third parties (such as advertisers) unless it has explicit permission or is legally required to do so. "Event data" may also be associated with contact information. This allows Facebook to offer better personalized advertising. After the matching process already mentioned, Facebook deletes the contact data again.

In order to be able to deliver ads in an optimized way, Facebook only uses event data if it has been combined with other data (collected by Facebook in other ways). Facebook also uses this event data for security, protection, development, and research purposes. Much of this data is transferred to Facebook via cookies. Cookies are small text files used to store data or information in browsers. Depending on the tools you use and whether you are a Facebook member, different numbers of cookies are created in your browser. We go into more detail about individual Facebook cookies in the descriptions of each Facebook tool. You can also find general information about the use of Facebook cookies at <https://www.facebook.com/policies/cookies>.

How long and where is the data stored?

Basically, Facebook stores data until it is no longer needed for its own services and Facebook products. Facebook has servers spread all over the world where its data is stored. However, customer data is deleted within 48 hours after it has been matched with its own user data.



How can I delete my data or prevent data storage?

In accordance with the Basic Data Protection Regulation, you have the right to information, correction, transferability and deletion of your data.

A complete deletion of the data only occurs if you delete your Facebook account completely. And this is how deleting your Facebook account works:

- 1) On the right side of Facebook, click Settings.
- 2) Then click on "Your Facebook information" in the left column.
- 3) Now click "Deactivation and deletion".
- 4) Now select "Delete account" and then click "Continue and delete account".
- 5) Now enter your password, click "Next" and then click "Delete account".

The storage of data that Facebook receives via our site takes place, among other things, via cookies (e.g. for social plugins). In your browser, you can deactivate, delete or manage individual or all cookies. Depending on which browser you use, this works in different ways. Under the section "Cookies" you will find the corresponding links to the respective instructions of the most popular browsers.

If you generally do not want cookies, you can set up your browser so that it always informs you when a cookie is to be set. In this way, you can decide for each individual cookie whether you allow it or not.

#### Legal basis

If you have consented that data from you can be processed and stored by integrated Facebook tools, this consent is considered the legal basis for data processing (Art. 6 (1) lit. a DSGVO). In principle, your data will also be stored and processed on the basis of our legitimate interest (Art. 6 para. 1 lit. f DSGVO) in fast and good communication with you or other customers and business partners. Nevertheless, we only use the tools insofar as you have given your consent. Most social media platforms also set cookies in your browser to store data. That is why we recommend that you read our privacy text about cookies carefully and view Facebook's privacy policy or cookie policy.

Facebook also processes data from you in the USA, among other places. We would like to point out that according to the opinion of the European Court of Justice, there is currently no adequate level of protection for the transfer of data to the USA. This may be associated with various risks to the legality and security of data processing.

As a basis for data processing with recipients located in third countries (outside the European Union, Iceland, Liechtenstein, Norway, i.e. in particular in the USA) or a data transfer there, Facebook uses so-called standard contractual clauses (= Art. 46. para. 2 and 3 DSGVO). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through these clauses, Facebook undertakes to comply with the European level of data protection when processing your relevant data, even if the data is stored, processed and managed in the US. These clauses are based on an implementing decision of the EU Commission. You can find the decision and the corresponding standard contractual clauses here, among other places: [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?locale=de](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de)

Facebook's data processing terms and conditions, which correspond to the standard contractual clauses, can be found at <https://www.facebook.com/legal/terms/dataprocessing>.

We hope we have brought you closer to the most important information about the use and data processing by Facebook tools. If you want to learn more about how Facebook uses your data, we recommend that you read the data policy at <https://www.facebook.com/about/privacy/update>.

#### Facebook Login Privacy Policy

We have integrated the convenient Facebook Login on our site. This allows you to easily log in to our site using your Facebook account without having to create another user account. If you decide to make your registration via the Facebook Login, you will be redirected to the social media network Facebook. There, the registration takes place via your Facebook user data. Through this login process, data about you or your user behavior is stored and transmitted to Facebook.

To store the data, Facebook uses various cookies. In the following, we show you the most important cookies that are set in your browser or already exist when you log in to our site via the Facebook login:

Name: fr

Value: 0jiejh4c2GnlufEJ9..Bde09j...1.0.Bde09j

Purpose: This cookie is used to make the social plugin on our website work in the best possible way.

Expiration date: after 3 months

Name: datr

Wert: 4Jh7XUA2111940724SEmPsSfzCOO4JFFI

Purpose: Facebook sets the "datr" cookie when a web browser accesses facebook.com, and the cookie helps identify login activity and protect users.

Expiration date: after 2 years

Name: \_js\_datr

Value: deleted

Purpose: This session cookie sets Facebook for tracking purposes, even if you don't have a Facebook account or are logged out.

Expiration date: after session end

Note: The cookies listed are only a small selection of the cookies available to Facebook. Other cookies include \_fbp, sb or wd. A complete enumeration is not possible, as Facebook has a large number of cookies and uses them variably.

On the one hand, the Facebook login offers you a quick and easy registration process, and on the other hand, it gives us the opportunity to share data with Facebook. This allows us to better tailor our offer and promotions to your interests and needs. Data that we receive from Facebook in this way is public data such as

Your Facebook name

your profile picture

a stored e-mail address

friend lists

button information (e.g. "Like" button)

birthday date

language

Place of residence

In return, we provide Facebook with information about your activities on our website. This includes information about the device you are using, which of our sub-pages you visit or which products you have purchased from us.

By using Facebook Login, you consent to the data processing. You can revoke this agreement at any time. If you want to learn more information about data processing by Facebook, we recommend the Facebook privacy policy at <https://www.facebook.com/policy.php?tid=111940724>.

Provided you are logged in to Facebook, you can change your settings for advertisements yourself at [https://www.facebook.com/adpreferences/advertisers/?entry\\_product=ad\\_settings\\_screen](https://www.facebook.com/adpreferences/advertisers/?entry_product=ad_settings_screen).

#### Facebook social plug-ins privacy policy

So-called social plug-ins of the company Facebook Inc. are installed on our website. You can recognize these buttons by the classic Facebook logo, such as the "Like" button (the hand with raised thumb) or by a clear "Facebook Plug-in" label. A social plug-in is a small part of Facebook that is integrated into our site. Each plug-in has its own function. The most commonly used functions are the well-known "Like" and "Share" buttons.

The following social plug-ins are offered by Facebook:

"Save" button

"Like" button, share, send and quote.

Page plug-in

Comments

Messenger plug-in

Embedded posts and video player

Group plug-in

Visit <https://developers.facebook.com/docs/plugins> for more information on how each plug-in is used. We use the social plug-ins on the one hand to provide you with a better user experience on our site, and on the other hand because Facebook can optimize our advertisements through them.

If you have a Facebook account or have visited <https://www.facebook.com/> before, Facebook has already set 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 site or interact with social plug-ins (e.g. the "Like" button).

The information received is deleted again or anonymized within 90 days. According to Facebook, this data includes your IP address, which website you visited, the date, the time and other information concerning your browser.

To prevent Facebook from collecting a lot of data during your visit to our website and connecting it with Facebook data, you must log out of Facebook during your website visit (log out).

If you are not logged into Facebook or do not have a Facebook account, your browser will send less information to Facebook because you have fewer Facebook cookies. Nevertheless, data such as your

IP address or which website you visit may be transmitted to Facebook. We would still like to explicitly point out that we do not know exactly about the exact content of the data. However, we try to inform you as best as possible about the data processing according to our current state of knowledge. You can also read how Facebook uses the data in the company's data policy at <https://www.facebook.com/about/privacy/update>.

The following cookies are set in your browser at a minimum when you visit a website with social plug-ins from Facebook:

Name: dpr

Value: not specified

Purpose: This cookie is used to make the social plug-ins on our website work.

Expiration date: after end of session

Name: fr

Wert: 0jeyh4111940724c2GnlufEJ9..Bde09j...1.0.Bde09j

Purpose: The cookie is also necessary for the plug-ins to work properly.

Expiration date:: after 3 months

Note: These cookies were set after a test, even if you are not a Facebook member.

If you are logged in to Facebook, you can change your settings for advertisements yourself at <https://www.facebook.com/adpreferences/advertisers/>. If you are not a Facebook user, you can basically manage your usage-based online advertising on <https://www.youronlinechoices.com/de/prafferenzmanagement/?tid=111940724>. There you have the option to deactivate or activate providers.

If you want to learn more about Facebook's privacy policy, we recommend that you read the company's own data policy at <https://www.facebook.com/policy.php?tip=111940724>.

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 set cookie settings such as IP address, time of consent, type of consent, individual consents. More details can be found at the respective tool used.

 Storage period: Depends on the tool used, you have to be prepared for periods of several years.

 Legal basis: Art. 6 para. 1 lit. a DSGVO (consent), Art. 6 para. 1 lit.f DSGVO (legitimate interests).

What is a cookie consent management platform?

We use a Consent Management Platform (CMP) software on our website, which makes it easier for us and you to correctly and securely handle scripts and cookies used. 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 for yourself whether and which scripts and cookies you allow or disallow. The following graphic illustrates the relationship between browser, web server and CMP.

## Consent Management Platform Overview

Why do we use a cookie management tool?

Our goal is to provide you with the best possible transparency in the area of data protection. In addition, we are also legally obligated to do so. We want to educate you as much as possible about all tools and all cookies that can store and process data from you. It is also your right to decide for yourself which cookies you accept and which you do not. In order to give 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 DSGVO-compliant information about them. You can then accept or reject cookies via the consent system.

What data is processed?

Within the framework of our cookie management tool, you can manage each 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 query you each time you visit our website again 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. Depending on the provider of the cookie management tool, the storage period of your cookie consent varies. In most cases, this data (such as pseudonymous user ID, time of consent, details of cookie categories or tools, browser, device information) is stored for up to two years.

Duration of data processing

We will inform you about the duration of data processing below, provided we have further information on this. In general, we process personal data only as long as it is strictly necessary for the provision of our services and products. Data that is stored in cookies is stored for different lengths of time. Some cookies are already deleted after you leave the website, others may be stored in your browser for several years. The exact duration of data processing depends on the tool used; in most

cases, you should be prepared for a storage period of several years. In the respective privacy statements of the individual providers, you will usually receive precise information about the duration of data processing.

## Right of objection

You also have the right and the possibility 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 through cookies by managing, disabling or deleting cookies in your browser.

Information on specific cookie management tools, if available, can be found in the following sections.


## Legal basis


If you consent to cookies, personal data about you will be processed and stored via these cookies. If we are allowed to use cookies through your consent (Article 6 (1) (a) DSGVO), 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 the 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 efficiently operate the website in a legally compliant manner, which constitutes a legitimate interest (Article 6 (1) (f) DSGVO).

## Miscellaneous Introduction


### Miscellaneous Privacy Policy Summary

 Data subjects: Visitors to the website

 Purpose: Improving the user experience.

 Data processed: Which data is processed depends largely on the services used. Mostly it is IP address and/or technical data. You can find more details about this in the respective tools used.

 Storage duration: depends on the tools used.

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

## What falls under "Other"?

The category "Other" includes those services that do not fit into one of the above categories. These are usually various plugins and embedded elements that enhance our website. As a rule, these functions are obtained from third-party providers and integrated into our website. For example, these are web search services such as Algolia Place, Giphy, Programmable Search Engine, or online services for weather data such as OpenWeather.

## Why do we use other third-party providers?

We want our website to provide you with the best web experience in our industry. For a long time, a website has been more than just a business card for companies. It is a place to help you find what you are looking for. To always make our website more interesting and helpful for you, we use various third-party services.

#### What data is processed?

Whenever elements are integrated into our website, your IP address is transmitted to the respective provider, stored and processed there. This is necessary because otherwise the content will not be sent to your browser and consequently will not be displayed accordingly. It may also happen that service providers also use pixel tags or web beacons. These are small graphics on websites that can record a log file and also create analyses of this file. With the information obtained, providers can improve their own marketing efforts. In addition to pixel tags, such information (such as which button you click or when you visit which page) can also be stored in cookies. In addition to analysis data about your web behavior, technical information such as your browser type or operating system can also be stored in them. Some providers may also link the data obtained with other internal services or with third-party providers. Each provider handles your data differently. Therefore, we recommend that you carefully read the privacy statements of the respective services. As a matter of principle, we endeavor to use only services that handle the issue of data protection very carefully.

#### Duration of data processing

We will inform you about the duration of data processing below, provided we have further information on this. In general, we only process personal data for as long as is absolutely necessary for the provision of our services and products.

#### Legal basis

If we ask for your consent and you also consent that we may use the service, this is considered the legal basis for the processing of your data (Art. 6 para. 1 lit. a DSGVO). In addition to the consent, there is a legitimate interest on our part to analyze the behavior of website visitors and thus to improve our offer technically and economically. The legal basis for this is Art. 6 para. 1 lit. f DSGVO (Legitimate Interests). Nevertheless, we only use the tools if you have given your consent.

Information on the specific tools, you will receive - if available - in the following sections.

#### Google Fonts Privacy Policy

##### Google Fonts Privacy Policy Summary



Data subjects: Visitors to the website.




Purpose: Optimization of our service performance.




Processed data: Data such as IP address and CSS and font requests.

More details can be found below in this privacy policy.



 Storage period: Font files are stored by Google for one year.

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

What are Google Fonts?

On our website, we use Google Fonts. These are the "Google Fonts" of the company Google Inc. For the European area, the company Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services.

For the use of Google Fonts you do not have to log in or provide a password. Furthermore, no cookies are stored in your browser. The files (CSS, fonts) are requested via the Google domains fonts.googleapis.com and fonts.gstatic.com. According to Google, the requests for CSS and fonts are completely separate from all other Google services. If you have a Google account, you do not need to worry that your Google account information, while using Google Fonts, will be transmitted to Google. Google records the usage of CSS (Cascading Style Sheets) and the fonts used and stores this data securely. We'll look at exactly what the data storage looks like in more detail.

Google Fonts (formerly Google Web Fonts) is a directory of over 800 fonts that Google makes available to their users for free.

Many of these fonts are released under the SIL Open Font License, while others are released under the Apache License. Both are free software licenses.

Why do we use Google Fonts on our website?

Google Fonts allows us to use fonts on our own website, and not have to upload them to our own server. Google Fonts is an important component to keep the quality of our website high. All Google Fonts are automatically optimized for the web and this saves data volume and is a big advantage especially for mobile use. When you visit our site, the low file size ensures a fast loading time. Furthermore, Google Fonts are secure web fonts. Different image synthesis systems (rendering) in different browsers, operating systems and mobile devices can lead to errors. Such errors can sometimes visually distort texts or entire web pages. Thanks to the fast Content Delivery Network (CDN), there are no cross-platform problems with Google Fonts. Google Fonts supports all major browsers (Google Chrome, Mozilla Firefox, Apple Safari, Opera) and works reliably on most modern mobile operating systems, including Android 2.2+ and iOS 4.2+ (iPhone, iPad, iPod). So, we use Google Fonts so that we can display our entire online service as beautifully and consistently as possible.

What data is stored by Google?

When you visit our website, the fonts are reloaded via a Google server. Through this external call, data is transmitted to the Google servers. In this way, Google also recognizes that you or your IP address is visiting our website. The Google Fonts API is designed to reduce the use, storage, and collection of end-user data to what is necessary for proper font delivery. API, by the way, stands for

"Application Programming Interface" and is used, among other things, as a data transmitter in software.

Google Fonts stores CSS and font requests securely at Google and is thus protected. Through the collected usage figures, Google can determine how well the individual fonts are received. Google publishes the results on internal analysis pages, such as Google Analytics. In addition, Google also uses data from its own web crawler to determine which websites are using Google fonts. This data is published to the Google Fonts BigQuery database. Entrepreneurs and developers use Google's BigQuery web service to be able to examine and move large amounts of data.

However, it is still important to remember that each Google Font request also automatically transmits information such as language settings, IP address, browser version, browser screen resolution, and browser name to Google's servers. Whether this data is also stored cannot be clearly determined or is not clearly communicated by Google.

How long and where is the data stored?

Google stores requests for CSS assets for one day on its servers, which are mainly located outside the EU. This allows us to use fonts with the help of a Google stylesheet. A stylesheet is a format template that can be used to easily and quickly change the design or font of a website, for example.

The font files are stored by Google for one year. Google thus pursues the goal of fundamentally improving the loading time of web pages. If millions of web pages refer to the same fonts, they are cached after the first visit and immediately reappear on all other web pages visited later. Sometimes Google updates font files to reduce file size, increase language coverage, and improve design.

How can I delete my data or prevent data storage?

Those data that Google stores for a day or a year cannot be easily deleted. The data is automatically transmitted to Google when the page is called up. To delete this data prematurely, you need to contact Google support at <https://support.google.com/?hl=de&tid=111940724>. Data storage you prevent in this case only if you do not visit our site.

Unlike other web fonts, Google allows us unlimited access to all fonts. So we can access an unlimited sea of fonts and get the most out of them for our website. You can find out more about Google Fonts and other issues at <https://developers.google.com/fonts/faq?tid=111940724>. Google does address privacy-related issues there, but it doesn't really include detailed information about data storage. It is relatively difficult to get really precise information from Google about stored data.

Legal basis

If you have consented to Google Fonts being used, the legal basis of the corresponding data processing is this consent. According to Art. 6 (1) lit. a DSGVO (consent), this consent constitutes the legal basis for the processing of personal data, as may occur in the case of collection by Google Fonts.

From our side, there is also a legitimate interest in using Google Font to optimize our online service. The corresponding legal basis for this is Art. 6 para. 1 lit. f DSGVO (Legitimate Interests). Nevertheless, we only use Google Font if you have given your consent.

Google also processes data from you in the USA, among other places. We would like to point out that according to the opinion of the European Court of Justice, there is currently no adequate level of protection for the transfer of data to the USA. This may be associated with various risks to the legality and security of data processing.

As a basis for data processing at recipients located in third countries (outside the European Union, Iceland, Liechtenstein, Norway, i.e. in particular in the USA) or a data transfer there, Google uses so-called standard contractual clauses (= Art. 46. para. 2 and 3 DSGVO). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through these clauses, Google undertakes to comply with the European level of data protection when processing your relevant data, even if the data is stored, processed and managed in the US. These clauses are based on an implementing decision of the EU Commission. You can find the decision and the corresponding standard contractual clauses here, among other places: [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?locale=de](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de)


The Google Ads Data Processing Terms, which also correspond to the standard contractual clauses for Google Fonts, can be found at <https://business.safety.google/adsprocessor/terms/>.


You can also read about which data is generally collected by Google and what this data is used for at <https://www.google.com/intl/de/policies/privacy/>.

## Google Maps Privacy Policy

### Google Maps Privacy Policy Summary


 Data subjects: Visitors to the website

 Purpose: Optimization of our service performance.

 Processed data: Data such as search terms entered, your IP address and also latitude or longitude coordinates.

You can find more details about this further down in this privacy policy.

 Storage duration: depending on the stored data.

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

What is Google Maps?

We use Google Maps from Google Inc. on our website. Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services in Europe. Google Maps allows us to better show you locations and thus adapt our service to your needs. By using Google Maps, data is transmitted to Google and stored on Google servers. Here we will now go into more detail about 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 map service provided by the company Google. With Google Maps, you can search for exact locations of cities, sights, accommodations or businesses online via a PC, tablet or app. If companies are represented on Google My Business, other information about the company is displayed in addition to the location. To show how to get there, map sections of a location can be embedded in a website using HTML code. Google Maps shows the earth's surface as a street map or as an aerial or satellite image. Thanks to the Street View images and the high-quality satellite images, very accurate representations are possible.

Why do we use Google Maps on our website?

All our efforts on this site are aimed at providing you with a useful and meaningful time on our website. By integrating Google Maps we can provide you with the most important information about various locations. You can see at a glance where we are located. The directions always show you the best or fastest way to us. You can get the directions for routes by car, by public transport, on foot or by bike. For us, the provision of Google Maps is part of our customer service.

What data is stored by Google Maps?

In order for Google Maps to fully provide their service, the company must record and store data from you. This includes, among other things, the search terms entered, your IP address and also the latitude or longitude coordinates. If you use the route planner function, the start address entered is also stored. However, this data storage happens on the websites of Google Maps. We can only inform you about this, but have no influence. Since we have integrated Google Maps into our website, Google sets at least one cookie (name: NID) in your browser. This cookie stores data about your user behavior. Google uses this data primarily to optimize its own services and to provide individual, personalized advertising for you.

The following cookie is set in your browser due to the integration of Google Maps:

Name: NID

Wert: 188=h26c1Ktha7fCQTx8rXgLyATyITJ111940724-5

Purpose: NID is used by Google to customize ads to your Google search. With the help of the cookie, Google "remembers" your most frequently entered search queries or your previous interaction with ads. This way, you will always get tailored ads. The cookie contains a unique ID that Google uses to collect your personal preferences for advertising purposes.

Expiration date: after 6 months

Note: We cannot guarantee completeness in the details of the stored data. Especially when using cookies, changes can never be excluded. In order to identify the cookie NID, a separate test page was created, where only Google Maps was integrated.

How long and where is the data stored?

Google servers are located in data centers all over the world. However, most servers are located in America. For this reason, your data is also increasingly stored in the USA. Here you can read exactly where the Google data centers are located:

<https://www.google.com/about/datacenters/inside/locations/?hl=de>.

Google distributes the data on different data carriers. This means that the data can be retrieved more quickly and is better protected against any attempts at manipulation. Each data center also has special emergency programs. For example, if there are problems with Google's hardware or a natural disaster cripples the servers, the data will pretty much remain protected anyway.

Google stores some data for a set period of time. For other data, Google only offers the option to delete it manually. Furthermore, the company also anonymizes information (such as advertising data) in server logs by deleting part of the IP address and cookie information after 9 and 18 months, respectively.

How can I delete my data or prevent data storage?

With the automatic location and activity data deletion feature introduced in 2019, location and web/app activity information will be stored for either 3 or 18 months, depending on your decision, and then deleted. In addition, you can also manually delete this data from your history at any time via your Google account. If you want to completely prevent your location tracking, you need to pause the "Web and App Activity" section in Google Account. Click "Data and personalization" and then click the "Activity setting" option. Here you can turn the activities on or off.

In your browser, you can also disable, delete or manage individual cookies. Depending on which browser you use, this always works slightly differently. Under the section "Cookies" you will find the corresponding links to the respective instructions of the most popular browsers.

If you basically do not want cookies, you can set up your browser so that it always informs you when a cookie is to be set. In this way, you can decide for each individual cookie whether you allow it or not.

#### Legal basis

If you have consented to Google Maps being used, the legal basis for the corresponding data processing is this consent. According to Art. 6 (1) lit. a DSGVO (consent), this consent constitutes the legal basis for the processing of personal data as it may occur during the collection by Google Maps.

From our side, there is also a legitimate interest in using Google Maps to optimize our online service. The corresponding legal basis for this is Art. 6 para. 1 lit. f DSGVO (Legitimate Interests). Nevertheless, we only use Google Maps if you have given your consent.

Google also processes data from you in the USA, among other places. We would like to point out that according to the opinion of the European Court of Justice, there is currently no adequate level of protection for the transfer of data to the USA. This may be associated with various risks to the legality and security of data processing.

As a basis for data processing at recipients located in third countries (outside the European Union, Iceland, Liechtenstein, Norway, i.e. in particular in the USA) or a data transfer there, Google uses so-called standard contractual clauses (= Art. 46. para. 2 and 3 DSGVO). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through these clauses, Google undertakes to comply with the European level of data protection when processing your relevant data, even if the data is stored, processed and managed in the US. These clauses are based on an implementing decision of the EU Commission. You can find the decision and the corresponding standard contractual clauses here, among other places: [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?locale=de](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de)

The Google Ads Data Processing Terms, which correspond to the standard contractual clauses, can be found at <https://business.safety.google/adsprocessor/terms/>.


If you want to learn more about Google's data processing, we recommend reading the company's in-house privacy policy at <https://policies.google.com/privacy?hl=de>.

Google reCAPTCHA Privacy Policy

Google reCAPTCHA Privacy Policy Summary


 Data subjects: Visitors to the website

 Purpose: Optimization of our service performance and protection against cyber attacks.

 Data Processed: Data such as IP address, browser information, your operating system, limited location and usage data.

More details can be found below in this privacy policy.

 Storage duration: depending on the stored data.

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

## What is reCAPTCHA?

Our primary goal is to secure and protect our website for you and for us in the best possible way. To ensure this, we use Google reCAPTCHA from the company Google Inc. For the European area, the company Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services. With reCAPTCHA we can determine whether you are really a flesh and blood human being and not a robot or other spam software. By spam we mean any unsolicited information sent to us electronically. With the classic CAPTCHAS, you usually had to solve text or image puzzles to verify the information. With reCAPTCHA from Google, we usually don't have to bother you with such puzzles. Here, in most cases, it is enough to simply check a box to confirm that you are not a bot. With the new Invisible reCAPTCHA version, you don't even have to set a checkmark anymore. You'll learn exactly how this works and, more importantly, what data is used to do it later in this privacy policy.

reCAPTCHA is a free captcha service from Google that protects websites from spam software and abuse by non-human visitors. Most commonly, this service is used when you fill out forms on the web. A captcha service is a kind of automatic Turing test, designed to ensure that an action on the Internet is performed by a human and not by a bot. In the classic Turing test (named after computer scientist Alan Turing), a human determines the distinction between a bot and a human. In captchas, the computer or a software program also does this. Classic captchas work with small tasks that are easy for humans to solve, but present significant difficulties for machines. With reCAPTCHA, you no longer have to actively solve puzzles. The tool uses modern risk techniques to distinguish humans from bots. Here, you only need to check the "I am not a robot" text box, or with Invisible reCAPTCHA, even that is no longer necessary. With reCAPTCHA, a JavaScript element is included in the source code and then the tool runs in the background and analyzes your user behavior. From these user actions, the software calculates a so-called captcha score. Google uses this score to calculate even before the captcha is entered how likely you are to be a human. reCAPTCHA, or captchas in general, are always used when bots could manipulate or abuse certain actions (such as registrations, surveys, etc.).

## Why do we use reCAPTCHA on our website?

We only want to welcome flesh and blood people to our site. Bots or spam software of any kind may confidently stay at home. That's why we pull out all the stops to protect ourselves and offer the best possible user experience for you. For this reason we use Google reCAPTCHA from Google. This way we can be pretty sure that we remain a "bot-free" website. By using reCAPTCHA, data is transmitted to Google to determine whether you are actually human. reCAPTCHA is therefore used to ensure the security of our website and, by extension, your security. For example, without reCAPTCHA, it could

happen that a bot registers as many e-mail addresses as possible during registration in order to "spam" forums or blogs with unwanted advertising content. With reCAPTCHA we can avoid such bot attacks.

What data is stored by reCAPTCHA?

reCAPTCHA collects personal data from users to determine whether actions on our website really originate from humans. Thus, the IP address and other data required by Google for the reCAPTCHA service may be sent to Google. IP addresses are almost always shortened beforehand within the member states of the EU or other contracting states to the Agreement on the European Economic Area before the data ends up on a server in the USA. The IP address is not combined with other data from Google unless you are logged in with your Google account while using reCAPTCHA. First, the reCAPTCHA algorithm checks whether Google cookies from other Google services (YouTube, Gmail, etc.) are already placed on your browser. Then, reCAPTCHA places an additional cookie on your browser and captures a snapshot of your browser window.

The following list of collected browser and user data does not claim to be complete. Rather, they are examples of data that, to our knowledge, are processed by Google.

Referrer URL (the address of the page from which the visitor comes)

IP address (e.g. 256.123.123.1)

Information about the operating system (the software that enables the operation of your computer. Known operating systems are Windows, Mac OS X or Linux)

Cookies (small text files that store data in your browser)

Mouse and keyboard behavior (every action you perform with the mouse or keyboard is stored)

Date and language settings (which language or date you have preset on your PC is saved)

All JavaScript objects (JavaScript is a programming language that allows websites to adapt to the user. JavaScript objects can collect all kinds of data under one name)

Screen resolution (shows how many pixels the image display consists of)

It is undisputed that Google uses and analyzes this data even before you click on the "I am not a robot" checkbox. With the Invisible reCAPTCHA version even the ticking is omitted and the whole recognition process runs in the background. How much and which data Google stores exactly, Google does not tell you in detail.

The following cookies are used by reCAPTCHA: Here we refer to the reCAPTCHA demo version from Google at <https://www.google.com/recaptcha/api2/demo>. All these cookies require a unique identifier for tracking purposes. Here is a list of cookies that Google reCAPTCHA has set on the demo version:



Name: IDE

Value: WqTUmlnmv\_qXyi\_DGNPLESKnRNrpgXoy1K-pAZtAkMbHI-111940724-8

Purpose: This cookie is set by the DoubleClick company (also owned by Google) to register and report a user's actions on the website in dealing with advertisements. In this way, advertising effectiveness can be measured and appropriate optimization measures can be taken. IDE is stored in browsers under the domain doubleclick.net.

Expiration date: after one year

Name: 1P\_JAR

Value: 2019-5-14-12

Purpose: This cookie collects statistics on website usage and measures conversions. A conversion occurs, for example, when a user becomes a buyer. The cookie is also used to display relevant advertisements to users. Furthermore, the cookie can be used to prevent a user from seeing the same ad more than once.

Expiration date: after one month

Name: ANID

Wert: U7j1v3dZa1119407240xgZFmiqWppRWKOr

Purpose: We couldn't find out much info about this cookie. Google's privacy policy mentions the cookie in the context of "advertising cookies" such as "DSID", "FLC", "AID", "TAID". ANID is stored under domain google.com.

Expiration date: after 9 months

Name: CONSENT

Value: YES+AT.en+20150628-20-0

Purpose: The cookie stores the status of a user's consent to use different services provided by Google. CONSENT is also used for security purposes to verify users, prevent credential fraud, and protect user data from unauthorized attacks.

Expiration date: after 19 years

Name: NID

Wert: 0WmuWqy111940724zILzqV\_nmt3sDXwPeM5Q

Purpose: NID is used by Google to customize ads to your Google search. With the help of the cookie, Google "remembers" your most typed search queries or your previous interaction with ads. This way, you always get tailored ads. The cookie contains a unique ID to collect personal settings of the user for advertising purposes.

Expiration date: after 6 months

Name: DV

Wert: gEAABBCjJMXcl0dSAAAANbqc111940724-4

Purpose: Once you have checked the "I am not a robot" box, this cookie will be set. The cookie is used by Google Analytics for personalized advertising. DV collects information in anonymous form and is further used to make user distinctions.

Expiration date: after 10 minutes

Note: This list cannot claim to be exhaustive, as Google's experience has shown that the choice of cookies is always subject to change.

How long and where is the data stored?

By inserting reCAPTCHA, data is transferred from you to the Google server. Where exactly this data is stored, Google does not make clear, even after repeated inquiries. Without having received confirmation from Google, it can be assumed that data such as mouse interaction, time spent on the website or language settings are stored on Google's European or American servers. The IP address that your browser transmits to Google is generally not merged with other Google data from other Google services. However, if you are logged into your Google account while using the reCAPTCHA plug-in, the data will be merged. The deviating data protection provisions of the Google company apply to this.

How can I delete my data or prevent data storage?

If you do not want any data about you and your behavior to be transmitted to Google, you must log out of Google completely and delete all Google cookies before you visit our website or use the reCAPTCHA software. Basically, as soon as you visit our site, the data is automatically transmitted to Google. To delete this data again, you must contact Google support at <https://support.google.com/?hl=de&tid=111940724>.

So, when you use our website, you agree that Google LLC and its agents automatically collect, process and use data.

Please note that when you use this tool, data about you may 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 may therefore not simply be transferred, stored and processed there unless there are suitable safeguards (such as EU standard contractual clauses) between us and the non-European service provider.

## Legal basis

If you have consented to Google reCAPTCHA being used, the legal basis for the corresponding data processing is this consent. According to Art. 6 (1) lit. a DSGVO (consent), this consent constitutes the legal basis for the processing of personal data as may occur when Google reCAPTCHA is used.

From our side, there is also a legitimate interest in using Google reCAPTCHA to optimize our online service and make it more secure. The corresponding legal basis for this is Art. 6 para. 1 lit. f DSGVO (Legitimate Interests). Nevertheless, we only use Google reCAPTCHA if you have given your consent.

Google also processes data from you in the USA, among other places. We would like to point out that according to the opinion of the European Court of Justice, there is currently no adequate level of protection for the transfer of data to the USA. This may be associated with various risks for the legality and security of data processing.

Google uses so-called standard contractual clauses (= Art. 46. para. 2 and 3 DSGVO) as the basis for data processing for recipients located in third countries (outside the European Union, Iceland, Liechtenstein, Norway, i.e. in particular in the USA) or a data transfer there. Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through these clauses, Google undertakes to comply with the European level of data protection when processing your relevant data, even if the data is stored, processed and managed in the US. These clauses are based on an implementing decision of the EU Commission. You can find the decision and the corresponding standard contractual clauses here, among other places: [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?locale=de](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de)

The Google Ads Data Processing Terms, which correspond to the standard contractual clauses, can be found at <https://business.safety.google/adsprocessor/terms/>.

You can learn a bit more about reCAPTCHA on Google's web developer page at <https://developers.google.com/recaptcha/>. Google does go into more detail about the technical development of reCAPTCHA here, but you will search in vain for precise information about data storage and privacy-related issues there as well. A good overview of Google's basic use of data can be found in the company's own privacy policy at <https://www.google.com/intl/de/policies/privacy/>.

All texts are protected by copyright.

Quelle: Erstellt mit dem Datenschutz Generator von AdSimple