

Privacy policy

Introduction and overview

We have prepared this privacy policy (version 03.04.2024-112758054) 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 commissioned by us (e.g. providers) - 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 provide you with comprehensive information about the data we process about you.

Data protection declarations usually sound very technical and use legal jargon. This privacy policy, on the other hand, is intended to describe the most important things to you as simply and transparently as possible. Where it is conducive to transparency, technical **terms are explained in a reader-friendly way**, links to further information are provided and **graphics are used**. We thus inform you in clear and simple language that we only process personal data as part of our business activities if there is a corresponding legal basis. This is certainly not possible by providing explanations that are as concise, unclear and legally technical as possible, as is often standard 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 any questions, please contact the responsible body named below or in the legal notice, follow the links provided and view further information on third-party websites. Our contact details can of course also be found in the legal notice.

Area of application

This privacy policy applies to all personal data processed by us in the company and to all personal data processed by companies commissioned by us (processors). By personal data, we mean information within the meaning of Art. 4 No. 1 GDPR, such as a person's name, email 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 stores) that we operate
- Social media presences and e-mail communication
- Mobile apps for smartphones and other devices

In short, the privacy policy applies to all areas in which personal data is processed in the company in a structured manner via the channels mentioned. Should we process data outside

If we enter into a legal relationship with you via 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 basis 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 April 27, 2016. You can of course read this EU General Data Protection Regulation online at EUR-Lex, the gateway 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 the data you entered in a contact form.
2. **Contract** (Article 6(1)(b) GDPR): To fulfill a contract or pre-contractual
We process your data in order to fulfill our obligations to you. For example, if we conclude a purchase agreement with you, we require 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 the case of legitimate interests that
If we 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 securely and efficiently. This processing is therefore a legitimate interest.

Other conditions such as recording in the public interest, the exercise of official authority and the protection of vital interests do not generally apply to us. If such a legal basis is relevant, it will be indicated at the appropriate point.

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

- In **Austria**, this is the Federal Act on the Protection of Natural Persons with regard to the Processing of Personal Data (**Data Protection Act**), or **DSG** for short.
- In **Germany**, the **Federal Data Protection Act (BDSG)** applies.

If other regional or national laws apply, we will inform you of this in the following sections.

Contact details of the person responsible

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

REPLOID Group AG

Philip Pauer, MBA MSc (CEO)

Terminalstrasse 23

A-4600 Wels Austria

E-mail: office@reploid.eu Phone:

[+43 660 / 475 55 56](tel:+436604755556)

Imprint: <https://reploid.eu/impressum/>

Storage duration

It is a general criterion for us that we only store personal data 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 the data processing no longer exists. In some cases, we are legally obliged to store certain data even after the original purpose has ceased to exist, for example for accounting purposes.

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

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

Rights under the General Data Protection Regulation

In accordance with Articles 13, 14 GDPR, we inform you of the following rights to which you are entitled in order to ensure fair and transparent processing of data:

- According to Article 15 GDPR, you have a right to information as to whether we process your data. If this is the case, you have the right to receive a copy of the data and the following information:
 - the purpose for which we carry out the 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 analyzed in order to create a personal profile of you.
- According to Article 16 GDPR, you have a right to rectification of data, which means that we must correct data if you find errors.
- According to Article 17 GDPR, you have the right to erasure ("right to be forgotten"), which specifically means that you may request the erasure of your data.
- According to Article 18 GDPR, you have the right to restriction of processing, which means that we may only store the data but no longer use it.
- According to Article 20 GDPR, you have the right to data portability, which means that we will provide you with your data in a commonly used format upon request.
- According to Article 21 GDPR, you have the right to object, which will result in a change in the 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 can object to the processing. We will then check as quickly as possible whether we can legally comply with this objection.
 - If data is used for direct marketing purposes, you can 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 for profiling purposes, you can object to this type of data processing at any time. We may then no longer use your data for profiling.
- Under Article 22 GDPR, you may have the right not to be subject to a decision based solely on automated processing (e.g. profiling).
- According to Article 77 GDPR, you have the right to lodge a complaint. This means that you can lodge a complaint with the data protection authority at any time if you believe that the processing of personal data violates the GDPR.

In short: You have rights - do not hesitate to contact the responsible office 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 lodge a complaint with 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: Dr. Andrea Jelinek

Address: Barichgasse 40-42, 1030 Vienna

Telephone no.: +43 1 52 152-0

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

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

Data transfer to third countries

We only transfer or process data to countries outside the scope of the GDPR (third countries) if you consent to this processing or other legal permission exists. This applies in particular if the processing is required by law or necessary to fulfill a contractual relationship and in any case only to the extent that this is generally permitted. In most cases, your consent is the most important reason why we process data in third countries. The processing of personal data in third countries such as the USA, where many software manufacturers offer services and have their server locations, may mean that personal data is processed and stored in unexpected ways.

We expressly point out that, in the opinion of the European Court of Justice, an adequate level of protection for data transfers to the USA currently only exists if a US company that processes personal data of EU citizens in the USA is an active participant in the EU-US Data Privacy Framework. You can find more information on this at:

https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en

Data processing by US services that are not active participants in the EU-US Data Privacy Framework may result in data not being processed and stored anonymously. Furthermore, US government authorities may be able to access individual data. In addition, data collected may be linked to data from other services of the same provider if you have a corresponding user account. Where possible, we try to use server locations within the EU if this is offered.

We will inform you in more detail about data transfer to third countries, if applicable, in the appropriate sections of this privacy policy.

Security of data processing

In order 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 for third parties to infer personal information from our data.


Art. 25 GDPR speaks here of "data protection by design and by default" 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 appropriate measures should be taken. If necessary, we will discuss specific measures below.

TLS encryption with https

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

This means that the complete transmission of all data from your browser to our web server is secured - nobody can "listen in".

We have thus introduced an additional layer of security and comply with data protection by design ([Article 25\(1\) GDPR](#)). 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 data transmission security by the small lock symbol  at the top left of the browser, to the left of the Internet address (e.g. examplepage.com) and the use of the https scheme (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

 Data subjects: Anyone who communicates with us by telephone, e-mail or online form

 Processed data: e.g. telephone number, name, e-mail address, data entered

Form data. You can find more details on this under the respective contact type used

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

 Storage period: Duration of the business case and the statutory provisions 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)

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

The data is processed for the handling and processing of your question and the associated business transaction. The data will be stored for as long as required by law.

Affected persons

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 in pseudonymized form on the respective end device and with the telecommunications provider used. In addition, data such as name

and telephone number are then sent by e-mail and stored for the purpose of responding to inquiries. The data will be deleted as soon as the business case has been completed and legal requirements permit.

e-mail

If you communicate with us by email, data may be stored on the respective end device (computer, laptop, smartphone, etc.) and data may be stored on the email server. The data will be deleted as soon as the business transaction has been completed and legal requirements permit.

Online forms

If you communicate with us using an online form, data is stored on our web server and may be forwarded to one of our e-mail addresses. The data will be deleted as soon as the business transaction has been completed and legal requirements permit.

Legal basis


The processing of the data is based on the following legal bases:


- Art. 6 para. 1 lit. a GDPR (consent): You give us your consent to store your data and to use it for purposes relating to the business transaction;
- Art. 6 para. 1 lit. b GDPR (contract): It is necessary 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 GDPR (legitimate interests): We want to handle customer inquiries and business communication in a professional manner. This requires certain technical facilities such as e-mail programs, exchange servers and mobile network operators in order to operate communication efficiently.


Cookies

Cookies summary

 Affected parties: Visitors to the website

 Purpose: depends on the cookie in question. You can find more details on this below or from the manufacturer of the software that sets the cookie.

 Processed data: Depending on the cookie used. You can find more details on this below or from the manufacturer of the software that sets the cookie.

 Storage duration: depending on the cookie, can vary 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.

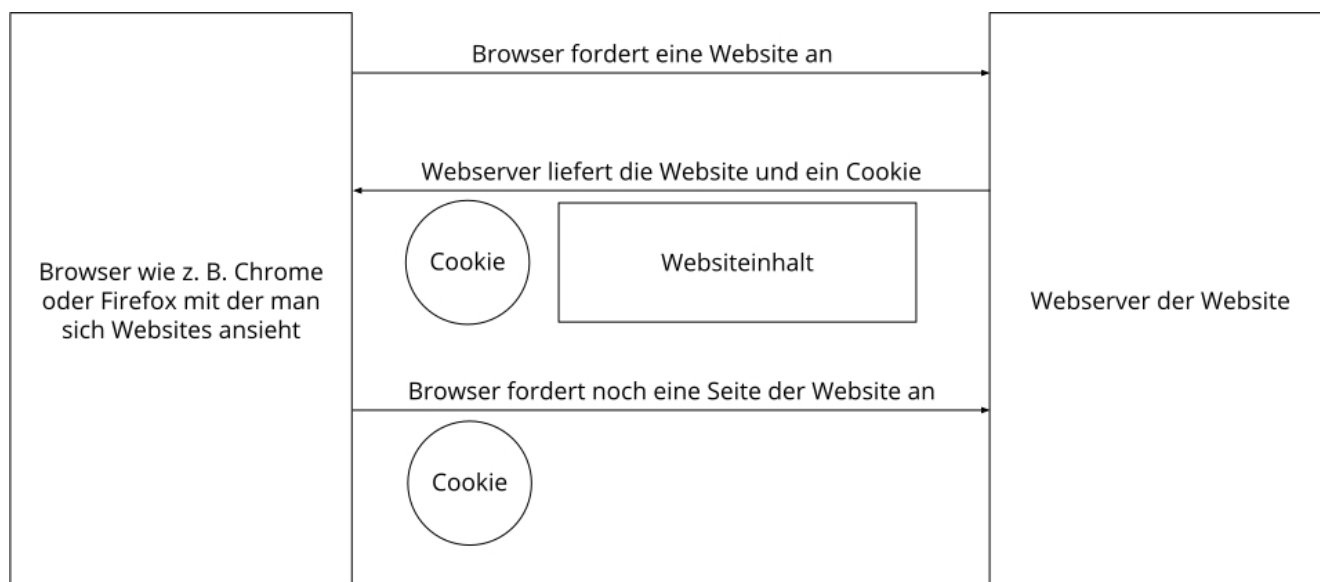
Below we explain what cookies are and why they are used so that you can better understand the following privacy policy.

Whenever you surf the internet, you use a browser. Well-known 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 cannot be denied: Cookies are really useful little helpers. Almost all websites use cookies. More precisely, they are HTTP cookies, as there are also other cookies for other areas of application. HTTP cookies are small files that are stored on your computer by our website. These cookie files are automatically stored in the cookie folder, the "brain" of your browser, so to speak. 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 visit our site again, your browser transmits the "user-related" information back to our site. Thanks to cookies, our website knows who you are and offers you the settings 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. 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 website, third-party cookies are created by partner websites (e.g. Google Analytics). Each cookie must be evaluated individually, as each cookie stores different data.

The expiry time of a cookie also varies from a few minutes to a few years. Cookies are not software programs and do not contain viruses, Trojans or other "malware". Cookies also cannot access information on your PC. Cookie data

can look like this, for example:

Name: _ga

Wert: GA1.2.1326744211.152112758054-9

Intended use: Differentiation of 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 used and is clarified in the following sections of the privacy policy. At this point, we would like to briefly explain the different types of HTTP cookies.

A distinction can be made between 4 types of cookies:

Essential cookies

These cookies are necessary to ensure basic website functions. For example, these cookies are needed when a user places a product in the shopping cart, then continues surfing on other pages and only goes to the checkout later. These cookies ensure that the shopping cart is not deleted even if the user closes their browser window.

Purposeful cookies

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

Targeted cookies

These cookies ensure better user-friendliness. 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 practical, but also very annoying.

When you visit a website for the first time, you are usually asked which of these cookie types you would like to allow. And of course this decision is also stored in a cookie.

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

Purpose of processing via cookies

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

What data is processed?

Cookies are little helpers for many different tasks. Unfortunately, it is not possible to generalize which 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 period depends on the cookie in question and is specified 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 delete all cookies manually 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 you withdraw your consent, whereby the legality of the storage until then remains unaffected.

Right to object - how can I delete cookies?

You decide how and whether you want to use cookies. Regardless of which service or website the cookies come from, you always have the option of deleting, deactivating or only partially allowing 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 this in your browser settings:

[Chrome: Delete, activate and manage cookies in Chrome Safari:](#)

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

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

[Explorer: Delete and manage cookies](#)

[Microsoft Edge: Deleting and managing cookies](#)

If you generally do not want to have cookies, you can set up your browser so that it

always informs you when a cookie is to be set. This allows you to decide for each individual cookie whether or not to allow it. The procedure differs depending on the browser. It is best to search for the instructions in Google using the search term "delete cookies Chrome" or "deactivate cookies Chrome" in the case of 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). However, there are still very different reactions to these directives within the EU countries. In Austria, however, this directive was implemented in Section 165 (3) of the Telecommunications Act (2021). In Germany, the cookie directives have not been implemented as national law.

Instead, this directive was largely implemented in Section 15 (3) of the German Telemedia Act (TMG).


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


If cookies that are not absolutely necessary are used, this will only take place with your consent. The legal basis in this respect is Art. 6 para. 1 lit. a GDPR.


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


Webhosting introduction

Web hosting summary

 Affected parties: Visitors to the website

 Purpose: professional hosting of the website and securing its operation

 Processed data: IP address, time of the website visit, browser used and other data. You can find more details on this below or from the web hosting provider used.

 Storage period: depending on the respective provider, but usually 2 weeks Legal basis: Art. 6 para. 1 lit.f GDPR (legitimate interests)

What is web hosting?

When you visit websites these days, 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 start page (homepage) to the very last subpage (like this one). By domain we mean, for example, example.de or example.com.

If you want to view a website on a computer, tablet or smartphone, you use a program called a web browser. You probably know a few web browsers by name: Google Chrome, Microsoft Edge, Mozilla Firefox and Apple Safari. We call them browsers or web browsers for short.

To display the website, the browser must connect to another computer where the website code is stored: the web server. Operating a web server is a complicated and time-consuming task, which is why this is usually done by professional providers. They offer web hosting and thus ensure reliable and error-free storage of website data. A lot of technical terms, but please stay tuned, it will get even better!

When the browser on your computer (desktop, laptop, tablet or 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; on the other hand, the web server must also store data for a certain period of time in order to ensure proper operation.

A picture is worth a thousand words, so the following graphic 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 website hosting and operational security
2. to maintain operational and IT security
3. Anonymous evaluation of access behavior to improve our offer and, if necessary, for criminal prosecution or prosecution of claims

What data is processed?

Even while you are currently visiting our website, our web server, i.e. the computer on which this website is stored, usually automatically saves data such as

- the complete Internet address (URL) of the website accessed•
- 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.beispielquellsite.de/vondabinichgekommen/)

- the host name and IP address of the device from which access is made (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-mentioned data is stored for two weeks and then automatically deleted. We do not pass this data on, but we cannot rule out the possibility of this data being 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 pass on 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 para. 1 lit. f GDPR (protection of legitimate interests), because the use of professional hosting with a provider is necessary in order 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.

As a rule, there is a contract between us and the hosting provider for order processing in accordance with Art. 28 f. GDPR, which ensures compliance with data protection and guarantees data security.

Web hosting provider External privacy policy

Below you will find the contact details of our external hosting provider, where, in addition to the information above, you can find out more about data processing:

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen
Germany


Phone: +49 (0)9831 505-0*
Fax: +49 (0)9831 505-3
E-mail: info@hetzner.com


You can find out more about data processing by this provider in the [privacy policy](#).

Website modular systems Introduction

Website builder systems Privacy policy summary

 Affected parties: Visitors to the website

 Purpose: Optimization of our service performance

 Processed data: Data such as technical usage information such as browser activity, clickstream activity, session heatmaps as well as contact details, IP address or your geographical location. You can find more details on this below in this privacy policy and in the providers' privacy policies.

 Storage duration: depends on the provider

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

What are website builder systems?

We use a modular website system for our website. Modular systems are special forms of a content management system (CMS). With a modular system, website operators can create a website very easily and without programming knowledge. In many cases, web hosters also offer modular systems. By using a modular system, your personal data can 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 declarations.

Why do we use website builder systems for our website?

The biggest advantage of a modular system is its ease of use. We want to offer you a clear, simple and well-organized 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 offer you an informative and enjoyable time on our website.

What data is stored by a modular system?

Exactly which data is stored depends, of course, on the website builder system used. Each provider processes and collects different data from the website visitor. As a rule, 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 collected. Tracking data (e.g. browser activity, clickstream activity, session heatmaps, etc.) may also be processed. Personal data may also be collected and stored. This usually involves contact data such as email address, telephone number (if you have provided this), 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 building block system used, if 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. The provider may store your data according to its own specifications, over which we have no influence.

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 builder 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 not all functions may then work as usual.

Legal basis

We have a legitimate interest in using a website building block system to optimize our online service and to present it to you in an efficient and user-friendly manner. The legal basis for this is Art. 6 para. 1 lit. f GDPR (legitimate interests). Nevertheless, we only use the modular system if 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 GDPR.


In this privacy policy, we have provided you with the most important general information about 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

WordPress.com Privacy Policy Summary

 Affected parties: Visitors to the website

 Purpose: Optimization of our service performance

 Processed data: Data such as technical usage information such as browser activity, clickstream activity, session heatmaps as well as contact details, IP address or your geographical location. You can find more details on this below in this privacy policy.

 Storage duration: It depends above all on the type of data stored and the specific settings.

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

What is WordPress?

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

In 2003, the company saw the light of day and developed into one of the best-known content management systems (CMS) in the world in a relatively short space of time. A CMS is software that helps us to design our website and present content in an attractive and organized way. The content can be text, audio and video.

By using WordPress, your personal data may also be collected, stored and processed. As a rule, mainly technical data such as operating system, browser, screen resolution or hosting provider are stored. However, personal data such as IP address, geographical data or contact details may also be processed.

Why do we use WordPress on our website?

We have many strengths, but real programming is not one of our core competencies.

Nevertheless, we want to have a powerful and attractive website that we can also manage and maintain ourselves. With a modular website system or a content management system such as WordPress, we can do just that. With WordPress, we don't have to be ace programmers to offer you a beautiful website. Thanks to WordPress, we can operate our website quickly and easily even without prior technical knowledge. If technical problems occur or we have special requests for our website, there are always our specialists who feel at home in HTML, PHP, CSS and co.

Thanks to the ease of use and comprehensive functions of WordPress, we can design our website according to our wishes and offer you a good user experience.

What data is processed by WordPress?

Non-personal data includes technical usage information such as browser activity, clickstream activity, session heatmaps and data about your computer, operating system, browser, screen resolution, language and keyboard settings, internet provider and date of the page visit.

Personal data is also collected. These are primarily contact data (e-mail address or telephone number, if you provide these), IP address or your geographical location.

WordPress can also use cookies to collect data. These often collect data about your behavior on our website. For example, it may record which subpages you particularly like to view, how long you spend on individual pages, when you visit a page, how long you stay on a particular page and when you leave a page.

leave again (bounce rate) or which default settings (e.g. language selection) you have made. Based on this data, WordPress can also better adapt its own marketing measures to your interests and user behavior. The next time you visit our website, you will therefore be shown our website as you have previously set it.

WordPress may also use technologies such as pixel tags (web beacons), for example to clearly identify you as a user and possibly offer interest-based advertising.

How long and where is the data stored?

How long the data is stored depends on various factors. So it mainly depends on the type of data stored and the specific settings of the website.

In principle, WordPress deletes data when it is no longer needed for its own purposes. There are of course exceptions, especially if legal obligations require the data to be stored for longer. Web server logs containing your IP address and technical data are deleted by WordPress or Automattic after 30 days. Automattic uses the data for this period to analyze the traffic on its own websites (e.g. all WordPress pages) and to resolve potential problems. Deleted content on WordPress websites is also stored in the recycle bin for 30 days to enable recovery, after which it may remain in backups and caches until it is deleted. The data is stored on Automattic's American servers.

How can I delete my data or prevent data storage?

You have the right and opportunity to access your personal data at any time and to object to its use and processing. You can also lodge a complaint with a state supervisory authority at any time.

In your browser, you also have the option of individually managing, deleting or deactivating cookies. Please note, however, that deactivated or deleted cookies may have a negative impact on the functions of our WordPress site. Depending on which browser you use, the management of cookies works slightly differently. In the "Cookies" section, you will find the relevant links to the instructions for the most popular browsers.

Legal basis

If you have consented to the use of WordPress, the legal basis for the corresponding data processing is this consent. According to Art. 6 para. 1 lit. a GDPR (consent), this consent constitutes the legal basis for the processing of personal data, as may occur when WordPress collects data.

We also have a legitimate interest in using WordPress to optimize our online service and present it to you in an attractive way. The corresponding

The legal basis is Art. 6 para. 1 lit. f GDPR (legitimate interests). Nevertheless, we only use WordPress if you have given your consent.

WordPress or Automattic processes your data in the USA, among other places. Automattic is an active participant in the EU-US Data Privacy Framework, which regulates the correct and secure transfer of personal data from EU citizens to the USA. You can find more information on this at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.


Automattic also uses so-called standard contractual clauses (= Art. 46 (2) and (3) GDPR). Standard Contractual Clauses (SCCs) 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 the EU-US Data Privacy Framework and the standard contractual clauses, Automattic 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: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de


You can find more details on the privacy policy and which data is processed by WordPress and how at <https://automattic.com/privacy/>.

Web Analytics Introduction

Web Analytics privacy policy summary

 Affected parties: Visitors to the website

 Purpose: Evaluation of visitor information to optimize the website. Processed data: Access statistics, the data such as locations of access, device data, access duration and time, navigation behavior, click behavior and IP addresses. You can find more details on this in the respective web analytics tool used.

 Storage period: depending on the web analytics tool used Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is web analytics?

We use software on our website to evaluate the behavior of website visitors, known as web analytics or web analysis for short. This involves collecting data that is stored, managed and processed by the respective analytics tool provider (also known as a tracking tool). The data is used to create analyses of user behavior on our website and made available to us as the website operator. In addition, most tools offer various test options. For example, we can test which offers or content are best received by our visitors. To do this, we show you two different offers for a limited period of time. After the test (known as an A/B test), we know which product or content is most popular.

which content our website visitors find more interesting. For such test procedures, as well as for other analytics procedures, user profiles can also be created and the data stored in cookies.

Why do we use web analytics?

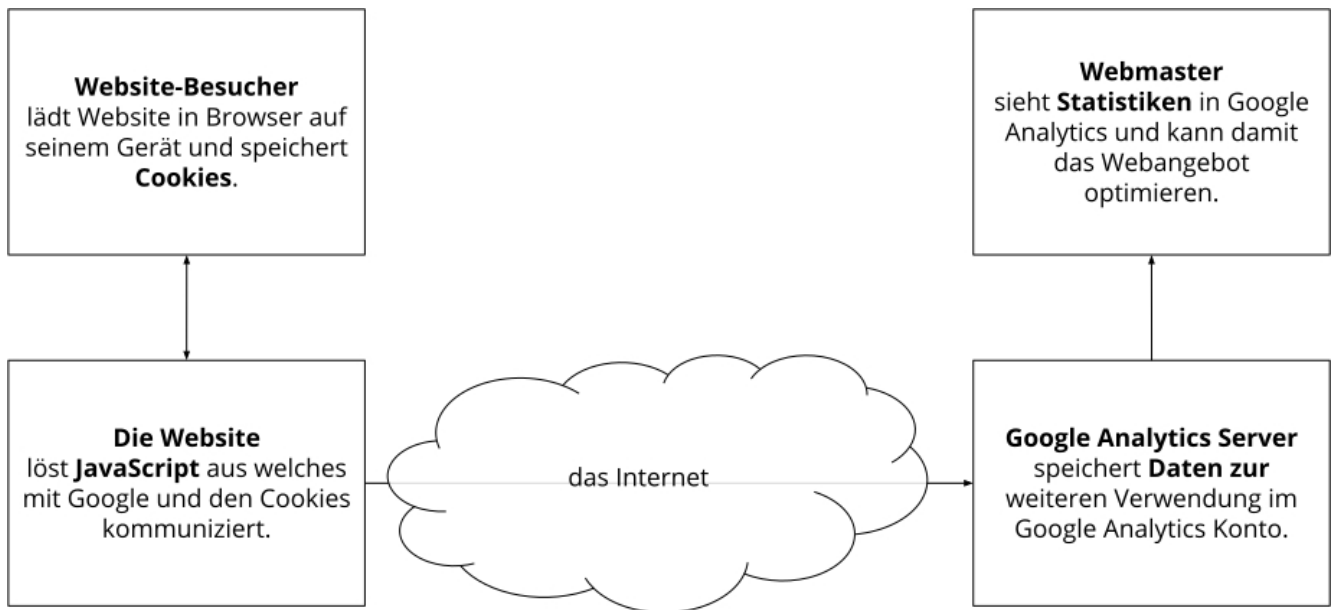
With our website, we have a clear goal in mind: we want to deliver the best web offering on the market for our industry. In order to achieve this goal, we want to offer the best and most interesting services on the one hand and make sure that you feel completely at ease on our website on the other. With the help of web analysis tools, we can take a closer look at the behavior of our website visitors and then improve our website accordingly for you and for us. For example, we can see the average age of our visitors, where they come from, when our website is visited the most or which content or products are particularly popular. All this information helps us to optimize the website and thus adapt it to your needs, interests and wishes.

What data is processed?

Exactly which data is stored depends, of course, on the analysis tools used. As a rule, however, the content you view on our website, which buttons or links you click on, when you access a page, which browser you use, which device (PC, tablet, smartphone, etc.) you use to visit the website or which computer system you use are stored, for example. If you have agreed that location data may also be collected, this may also be processed by the web analysis tool provider.

Your IP address is also stored. According to the General Data Protection Regulation (GDPR), IP addresses are personal data. However, your IP address is usually stored pseudonymized (i.e. in an unrecognizable and shortened form). For the purpose of testing, web analysis and web optimization, no direct data such as your name, age, address or e-mail address is stored. All this data, if collected, is stored in pseudonymized form. This means that you cannot be identified as a person.

The following example shows schematically how Google Analytics works as an example of client-based web tracking with Java Script code.



How long the respective data is stored always depends on the provider. Some cookies only store data for a few minutes or until you leave the website, while other cookies can store data for several years.

Duration of data processing

We will inform you about the duration of data processing below, if 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. If required by law, for example in the case of accounting, this storage period may also be exceeded.

Right of objection

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

Legal basis

The use of web analytics requires your consent, which we have obtained with our cookie pop-up. According to **Art. 6 para. 1 lit. a GDPR (consent)**, this consent constitutes the legal basis for the processing of personal data, as may occur when it is collected by web analytics tools.

In addition to consent, we have a legitimate interest in analyzing the behavior of website visitors in order to improve our offer technically and economically. With the help of web analytics, we recognize errors on the website, can detect attacks

identify and improve efficiency. The legal basis for this is **Art. 6 para. 1 lit. f GDPR (legitimate interests)**. Nevertheless, we only use the tools if you have given your consent.


Since web analytics tools use cookies, we recommend that you also read our general privacy policy on cookies. To find out exactly which of your data is stored and processed, you should read the privacy policies of the respective tools.


Information on special web analytics tools, if available, can be found in the following sections.

Google Analytics privacy policy

Google Analytics privacy policy summary

 Affected parties: Visitors to the website

 Purpose: Evaluation of visitor information to optimize the website. Processed data: Access statistics, the data such as locations of access, device data, access duration and time, navigation behavior and click behavior. You can find more details on this below in this privacy policy.

 Storage duration: individually adjustable, by default Google Analytics stores 4 data for 14 months

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

What is Google Analytics?

On our website, we use the analysis tracking tool Google Analytics in the version Google Analytics 4 (GA4) of the American 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. Google Analytics collects data about your actions on our website. However, by combining various technologies such as cookies, device IDs and login information, you can be identified as a user across different devices. This means that your actions can also be analyzed across platforms.

For example, when you click on a link, this event is stored in a cookie and sent to Google Analytics. The reports we receive from Google Analytics help us to better tailor our website and our service to your wishes. In the following, we will go into more detail about the tracking tool and inform you in particular about which data is processed and how you can prevent this.

Google Analytics is a tracking tool that is used to analyze the traffic on our website. These measurements and analyses are based on a pseudonymous user identification number. This number does not contain any personal data such as name or address, but is used to assign events to an end device. GA4 uses an event-based model that provides detailed information on user interactions such as page views, clicks, scrolling, conversion events

recorded. In addition, various machine learning functions have also been built into GA4 to better understand user behavior and certain trends. GA4 relies on modeling with the help of machine learning functions. This means that missing data can also be extrapolated on the basis of the collected data in order to optimize the analysis and also to be able to make forecasts.

For Google Analytics to work in principle, a tracking code is built into the code of our website. When you visit our website, this code records various events that you perform on our website. With GA4's event-based data model, we as website operators can define and track specific events in order to obtain analyses of user interactions. In addition to general information such as clicks or page views, specific events that are important for our business can also be tracked. Such specific events can be, for example, the sending of a contact form or the purchase of a product.

As soon as you leave our website, this data is sent to the Google Analytics servers and stored there.

Google processes the data and we receive reports about your user behavior. These may include the following reports:

- Target group reports: We use target group reports to get to know our users better and know more precisely who is interested in our service.
- Ad reports: Ad reports make it easier for us to analyze and improve our online advertising.
- Acquisition reports: Acquisition reports provide us with helpful information on how we can get more people interested in our service.
- Behavior reports: Here we learn how you interact with our website. We can track which route you take on our site and which links you click on.
- Conversion reports: Conversion is a process in which you perform a desired action as a result of a marketing message. For example, when you go from being just a website visitor to a buyer or newsletter subscriber. With the help of these reports, we learn more about how our marketing measures are received by you. This is how we want to increase our conversion rate.
- Real-time reports: Here we always know immediately what is happening on our website. For example, we can see how many users are currently reading this text.

In addition to the analysis reports mentioned above, Google Analytics 4 also offers the following functions, among others:

- Event-based data model: This model captures very specific events that can take place on our website. For example, playing a video, purchasing a product or subscribing to our newsletter.
- Extended analysis functions: These functions enable us to understand your behavior on our website or certain general trends even better. For example, we can

Segment user groups, make comparative analyses of target groups or track your path on our website.

- Predictive modeling: Based on collected data, missing data can be extrapolated using machine learning to predict future events and trends. This can help us to develop better marketing strategies.
- Cross-platform analysis: Data can be collected and analyzed from both websites and apps. This gives us the opportunity to analyze user behavior across platforms, provided you have of course consented to data processing.

Why do we use Google Analytics on our website?

Our goal with this website is clear: we want to offer you the best possible service. The statistics and data from Google Analytics help us to achieve this goal.

The statistically analyzed data gives us a clear picture of the strengths and weaknesses of our website. On the one hand, we can optimize our site so that it can be found more easily by interested people on Google. On the other hand, the data helps us to better understand you as a visitor. We therefore know exactly what we need to improve on our website in order to offer you the best possible service. The data also helps us to carry out our advertising and marketing measures more individually and cost-effectively. After all, it only makes sense to show our products and services to people who are interested in them.

What data is stored by Google Analytics?

Google Analytics uses a tracking code to create a random, unique ID that is linked to your browser cookie. This is how Google Analytics recognizes you as a new user and you are assigned a user ID. The next time you visit our site, you will be recognized as a "returning" user is recognized. All collected data is stored together with this user ID. This makes it possible to evaluate pseudonymous user profiles.

In order to be able to analyze our website with Google Analytics, a property ID must be inserted into the tracking code. The data is then saved in the corresponding property. The Google Analytics 4 property is standard for every newly created property. Depending on the property used, data is stored for different lengths of time.

Through identifiers such as cookies, app instance IDs, user IDs or user-defined event parameters, your interactions are measured across platforms if you have given your consent. Interactions are all types of actions that you perform on our website.

If you also use other Google systems (such as a Google account), data generated via Google Analytics may be linked to third-party cookies. Google does not pass on any Google Analytics data unless we as the website operator authorize this. Exceptions may be made if required by law.

According to Google, no IP addresses are logged or stored in Google Analytics 4. However, Google uses the IP address data to derive location data and deletes it immediately afterwards. All IP addresses that are collected from users in the EU are therefore deleted before the

data is stored in a data center or on a server.

Since Google Analytics 4 focuses on event-based data, the tool uses significantly fewer cookies compared to previous versions (such as Google Universal Analytics).

However, there are some specific cookies that are used by GA4. These include, for example:

Name: `_ga`

Wert: 2.1326744211.152112758054-5

Intended use: By default, analytics.js uses the `_ga` cookie to store the user ID. It is basically used to differentiate between website visitors.

Expiration date: after 2 years

Name: `_gid`

Wert: 2.1687193234.152112758054-1

Purpose: The cookie is also used to distinguish website visitors

Expiration date: after 24 hours

Name: `_gat_gtag_UA_<property-id>`

Value: 1

Purpose: Used to reduce the request rate. If Google Analytics is provided via Google Tag Manager, this cookie is given the name `_dc_gtm_<property-id>`.

Expiration date: after 1 minute

Note: This list cannot claim to be exhaustive, as Google is constantly changing its choice of cookies. The aim of GA4 is also to improve data protection. The tool therefore offers a number of options for controlling data collection. For example, we can set the storage duration ourselves and also control data collection.

Here we show you an overview of the most important types of data that are collected with Google Analytics:

Heatmaps: Google creates so-called heatmaps. Heatmaps allow you to see exactly those areas that you click on. This gives us information about where you are "traveling" on our site.

Session duration: Google defines session duration as the time you spend on our site without leaving the page. If you have been inactive for 20 minutes, the session ends automatically.

Bounce rate: A bounce is when you only view one page on our website and then leave our website again.

Account creation: When you create an account on our website or place an order, Google Analytics collects this data.

Location: IP addresses are not logged or stored in Google Analytics. However

are used to derive location data shortly before the IP address is deleted.

Technical information: Technical information includes your browser type, your internet provider or your screen resolution.

Source of origin: Google Analytics or we are of course also interested in which website or which advertisement you came to our site from.

Other data includes contact details, any ratings, playing media (e.g. when you play a video on our site), sharing content via social media or adding it to your favorites. The list is not exhaustive and is only intended to provide a general overview of data storage by Google Analytics.

How long and where is the data stored?

Google has distributed its servers all over the world. Here you can read exactly where the Google data centers are located: <https://www.google.com/about/datacenters/locations/?hl=de>

Your data is distributed on different physical data carriers. This has the advantage that the data can be accessed more quickly and is better protected against manipulation. There are appropriate emergency programs for your data in every Google data center. If, for example, the hardware at Google fails or natural disasters paralyze servers, the risk of a service interruption at Google remains low.

The retention period of the data depends on the properties used. The storage period is always defined separately for each individual property. Google Analytics offers us four options to control the storage period:

- 2 months: this is the shortest storage period.
- 14 months: by default, GA4 stores the data for 14 months.
- 26 months: you can also save the data for 26 months.
- Data is only deleted when we delete it manually

In addition, there is also the option that data will only be deleted if you no longer visit our website within the period selected by us. In this case, the retention period is reset each time you visit our website again within the specified period.

Once the specified period has expired, the data will be deleted once a month. This retention period applies to your data linked to cookies, user recognition and advertising IDs (e.g. DoubleClick domain cookies). Reporting results are based on aggregated data and are stored independently of user data. Aggregated data is an amalgamation of individual data into a larger unit.

How can I delete my data or prevent data storage?

Under European Union data protection law, you have the right to request information about your

data, update, delete or restrict it. You can use the browser add-on to deactivate Google Analytics JavaScript (analytics.js, gtag.js) to prevent Google Analytics 4 from using your data. You can download and install the browser add-on at <https://tools.google.com/dlpage/gaoptout?hl=de>. Please note that this add-on only deactivates data collection by Google Analytics.

If you want to deactivate, delete or manage cookies, you will find the relevant links to the instructions for the most popular browsers in the "Cookies" section.

Legal basis

The use of Google Analytics requires your consent, which we have obtained with our cookie pop-up. According to **Art. 6 para. 1 lit. a GDPR (consent)**, this consent constitutes the legal basis for the processing of personal data, as may occur when it is collected by web analytics tools.

In addition to consent, we have a legitimate interest in analyzing the behavior of website visitors in order to improve our offer technically and economically. With the help of Google Analytics, we can detect errors on the website, identify attacks and improve efficiency. The legal basis for this is **Art. 6 para. 1 lit. f**

GDPR (legitimate interests). Nevertheless, we only use Google Analytics if you have given your consent.
have given their consent.

Google also processes your data in the USA, among other places. Google is an active participant in the EU-US Data Privacy Framework, which regulates the correct and secure transfer of personal data from EU citizens to the USA. You can find more information on this at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Google also uses so-called standard contractual clauses (= Art. 46 (2) and (3) GDPR). Standard Contractual Clauses (SCCs) 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 the EU-US Data Privacy Framework and the standard contractual 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 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: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

The Google Ads Data Processing Terms, which refer to the standard contractual clauses, can be found at <https://business.safety.google/intl/de/adsprocessorterms/>.

We hope we have been able to provide you with the most important information about data processing by Google Analytics. If you would like to find out more about the tracking service, we recommend these two links:

<https://marketingplatform.google.com/about/analytics/terms/de/> and <https://support.google.com/analytics/answer/6004245?hl=de>.

If you want to find out more about data processing, use the Google privacy policy at <https://policies.google.com/privacy?hl=de>.

Google Analytics reports on demographic characteristics and interests

We have activated the functions for advertising reports in Google Analytics. The reports on demographic characteristics and interests contain information on age, gender and interests. This allows us to get a better picture of our users without being able to assign this data to individual persons. You can find out more about the advertising functions at https://support.google.com/analytics/answer/3450482?hl=de_AT&utm_id=ad.

You can stop the use of the activities and information of your Google account under "Settings for advertising" at <https://adssettings.google.com/authenticated> via a checkbox.

Google Analytics in consent mode

Depending on your consent, your personal data will be processed by Google Analytics in the so-called consent mode. You can choose whether or not to consent to Google Analytics cookies. This also allows you to choose which of your data Google Analytics may process. This collected data is mainly used to measure user behavior on the website, to display targeted advertising and to provide us with web analytics reports. As a rule, you consent to data processing by Google via a cookie consent tool. If you do not consent to data processing, only aggregated data will be collected and processed. This means that data cannot be assigned to individual users and therefore no user profile is created for you. You can also only consent to statistical measurement. No personal data is processed and therefore not used for advertising or advertising success.

Google Analytics IP anonymization

We have implemented IP address anonymization from Google Analytics on this website. This function was developed by Google so that this website can comply with the applicable data protection regulations and recommendations of the local data protection authorities if they prohibit the storage of the full IP address. The anonymization or masking of the IP takes place as soon as the IP addresses arrive in the Google Analytics data collection network and before any storage or processing of the data takes place.


You can find more information on IP anonymization


at <https://support.google.com/analytics/answer/2763052?hl=de>.

Social media introduction


Social media privacy policy summary

 Affected parties: Visitors to the website

 Purpose: Presentation and optimization of our services, contact with visitors, interested parties, etc., advertising

 Processed data: Data such as telephone numbers, e-mail addresses, contact details, user behavior data, information about your device and your IP address.

You can find more details on this in the respective social media tool used.

 Storage duration: depending on the social media platforms used Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is social media?

In addition to our website, we are also active on various social media platforms. User data may be processed so that we can target users who are interested in us via the social networks. In addition, elements of a social media platform may also be embedded directly in our website. This is the case, for example, if you click on a social button on our website and are forwarded directly to our social media presence. Social media refers to websites and apps that registered members can use to produce content, share content openly or in specific groups and network with other members.

Why do we use social media?

For years, social media platforms have been the place where people communicate and get in touch online. With our social media presence, we can bring our products and services closer to interested parties. The social media elements integrated on our website help you to switch to our social media content quickly and without complications.

The data that is stored and processed through your use of a social media channel is primarily for the purpose of carrying out web analyses. The aim of these analyses is to be able to develop more precise and personalized marketing and advertising strategies.

Depending on your behavior on a social media platform, the evaluated data can be used to draw conclusions about your interests and create user profiles. This also enables the platforms to present you with customized advertisements. Cookies are usually set in your browser for this purpose, which store data on your usage behavior.

As a rule, we assume that we remain responsible under data protection law, even if we use the services of a social media platform. However, the European Court of Justice has ruled that in certain cases, the operator of the social media platform, together with

may be jointly responsible with us within the meaning of Art. 26 GDPR. If this is the case, we will point this out separately and work on the basis of an agreement to this effect. The essence of the agreement is then reproduced below for the platform concerned.

Please note that when using the social media platforms or our built-in elements, your data may also be processed outside the European Union, as many social media channels, such as Facebook or Twitter, are American companies. As a result, you may not be able to claim or enforce your rights in relation to your personal data as easily.

What data is processed?

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

All data that is collected via a social media platform is also stored on the provider's servers. This means that only the providers have access to the data and can provide you with the appropriate information or make changes.

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

Duration of data processing

We will inform you about the duration of data processing below if we have further information on this. For example, the social media platform Facebook stores data until it is no longer required for its own purposes. However, customer data that is compared with our own user data is deleted within two days. In general, we only process personal data for as long as is absolutely necessary for the provision of our services and products. If required by law, for example in the case of accounting, this storage period may be exceeded.

Right of objection

You also have the right and the option to withdraw your consent to the use of cookies or third-party providers such as embedded social media elements at any time. This works either via our cookie management tool or via other opt-out functions. For example, you can also prevent data collection by cookies by changing the settings in your

Manage, deactivate or delete cookies in your browser.

As social media tools may use cookies, we also recommend that you read our general privacy policy on cookies. To find out exactly which of your data is stored and processed, you should read the privacy policies of the respective tools.

Legal basis

If you have consented to your data being processed and stored by integrated social media elements, this consent is the legal basis for data processing (**Art. 6 para. 1 lit. a GDPR**). In principle, your data will be processed if

consent, also on the basis of our legitimate interest (**Art. 6 para. 1 lit. f GDPR**)


We store and process your data for the purpose of fast and good communication with you or other customers and business partners. Nevertheless, we only use these tools if you have given your consent. Most social media platforms also set cookies in your browser to store data. We therefore recommend that you read our data protection text on cookies carefully and consult the privacy policy or cookie guidelines of the respective service provider.


Information on specific social media platforms - if available - can be found in the following sections.

Facebook privacy policy


Facebook privacy policy summary

 Affected parties: 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.

You can find more details 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 GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What are Facebook tools?

We use selected tools from Facebook on our website. Facebook is a social media network of Meta Platforms Inc. or, for the European region, Meta Platforms Ireland Limited, 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 and forwarded from you via our embedded Facebook elements or via our Facebook page (fan page), both we and Facebook Ireland Ltd. are responsible for this. Facebook is solely responsible for the further processing of this data.

Responsibility. Our joint obligations have also been enshrined in a publicly accessible agreement at 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 website. 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 address 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.

In addition to many other products, Facebook also offers the so-called "Facebook Business Tools". This is the official term used by Facebook. However, as the term is hardly known, we have decided to simply call them Facebook tools. These include, among others:

- 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 expands services and has the ability to obtain information about user activity outside of Facebook.

Why do we use Facebook tools on our website?

We only want to show our services and products to people who are really interested in them. With the help of advertisements (Facebook ads), we can reach precisely these people. However, Facebook needs information about people's wishes and needs in order to show users suitable advertising. So the

We provide Facebook with information about user behavior (and contact details) on our website. As a result, Facebook collects better user data and can display suitable advertising about our products and services to interested people. The tools thus enable customized advertising campaigns on Facebook.

Facebook calls data about your behavior on our website "event data". This is also

used for measurement and analysis services. Facebook can thus on our behalf "Campaign reports" on the impact of our advertising campaigns. We also use analytics to gain a better insight into how you use our services, website or products. This allows us to optimize your user experience on our website with some of these tools. For example, you can use the social plug-ins 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) can be sent to Facebook. Depending on the tools used, customer data such as name, address, telephone number and IP address may be sent.

Facebook uses this information to match the data with the data it has about you (if you are a Facebook member). Before customer data is transmitted to Facebook, it is hashed. This means that a data set of any size is transformed into a character string. This is also used to encrypt data.

In addition to the 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 the company has explicit permission or is legally obliged to do so. "Event data" can also be linked to contact details. This allows Facebook to offer better personalized advertising. After the aforementioned matching process, Facebook deletes the contact data again.

In order to deliver optimized ads, Facebook only uses the 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 that are used to store data or information in browsers. Depending on the tools used and whether you are a Facebook member, different numbers of cookies are stored in your browser. We go into more detail about individual Facebook cookies in the descriptions of the individual Facebook tools. 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?

In principle, Facebook stores data until it is no longer needed for its own services and Facebook products. Facebook has servers all over the world where its data is stored. However, customer data is deleted within 48 hours after it has been compared with the company's own user data.

How can I delete my data or prevent data storage?

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

The data will only be completely deleted if you delete your Facebook account completely. And this is how deleting your Facebook account works:

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

The data that Facebook receives via our site is stored using cookies (e.g. for social plugins). You can deactivate, delete or manage individual or all cookies in your browser. Depending on which browser you use, this works in different ways. In the "Cookies" section, you will find the relevant links to the instructions for the most popular browsers.

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

Legal basis

If you have consented to your data being processed and stored by integrated Facebook tools, this consent is the legal basis for data processing (**Art. 6 para. 1 lit. a GDPR**). In principle, your data is also stored on

On the basis of our legitimate interest (**Art. 6 (1) (f) GDPR**) in a fast and secure stored and processed for good communication with you or other customers and business partners. Nevertheless, we only use these tools if you have given your consent. Most social media platforms also set cookies in your browser to store data. We therefore recommend that you read our privacy policy about cookies carefully and take a look at Facebook's privacy policy or cookie guidelines.

Facebook also processes your data in the USA, among other places. Facebook or Meta Platforms is an active participant in the EU-US Data Privacy Framework, which regulates the correct and secure transfer of personal data from EU citizens to the USA. You can find more information on this at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

In addition, Facebook uses so-called standard contractual clauses (= Art. 46 (2) and (3) GDPR). Standard Contractual Clauses (SCCs) have been approved by the EU Commission.

and are intended to ensure that your data complies with European data protection standards even if it is transferred to and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the standard contractual 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 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: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de


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


We hope we have provided you with the most important information about the use and data processing by the Facebook tools. If you would like to find out more about how Facebook uses your data, we recommend that you read the data policy at <https://www.facebook.com/privacy/policy/>.

Instagram privacy policy


Instagram privacy policy summary

 Affected parties: Visitors to the website

 Purpose: Optimization of our service performance

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

You can find more details below in the privacy policy.

 Storage period: until Instagram no longer needs the data for its purposes Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is Instagram?

We have integrated Instagram functions on our website. Instagram is a social media platform of the company Instagram LLC, 1601 Willow Rd, Menlo Park CA 94025, USA. Instagram has been a subsidiary of Meta Platforms Inc. since 2012 and is a Facebook product. Embedding Instagram content on our website is called embedding. This allows us to show you content such as buttons, photos or videos from Instagram directly on our website. When you visit web pages on our website that have an Instagram function integrated, data is transmitted to Instagram, stored and processed. Instagram uses the same systems and technologies as Facebook. Your data is therefore processed across all Facebook companies.

In the following, we want to give you a more detailed insight into why Instagram collects data, what data is involved and how you can largely control data processing. Since Instagram belongs to Meta Platforms Inc., we obtain our information from the Instagram guidelines on the one hand, but also from the Meta privacy policy itself on the other.

Instagram is one of the best-known social media networks in the world. Instagram combines the advantages of a blog with the benefits of audiovisual platforms such as YouTube or Vimeo. You can upload photos and short videos to "Insta" (as many users casually call the platform), edit them with various filters and also share them on other social networks. And if you don't want to be active yourself, you can also just follow other interesting users.

Why do we use Instagram on our website?

Instagram is the social media platform that has really gone through the roof in recent years. And of course we have also responded to this boom. We want you to feel as comfortable as possible on our website. That's why a varied presentation of our content is a matter of course for us. The embedded Instagram functions allow us to enrich our content with helpful, funny or exciting content from the Instagram world. As Instagram is a subsidiary of Facebook, the data collected can also be useful to us for personalized advertising on Facebook. This means that only people who are genuinely interested in our products or services receive our advertisements.

Instagram also uses the collected data for measurement and analysis purposes. We receive summarized statistics and thus more insight into your wishes and interests. It is important to note that these reports do not identify you personally.

What data is stored by Instagram?

When you visit one of our pages that has Instagram functions (such as Instagram images or plugins), your browser automatically connects to Instagram's servers. In the process, data is sent to Instagram, stored and processed. This happens regardless of whether you have an Instagram account or not. This includes information about our website, your computer, purchases made, advertisements you see and how you use our services. The date and time of your interaction with Instagram are also stored. If you have an Instagram account or are logged in, Instagram stores significantly more data about you.

Facebook distinguishes between customer data and event data. We assume that this is exactly the case with Instagram. Customer data includes, for example, name, address, telephone number and IP address. This customer data is only transmitted to Instagram once it has been hashed. Hashing means that a data record is converted into a character string. This allows the contact data to be encrypted. The "event data" mentioned above is also transmitted. By "event data", Facebook - and consequently Instagram - means data about your user behavior. Contact data may also be combined with event data. The contact data collected is compared with the data that Instagram already has about you.

The collected data is transmitted to Facebook via small text files (cookies), which are usually set in your browser. Depending on the Instagram functions used and whether

If you have an Instagram account yourself, different amounts of data are stored.

We assume that Instagram processes data in the same way as Facebook. This means that if you have an Instagram account or have visited www.instagram.com, Instagram has at least set a cookie. If this is the case, your browser sends information to Instagram via the cookie as soon as you come into contact with an Instagram function.

This data is deleted or anonymized after 90 days at the latest (after reconciliation). Although we have studied Instagram's data processing intensively, we cannot say exactly what data Instagram collects and stores.

Below we show you the minimum cookies that are set in your browser when you click on an Instagram function (such as a button or an Insta image). In our test, we assume that you do not have an Instagram account. If you are logged in to Instagram, significantly more cookies will of course be set in your browser.

These cookies were used in our test:

Name: csrftoken

Value: ""

Purpose: This cookie is most likely set for security reasons to prevent falsification of requests. However, we were unable to find out more about this.

Expiration date: after one year

Name: mid

Value: ""

Purpose: Instagram sets this cookie to optimize its own services and offers on and off Instagram. The cookie defines a unique user ID.

Expiration date: after the end of the session

Name: fbsr_112758054124024

Value: not specified

Purpose: This cookie stores the log-in request for users of the Instagram app.

Expiration date: after the end of the session

Name: rur

Value: ATN

Purpose: **This is** an Instagram cookie that ensures functionality on Instagram.

Expiration date: after the end of the session

Name: urlgen

Wert: "{\"194.96.75.33\": 1901}:1iEtYv:Y833k2_UjKvXgYe112758054\"

Purpose: This cookie is used for Instagram's marketing purposes.

Expiration date: after the end of the session

Note: We cannot claim completeness here. Which cookies are set in individual cases depends on the embedded functions and your use of Instagram.

How long and where is the data stored?

Instagram shares the information received between the Facebook companies with external partners and with people you connect with worldwide. Data processing is carried out in compliance with our own data policy. For security reasons, among others, your data is distributed on Facebook servers around the world. Most of these servers are located in the USA.

How can I delete my data or prevent data storage?

Thanks to the General Data Protection Regulation, you have the right to access, portability, rectification and erasure of your data. You can manage your data in the Instagram settings. If you want to completely delete your data on Instagram, you must permanently delete your Instagram account.

And this is how deleting your Instagram account works:

First open the Instagram app. On your profile page, go to the bottom and click on "Help area". You will now be taken to the company's website. On the website, click on "Manage your account" and then on "Delete your account".

If you delete your account completely, Instagram will delete posts such as your photos and status updates. Information that other people have shared about you does not belong to your account and is therefore not deleted.

As mentioned above, Instagram stores your data primarily via cookies. You can manage, deactivate or delete these cookies in your browser. Depending on your browser, the management always works a little differently. In the "Cookies" section, you will find the relevant links to the instructions for the most popular browsers.

You can also set up your browser so that you are always informed when a cookie is to be set. Then you can always decide individually whether you want to allow the cookie or not.

Legal basis

If you have consented to your data being processed and stored by integrated social media elements, this consent is the legal basis for data processing (**Art. 6 para. 1 lit. a GDPR**). In principle, your data is also stored on

On the basis of our legitimate interest (**Art. 6 (1) (f) GDPR**) in a fast and secure stored and processed for good communication with you or other customers and business partners. Nevertheless, we only use the integrated social media elements if you have given your consent. Most social media platforms also set cookies in your browser.

Browser to store data. We therefore recommend that you read our data protection text on cookies carefully and consult the privacy policy or cookie guidelines of the respective service provider.

Instagram also processes your data in the USA, among other places. Instagram or Meta Platforms is an active participant in the EU-US Data Privacy Framework, which regulates the correct and secure transfer of personal data of EU citizens to the USA. You can find more information on this at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.


Instagram also uses so-called standard contractual clauses (= Art. 46 (2) and (3) GDPR). Standard Contractual Clauses (SCCs) 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 the EU-US Data Privacy Framework and the Standard Contractual Clauses, Instagram 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 others: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

We have tried to provide you with the most important information about data processing by Instagram. You can find out more about Instagram's data policy at <https://privacycenter.instagram.com/policy/>.


Online Marketing Introduction

Online marketing privacy policy summary

 Affected parties: Visitors to the website

 Purpose: Evaluation of visitor information to optimize the website. Processed data: Access statistics, the data such as locations of access, device data, Access duration and time, navigation behavior, click behavior and IP addresses. Personal data such as name or e-mail address can also be processed.

You can find more details on this in the respective online marketing tool used.

 Storage period: depending on the online marketing tools used Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit.f GDPR (legitimate interests)

What is online marketing?

Online marketing refers to all measures that are carried out online in order to achieve marketing goals such as increasing brand awareness or closing a deal. Our online marketing measures are also aimed at drawing people's attention to our website. We therefore use online marketing to show our offer to many interested people. This usually involves online advertising, content marketing or search engine optimization. So that we can use online marketing efficiently and

personal data is also stored and processed so that we can use our online marketing measures in a targeted manner. On the one hand, the data helps us to show our content only to those people who are actually interested in it and, on the other hand, we can measure the advertising success of our online marketing measures.

Why do we use online marketing tools?

We want to show our website to everyone who is interested in what we have to offer. We are aware that this is not possible without deliberate measures. That's why we do online marketing. There are various tools that make it easier for us to work on our online marketing measures and also use data to constantly provide suggestions for improvement. This allows us to tailor our campaigns more precisely to our target group. The purpose of these online marketing tools is ultimately to optimize our offering.

What data is processed?

To ensure that our online marketing works and the success of the measures can be measured, user profiles are created and data is stored in cookies (small text files), for example. With the help of this data, we can not only place traditional advertising, but also display our content directly on our website in the way you prefer. There are various third-party tools that offer these functions and collect and store your data accordingly. For example, the named cookies store which web pages you have visited on our website, how long you have viewed these pages, which links or buttons you click or which website you came to us from. Technical information may also be stored. For example, your IP address, which browser you use, from which device you visit our website or the time when you accessed our website and when you left it again. If you have agreed that we may also determine your location, we may also store and process this.

Your IP address is stored in pseudonymized form (i.e. shortened). Unique data that directly identifies you as a person, such as your name, address or e-mail address, is also only stored in pseudonymized form as part of the advertising and online marketing process. This means that we cannot identify you as a person, but only the pseudonymized information stored in the user profiles.

The cookies may also be used, analyzed and used for advertising purposes on other websites that work with the same advertising tools. The data can then also be stored on the servers of the advertising tool providers.

In exceptional cases, unique data (name, email address, etc.) may also be stored in the user profiles. This storage occurs, for example, if you are a member of a social media channel that we use for our online marketing measures and the network links previously received data to the user profile.

With all the advertising tools we use that store data from you on their servers, we only ever receive summarized information and never data that you provide as an individual.

recognizable. The data only shows how well advertising measures worked. For example, we can see which measures prompted you or other users to visit our website and purchase a service or product there. Based on the analyses, we can improve our advertising offer in the future and adapt it even more precisely to the needs and wishes of interested persons.

Duration of data processing

We will inform you about the duration of data processing below if 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. Data stored in cookies is stored for different lengths of time. Some cookies are deleted as soon as you leave the website, while others may be stored in your browser for several years. You can usually find detailed information about the individual cookies used by the provider in the respective data protection declarations of the individual providers.

Right of objection

You also have the right and the option to withdraw your consent to the use of cookies or third-party providers at any time. This works either via our cookie management tool or via other opt-out functions. For example, you can also prevent data collection by cookies by managing, deactivating or deleting cookies in your browser. The lawfulness of the processing until the revocation remains unaffected.

As cookies can generally be used with online marketing tools, we also recommend that you read our general privacy policy on cookies. To find out exactly which of your data is stored and processed, you should read the privacy policies of the respective tools.

Legal basis

If you have consented to the use of third-party providers, the legal basis for the corresponding data processing is this consent. According to **Art. 6 para. 1 lit. a GDPR (consent)**, this consent constitutes the legal basis for the processing of personal data, as may occur when it is collected by online marketing tools.

We also have a legitimate interest in measuring online marketing measures in anonymized form in order to optimize our offer and our measures with the help of the data obtained. The legal basis for this is **Art. 6 para. 1 lit. f**

GDPR (legitimate interests). Nevertheless, we only use the tools insofar as you have a have given their consent.

Information on special online marketing tools - if available - can be found in the following sections.

Facebook Custom Audiences privacy policy

We use Facebook Custom Audiences, a server-side event tracking tool, on our website. The service provider is the American company Meta Platforms Inc. Meta Platforms Ireland Limited (4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland) is responsible for the European region.

Facebook also processes your data in the USA, among other places. Facebook or Meta Platforms is an active participant in the EU-US Data Privacy Framework, which regulates the correct and secure transfer of personal data from EU citizens to the USA. You can find more information on this at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

In addition, Facebook uses so-called standard contractual clauses (= Art. 46 (2) and (3) GDPR). Standard Contractual Clauses (SCCs) 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 the EU-US Data Privacy Framework and the standard contractual 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 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: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de


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

You can find out more about the data processed through the use of Facebook Custom Audiences in the privacy policy at <https://www.facebook.com/about/privacy>.

LinkedIn Insight Tag Privacy Policy

LinkedIn Insight Tag Privacy Policy Summary

 Affected parties: Visitors to the website

 Purpose: Evaluation of visitor information to optimize the website. Processed data: Access statistics, the data such as locations of access, device data,

Access duration and time, navigation behavior, click behavior and IP addresses. More details on this can be found below and in LinkedIn's privacy policy.

 Storage period: direct identifiers by LinkedIn Insight tag are removed within seven days

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

What is LinkedIn Insight Tag?

We use the conversion tracking tool LinkedIn Insight Tag on our website. Service provider

is the American company LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA. LinkedIn Ireland Unlimited (Wilton Place, Dublin 2, Ireland) is responsible for data protection aspects in the European Economic Area (EEA), the EU and Switzerland.

By embedding the tracking tool, data can be sent to LinkedIn, stored and processed there. In this privacy policy, we want to inform you about what data is involved, how the network uses this data and how you can manage or prevent data storage.

LinkedIn is the largest social network for business contacts. Unlike Facebook, for example, the company focuses exclusively on establishing business contacts. Companies can present services and products on the platform and establish business relationships. Many people also use LinkedIn to look for jobs or to find suitable employees for their own company. In Germany alone, the network has over 11 million members. In Austria, there are around 1.3 million.

LinkedIn's conversion tracking tool is a small JavaScript code that we have integrated into our website. This function helps us to better adapt our advertising offer to your interests and needs. In the following article, we will go into more detail about why we use LinkedIn Insight Tag, what data is stored in the process and how you can prevent this data storage.

Why do we use LinkedIn Insight tag on our website?

We use LinkedIn Insight Tag to draw attention to our offer. The aim is to ensure that our advertising campaigns only reach people who are interested in our offers. With the LinkedIn Insight tag, we can collect detailed information about your website behavior if you are also a LinkedIn member. We can also see which keywords, ads, ad groups and campaigns on LinkedIn lead to the desired customer actions. We see how many customers interact with our ads on a device and then perform a conversion. This data allows us to calculate our cost-benefit factor, measure the success of individual advertising measures and consequently optimize our online marketing measures. We can also use the data obtained to make our website more interesting for you and adapt our advertising offer even more individually to your needs.

What data is stored by LinkedIn Insight Tag?

As mentioned above, we have integrated a conversion tracking tag or code snippet on our website in order to better analyze certain user actions. If you click on one of our LinkedIn ads, a cookie may be stored on your computer (usually in the browser) or mobile device. In principle, LinkedIn processes data using a combination of cookies and server-side functions.

As soon as you complete an action on the website, LinkedIn recognizes the cookie and saves it.

Your action as a so-called conversion. As long as you are browsing our website, we and LinkedIn recognize that you have found us via our LinkedIn ad. The cookie is read and sent back to LinkedIn with the conversion data. It is also possible that other cookies are used to measure conversions.

In addition to your IP address, the URL, referrer URL, device and browser properties and the timestamp are also stored. The IP address is considered personal data and is shortened or hashed by LinkedIn.

You may be wondering what conversions actually are. A conversion occurs when you go from being a purely interested website visitor to an acting visitor. This always happens when you click on our ad and then take another action, such as visiting our website or purchasing a product. We use LinkedIn's conversion tracking tool to record what happens after a user clicks on our LinkedIn ad. For example, we can see whether products are purchased, services are used or whether you have signed up for our newsletter.

In addition, demographic data that you have entered in your LinkedIn profile can also be processed. This may include information about your profession, geographical location, industry or company.

We receive a report from LinkedIn with statistical evaluations. For example, we find out the total number of users who clicked on our ad and we can see which advertising measures were well received.

How long and where is the data stored?

In principle, LinkedIn retains your personal data for as long as the company considers it necessary to provide its own services. However, LinkedIn deletes your personal data when you delete your account. In some exceptional cases, LinkedIn retains some data in aggregated and anonymized form even after you delete your account.

Direct identifiers by LinkedIn Insight tag are removed within seven days to pseudonymize the data. The resulting pseudonymized data will be deleted within 180 days.

The data is stored on various servers in America and presumably also in Europe.

How can I delete my data or prevent data storage?

You have the right to access and delete your personal data at any time.

You have the option not to participate in LinkedIn's conversion tracking. If you do

If you deactivate the Google Conversion Tracking cookie via your browser or do not consent to data processing via the Consent Manager (pop-up), you are blocking conversion tracking. In this case, you will not be included in the statistics of the tracking tool. You can change the cookie settings in your browser at any time. This works slightly differently for each browser. In the "Cookies" section, you will find the relevant links to the instructions for the most popular browsers.

You can also manage, change and delete your data in your LinkedIn account. You can also request a copy of your personal data from LinkedIn.

How to access the account data in your LinkedIn profile:

In LinkedIn, click on your profile icon and select the "Settings and privacy" section. Now click on "Privacy" and then on "Change" in the "How LinkedIn uses your data" section. In just a short time, you can download selected data about your web activity and account history.

Legal basis

If you have consented to the use of the LinkedIn Insight tag, the legal basis for the corresponding data processing is this consent. According to Art. 6 para. 1 lit. a GDPR (consent), this consent constitutes the legal basis for the processing of personal data, as may occur when the LinkedIn Insight tag is collected.

We also have a legitimate interest in using the LinkedIn Insight tag to optimize our online service and our marketing measures. The legal basis for this is Art. 6 para. 1 lit. f GDPR (legitimate interests). Nevertheless, we only use the LinkedIn Insight tag if you have given your consent.

LinkedIn also processes your data in the USA, among other places. We would like to point out that, in the opinion of the European Court of Justice, there is currently no adequate level of protection for data transfers to the USA. This may entail various risks for the legality and security of data processing.

LinkedIn uses so-called standard contractual clauses (= Art. 46. para. 2 and 3 GDPR) as the basis for data processing with recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, i.e. in particular in the USA) or data transfer to these countries. Standard Contractual Clauses (SCCs) 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 and stored in third countries (such as the USA). Through these clauses, LinkedIn 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


You can find more information on LinkedIn's standard contractual clauses at <https://de.linkedin.com/legal//dpa> or <https://www.linkedin.com/legal//eu-sccs>


You can find out more about LinkedIn Insight Tag at <https://www.linkedin.com/help/linkedin/answer/a427660>. You can also find out more about the data processed through the use of LinkedIn Insight Tag in the privacy policy at <https://de.linkedin.com/legal/privacy-policy>.


Cookie Consent Management Platform Introduction

Cookie Consent Management Platform Summary

 Affected: Website visitors

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

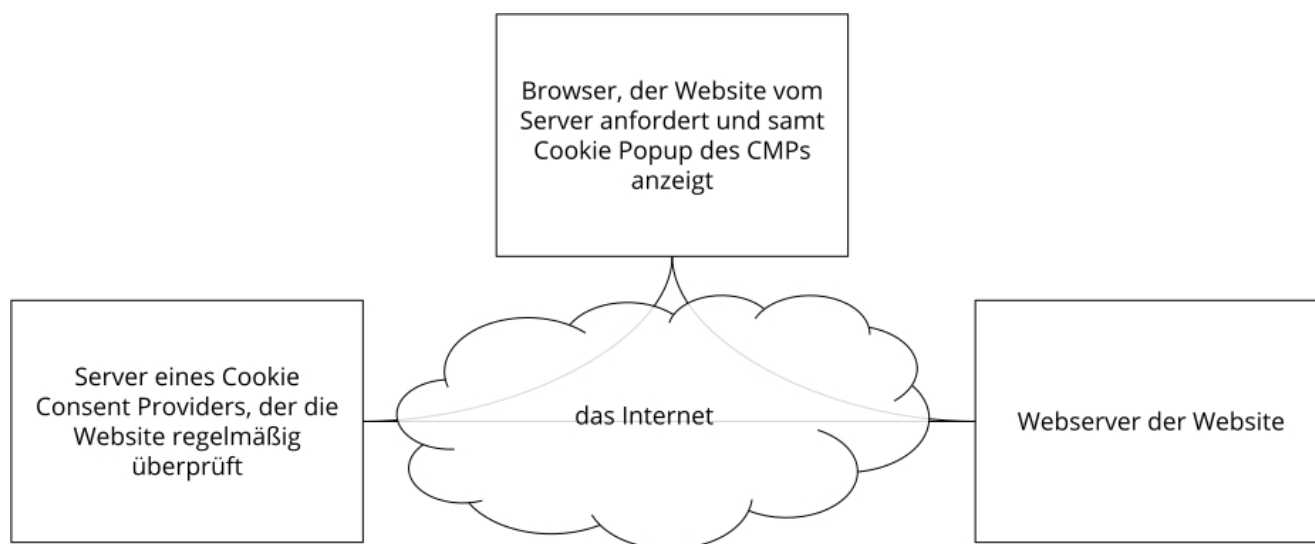
 Processed data: Data for managing the cookie settings such as IP address, time of consent, type of consent, individual consents. You can find more details on this in the respective tool used.

 Storage duration: Depends on the tool used, you have to be prepared for periods of 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 makes it easier for us and you to handle scripts and cookies correctly and securely. The software automatically creates a cookie pop-up, scans and checks all scripts and cookies, provides you with the cookie consent required under data protection law and helps us and you to keep track of all cookies. Most cookie consent management tools identify and categorize all existing cookies. As a website visitor, you then decide for yourself whether and which scripts and cookies you allow or do not allow. The following graphic shows the relationship between browser, web server and CMP.



Why do we use a cookie management tool?

Our aim is to offer you the best possible transparency in the area of data protection. We are also legally obliged to do so. We want to provide you with as much information as possible about all tools and all cookies that can store and process your data. It is also your right to decide for yourself which cookies you accept and which you do not. In order to grant you this right, we first need to know exactly which cookies have landed 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 about them. You can then accept or reject cookies via the consent system.

What data is processed?

As part of our cookie management tool, you can manage each individual cookie yourself and have complete control over the storage and processing of your data. The declaration of your consent is stored so that we do not have to ask you every time you visit our website and we can also prove your consent if required by law. This is stored either in an opt-in cookie or on a server. The storage period of your cookie consent varies depending on the provider of the cookie management tool. In most cases, this data (e.g. 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 if 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. Data stored in cookies is stored for different lengths of time. Some cookies are deleted as soon as you leave the website, while others can be stored in your browser for several years.

be stored in your browser. The exact duration of data processing depends on the tool used, but in most cases you should be prepared for a storage period of several years. You can usually find precise information about the duration of data processing in the respective data protection declarations of the individual providers.

Right of objection

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

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


Legal basis


If you consent to cookies, your personal data will be processed and stored via these cookies. If we are permitted to use cookies on the basis of your **consent** (Article 6(1)(a) GDPR), this consent is also the legal basis for the use of cookies and the processing of your data. Cookie consent management platform software is used to manage your consent to cookies and to enable you to give your consent. The use of this software enables us to operate the website in an efficient and legally compliant manner, which constitutes a **legitimate interest** (Article 6(1)(f) GDPR).

Security & Anti-Spam


Security & Anti-Spam Privacy Policy Summary

 Data subject: Visitors to the website

 Purpose: Cybersecurity

 Processed data: Data such as your IP address, name or technical data such as browser version

You can find more details on this below and in the individual data protection texts.

 Storage period: Most of the data is stored until it is no longer required for the fulfillment of the service

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

What is security & anti-spam software?

With so-called security and anti-spam software, you and we can protect ourselves from various spam or phishing emails and possible other cyberattacks. Spam refers to advertising emails from a mass mailing that you did not request yourself. Such emails are also known as data junk and can also cause costs. Phishing emails, on the other hand, are messages that aim to gain trust via fake messages or websites.

to gain access to personal data. Anti-spam software usually protects against unwanted spam messages or malicious emails that could introduce viruses into our system. We also use general firewall and security systems to protect our computers from unwanted network attacks.

Why do we use security & anti-spam software?

We attach great importance to security on our website. After all, it's not just about our security, but above all about yours. Unfortunately, cyber threats are now part of everyday life in the world of IT and the Internet. Hackers often try to steal personal data from an IT system with the help of a cyber attack. And that is why a good defense system is absolutely essential. A security system monitors all incoming and outgoing connections to our network or computer. To achieve even greater security against cyber attacks, we also use other external security services in addition to the standardized security systems on our computer. This prevents unauthorized data traffic and protects us from cybercrime.

What data is processed by security & anti-spam software?

Exactly which data is collected and stored depends of course on the respective service. However, we always strive to use only programs that collect data very sparingly or only store data that is necessary for the performance of the service offered. In principle, the service may store data such as name, address, IP address, e-mail address and technical data such as browser type or browser version. Any performance and log data may also be collected in order to detect possible incoming threats in good time. This data is processed as part of the services and in compliance with the applicable laws. This also includes the GDPR for US providers (via the standard contractual clauses). In some cases, these security services also work with third-party providers who may store and/or process data under instructions and in accordance with the data protection guidelines and other security measures. Data is usually stored via cookies.

Duration of data processing

We will inform you about the duration of data processing below if we have further information on this. For example, security programs store data until you or we revoke the data storage. In general, personal data is only stored for as long as is absolutely necessary for the provision of the services. Unfortunately, in many cases we do not receive precise information from the providers about the length of storage.

Right of objection

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

manage, deactivate or delete.

As such security services may also use cookies, we recommend that you read our general privacy policy on cookies. To find out exactly which of your data is stored and processed, you should read the privacy policies of the respective tools.

Legal basis

We use the security services mainly on the basis of our legitimate interests (Art. 6 para. 1 lit. f GDPR) in a good security system against various cyber attacks.

Certain processing operations, in particular the use of cookies and the use of security functions, require your consent. If you have consented to your data being processed and stored by integrated security services, this consent is the legal basis for data processing (Art. 6 para. 1 lit. a GDPR). Most of the services we use set cookies in your browser to store data. We therefore recommend that you read our data protection text on cookies carefully and view the privacy policy or cookie guidelines of the respective service provider.


Information on special tools - if available - can be found in the following sections.

Google reCAPTCHA privacy policy

Google reCAPTCHA privacy policy summary

 Affected parties: Visitors to the website

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

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

You can find more details below in this privacy policy.

 Storage duration: depending on the stored data

Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (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 Google Inc. For the European region, 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 person and not a robot or other spam software. By spam we mean any unsolicited information that is sent to us electronically. With the classic CAPTCHAs, you usually had to solve text or picture puzzles to verify your identity. With reCAPTCHA from Google, we don't usually have to bother you with such puzzles. In most cases, all you have to do is tick a box to confirm that you are not a bot. With the new Invisible reCAPTCHA

version, you no longer even need to check a box. You can find out exactly how this works and, above all, which data is used for this in the course of this privacy policy.

reCAPTCHA is a free captcha service from Google that protects websites from spam software and misuse by non-human visitors. This service is most commonly used when you fill out forms on the Internet. A Captcha service is a type 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 the computer scientist Alan Turing), a human determines the difference between a bot and a human. With captchas, this is also done by a computer or a software program. Classic captchas work with small tasks that are easy for humans to solve but present considerable difficulties for machines. With reCAPTCHA, you no longer have to actively solve puzzles. The tool uses modern risk techniques to distinguish humans from bots. All you have to do here is tick the "I am not a robot" text field, and with Invisible reCAPTCHA even this is no longer necessary. With reCAPTCHA, a JavaScript element is integrated into the source code and then the tool runs in the background and analyzes your user behaviour. The software calculates a so-called captcha score from these user actions. Google uses this score to calculate the probability that you are human even before you enter the captcha. reCAPTCHA or captchas in general are always used when bots could manipulate or abuse certain actions (e.g. registrations, surveys, etc.).

Why do we use reCAPTCHA on our website?

We only want to welcome people of flesh and blood on our site. Bots and spam software of all kinds can safely stay at home. That's why we do everything we can to protect ourselves and offer you the best possible user-friendliness. 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 a human being. reCAPTCHA therefore serves 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 subsequently "spam" forums or blogs with unwanted advertising content. With reCAPTCHA, we can prevent such bot attacks.

What data is stored by reCAPTCHA?

reCAPTCHA collects personal data from users in order to determine whether the actions on our website actually originate from people. The IP address and other data that Google requires for the reCAPTCHA service may therefore be sent to Google. IP addresses are almost always truncated within the member states of the EU or other signatory states to the Agreement on the European Economic Area before the data is sent to a server in the USA. The IP address is not combined with other Google data 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.) have already been placed on your browser. Then reCAPTCHA places an additional cookie in your browser and captures a snapshot of your

browser window.

The following list of collected browser and user data does not claim to be exhaustive. 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 your computer to operate. Common 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 saved)
- 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 enables websites to adapt to the user. JavaScript objects can collect all kinds of data under one name)
- Screen resolution (indicates 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, you don't even have to check the box and the entire recognition process runs in the background. Google does not tell you in detail exactly how much and what data it stores.

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-112758054-8

Purpose: This cookie is set by the company DoubleClick (also owned by Google) to register and report the actions of a user on the website in dealing with advertisements. This allows the effectiveness of advertising to be measured and appropriate optimization measures to 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. The cookie can also be used to prevent a user from seeing the same ad more than once.

Expiration date: after one month

Name: ANID

Wert: U7j1v3dZa1127580540xgZFmiqWppRWKOr

Purpose: We were unable to find out much information about this cookie. In Google's privacy policy, the cookie is mentioned in connection with "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.de+20150628-20-0

Purpose: The cookie stores the status of a user's consent to the use of various Google services. CONSENT is also used for security purposes to verify users, prevent fraudulent login information and protect user data from unauthorized attacks.

Expiration date: after 19 years

Name: NID

Wert: 0WmuWqy112758054zILzqV_nmt3sDXwPeM5Q

Intended use: NID is used by Google to customize advertisements to your Google searches. With the help of the cookie, Google "remembers" your most frequently entered search queries or your previous interaction with ads. So you always get customized ads. The cookie contains a unique ID to collect the user's personal settings for advertising purposes.

Expiration date: after 6 months

Name: DV

Wert: gEAABBCjJMXcl0dSAAAANbqc112758054-4

Intended use: As soon as you have checked the "I am not a robot" box, this cookie is set. The cookie is used by Google Analytics for personalized advertising. DV collects information in anonymized form and is also used to make user distinctions.

Expiration date: after 10 minutes

Note: This list cannot claim to be exhaustive, as experience has shown that Google changes its choice of cookies from time to time.

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 is not made clear by Google, even after repeated requests. 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 the European or American Google servers. The IP address that your browser transmits to Google is 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 Google 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. In principle, the data is automatically transmitted to Google as soon as you visit our website. To delete this data, you must [contact](https://support.google.com/?hl=de&tid=112758054) Google support at <https://support.google.com/?hl=de&tid=112758054>.

Therefore, when you use our website, you consent to Google LLC and its representatives automatically collecting, processing and using data.

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

Legal basis

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

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

Google also processes your data in the USA, among other places. Google is an active participant in the EU-US Data Privacy Framework, which regulates the correct and secure transfer of personal data from EU citizens to the USA. You can find more information on this at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Google also uses so-called standard contractual clauses (= Art. 46 (2) and (3) GDPR). Standard Contractual Clauses (SCCs) 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 the EU-US Data Privacy Framework and the standard contractual 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 USA. These clauses are based on an implementing decision of the EU Commission. You can find the decision and the corresponding


Standard contractual clauses, e.g. here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de


The Google Ads Data Processing Terms, which refer to the standard contractual clauses, can be found at <https://business.safety.google/intl/de/adsprocessorterms/>.


You can find out a little more about reCAPTCHA on Google's web developer page at <https://developers.google.com/recaptcha/>. Although Google goes into more detail here about the technical development of reCAPTCHA, you will search in vain for precise information about data storage and data protection issues. A good overview of the basic use of data at Google can be found in the company's own privacy policy at <https://policies.google.com/privacy>.

Audio & Video Introduction


Audio & Video Privacy Policy Summary

 Affected parties: Visitors to the website

 Purpose: Optimization of our service performance

 Processed data: Data such as contact details, user behavior data, information about your device and your IP address may be stored.

You can find more details on this below in the corresponding data protection texts.

 Storage period: Data is generally stored for as long as it is required for the purpose of the service

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

What are audio and video elements?

We have integrated audio and video elements on our website so that you can watch videos or listen to music/podcasts directly via our website. The content is provided by service providers. All content is therefore also obtained from the corresponding servers of the providers.

These are integrated functional elements from platforms such as YouTube, Vimeo or Spotify. The use of these portals is usually free of charge, but paid content can also be published. With the help of these integrated elements, you can listen to or view the respective content via our website.

If you use audio or video elements on our website, your personal data may also be transmitted to the service providers, processed and stored.

Why do we use audio & video elements on our website?

Of course we want to provide you with the best offer on our website. And we are aware that content is no longer just conveyed in text and static images. Instead of simply giving you a link to a video, we offer you audio and video content directly on our website.

Video formats that are entertaining or informative and ideally even both. This expands our service and makes it easier for you to access interesting content. In addition to our texts and images, we also offer video and/or audio content.

What data is stored by audio & video elements?

When you access a page on our website that has an embedded video, for example, your server connects to the server of the service provider. Your data is also transmitted to the third-party provider and stored there. Some data is collected and stored regardless of whether you have an account with the third-party provider or not. This usually includes your IP address, browser type, operating system and other general information about your end device. In addition, most providers also collect information about your web activity. This includes, for example, session duration, bounce rate, which button you clicked on or which website you used to access the service. All this information is usually stored using cookies or pixel tags (also known as web beacons).

Pseudonymized data is usually stored in cookies in your browser. You can always find out exactly which data is stored and processed in the privacy policy of the respective provider.

Duration of data processing

You can find out exactly how long the data is stored on the servers of the third-party providers either below in the data protection text of the respective tool or in the provider's privacy policy. In principle, personal data is only ever processed for as long as is absolutely necessary for the provision of our services or products. This generally also applies to third-party providers. In most cases, you can assume that certain data will be stored on the servers of third-party providers for several years. Data can be stored for different lengths of time, especially in cookies. Some cookies are deleted as soon as you leave the website, while others may be stored in your browser for several years.

Right of objection

You also have the right and the option to withdraw your consent to the use of cookies or third-party providers at any time. This works either via our cookie management tool or via other opt-out functions. For example, you can also prevent data collection by cookies by managing, deactivating or deleting cookies in your browser. The lawfulness of the processing until the revocation remains unaffected.

Since the integrated audio and video functions on our website usually also use cookies, you should also read our general privacy policy on cookies. You can find out more about the handling and storage of your data in the privacy policies of the respective third-party providers.

Legal basis


If you have consented to your data being processed by integrated audio and video


elements can be processed and stored, this consent is the legal basis for data processing (**Art. 6 para. 1 lit. a GDPR**). In principle, your data will also be processed on the basis of our legitimate interest (**Art. 6 para. 1 lit. f GDPR**) in a fast and efficient processing of your data. stored and processed for good communication with you or other customers and business partners. Nevertheless, we only use the integrated audio and video elements if you have given your consent.

YouTube privacy policy


YouTube privacy policy summary

 Affected parties: Visitors to the website

 Purpose: Optimization of our service performance

 Processed data: Data such as contact details, user behavior data, information about your device and your IP address may be stored.

You can find more details below in this privacy policy.

 Storage period: Data is generally stored for as long as it is required for the purpose of the service

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

What is YouTube?

We have integrated YouTube videos on our website. This allows us to present interesting videos directly on our site. YouTube is a video portal that has been a subsidiary of Google since 2006. The video portal is operated by YouTube, LLC, 901 Cherry Ave, San Bruno, CA 94066, USA. When you access a page on our website that has a YouTube video embedded, your browser automatically connects to the YouTube or Google servers. Various data is transmitted (depending on the settings). Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all data processing in Europe.

In the following, we would like to explain to you in more detail what data is processed, why we have integrated YouTube videos and how you can manage or delete your data.

On YouTube, users can watch, rate, comment on and upload videos for free. Over the last few years, YouTube has become one of the most important social media channels worldwide. To enable us to display videos on our website, YouTube provides a code snippet that we have integrated into our site.

Why do we use YouTube videos on our website?

YouTube is the video platform with the most visitors and the best content. We strive to offer you the best possible user experience on our website. And of course, interesting videos are a must. With the help of our embedded videos, we provide you with further helpful content in addition to our texts and images. In addition, our website is easier to find on the Google search engine thanks to the embedded videos.

Even if we place ads via Google Ads, Google can - thanks to the data collected - only show these ads to people who are interested in our offers.

What data is stored by YouTube?

As soon as you visit one of our pages that has a YouTube video embedded, YouTube sets at least one cookie that stores your IP address and our URL. If you are logged into your YouTube account, YouTube can usually assign your interactions on our website to your profile using cookies. This includes data such as session duration, bounce rate, approximate location, technical information such as browser type, screen resolution or your internet provider. Other data may include contact details, any ratings, the sharing of content via social media or adding to your favorites on YouTube.

If you are not logged into a Google account or a YouTube account, Google stores data with a unique identifier that is linked to your device, browser or app. For example, your preferred language setting is retained. But a lot of interaction data cannot be saved because fewer cookies are set.

In the following list, we show cookies that were set in the browser in a test. On the one hand, we show cookies that are set without a logged-in YouTube account. On the other hand, we show cookies that are set with a logged-in account. The list cannot claim to be complete because the user data always depends on the interactions on YouTube.

Name: YSC

Value: b9-CV6ojl5Y112758054-1

Purpose: This cookie registers a unique ID to store statistics of the video viewed.

Expiration date: after the end of the session

Name: PREF

Value: f1=50000000

Purpose: This cookie also registers your unique ID. Google receives statistics on how you use YouTube videos on our website via PREF.

Expiration date: after 8 months

Name: GPS

Value: 1

Purpose: This cookie registers your unique ID on mobile devices to track the GPS location.

Expiration date: after 30 minutes

Name: VISITOR_INFO1_LIVE

Value: 95Chz8bagyU

Purpose: This cookie attempts to estimate the user's bandwidth on our websites (with integrated YouTube video).

Expiration date: after 8 months

Other cookies that are set when you are logged in to your YouTube account:

Name: APISID

Wert: zILlvCIZSkqGsSwI/AU1aZI6HY7112758054-

Purpose: This cookie is used to create a profile of your interests. The data is used for personalized advertisements.

Expiration date: after 2 years

Name: CONSENT

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

Purpose: The cookie stores the status of a user's consent to the use of various Google services. CONSENT is also used for security purposes to check users and protect user data from unauthorized attacks.

Expiration date: after 19 years

Name: HSID

Value: AcRwpgUik9Dveht0I

Purpose: This cookie is used to create a profile of your interests. This data helps to display personalized advertising.

Expiration date: after 2 years

Name: LOGIN_INFO

Value: AFmmF2swRQIhALI6aL...

Purpose: This cookie stores information about your login data.

Expiration date: after 2 years

Name: SAPISID

Value: 7oaPxoG-pZsJuuF5/AnUdDUIsJ9iJz2vdM

Purpose: This cookie works by uniquely identifying your browser and device. It is used to create a profile of your interests.

Expiration date: after 2 years

Name: SID

Value: oQfNKjAsI112758054-

Purpose: This cookie stores your Google Account ID and your last login time in digitally signed and encrypted form.

Expiration date: after 2 years

Name: SIDCC

Value: AN0-TYuqub2JOcDTyL

Purpose: This cookie stores information about how you use the website and what advertisements you may have seen before visiting our site.

Expiration date: after 3 months

How long and where is the data stored?

The data that YouTube receives from you and processes is stored on Google servers. Most of these servers are located in America. At <https://www.google.com/about/datacenters/locations/?hl=de> you can see exactly where the Google data centers are located. Your data is distributed across the servers. This means that the data can be accessed more quickly and is better protected against manipulation.

Google stores the data collected for different lengths of time. You can delete some data at any time, others are automatically deleted after a limited time and others are stored by Google for a longer period of time. Some data (such as elements from "My activity", photos or documents, products) that are stored in your Google account remain stored until you delete them. Even if you are not signed in to a Google Account, you can delete some data associated with your device, browser or app.

How can I delete my data or prevent data storage?

In principle, you can delete data in your Google account manually. With the automatic deletion function for location and activity data introduced in 2019, information is stored for either 3 or 18 months, depending on your decision, and then deleted.

Regardless of whether you have a Google account or not, you can configure your browser so that cookies are deleted or deactivated by Google. Depending on which browser you use, this works in different ways. In the "Cookies" section, you will find the relevant links to the instructions for the most popular browsers.

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

Legal basis

If you have consented to your data being processed and stored by integrated YouTube elements, this consent is the legal basis for data processing (**Art. 6 para. 1 lit. a GDPR**). In principle, your data is also stored on

On the basis of our legitimate interest (**Art. 6 (1) (f) GDPR**) in a fast and secure stored and processed for good communication with you or other customers and business partners. Nevertheless, we only use the integrated YouTube elements if you have given your consent. YouTube also sets cookies in your browser to store data. We therefore recommend that you read our data protection text on cookies carefully and consult the privacy policy or cookie guidelines of the respective service provider.

YouTube also processes your data in the USA, among other places. YouTube and Google are active participants in the EU-US Data Privacy Framework, which regulates the correct and secure transfer of personal data from EU citizens to the USA. You can find more information on this at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.


Google also uses so-called standard contractual clauses (= Art. 46 (2) and (3) GDPR). Standard Contractual Clauses (SCCs) 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 the EU-US Data Privacy Framework and the standard contractual 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 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: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de


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


As YouTube is a subsidiary of Google, there is a joint privacy policy. If you would like to find out more about how your data is handled, we recommend that you read the privacy policy at <https://policies.google.com/privacy?hl=de>.

Web design introduction

Webdesign Privacy Policy Summary

 Affected parties: Visitors to the website

 Purpose: Improvement of the user experience

 Processed data: Which data is processed depends heavily on the services used. This usually involves the IP address, technical data, language settings, browser version, screen resolution and browser name. You can find more details on this in the respective web design tools used.

 Storage duration: depending on the tools used

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

What is web design?

We use various tools on our website that serve our web design. Web design is not, as is often assumed, just about making our website look pretty, but also about functionality and performance. But of course the right look of a website is also one of the major goals of professional web design. Web design is a branch of media design and deals with the visual as well as the structural and functional design of a website. The aim of web design is to improve your experience on our website. In web design jargon, this is referred to as user experience (UX) and usability. User experience refers to all impressions and experiences that website visitors have on a website. Usability is a sub-item of user experience. This is about the user-friendliness of a website. The main focus here is on ensuring that content, subpages or products are clearly structured and that you can find what you are looking for quickly and easily. To give you the best possible experience on our website

we also use so-called web design tools from third-party providers. Under the category In this privacy policy, "web design" therefore includes all services that improve the design of our website. This may include, for example, fonts, various plugins or other integrated web design functions.

Why do we use web design tools?

How you absorb information on a website depends very much on the structure, functionality and visual perception of the website. This is why good and professional web design has become increasingly important for us. We are constantly working on improving our website and also see this as an extended service for you as a website visitor. Furthermore, a beautiful and functioning website also has economic advantages for us.

After all, you will only visit us and take advantage of our services if you feel completely at ease.

What data is stored by web design tools?

When you visit our website, web design elements may be integrated into our pages that can also process data. Exactly what data is involved naturally depends heavily on the tools used. Below you can see exactly which tools we use for our website. For more detailed information about data processing, we recommend that you also read the privacy policies of the tools used. In most cases, this will tell you what data is processed, whether cookies are used and how long the data is stored. Fonts such as Google Fonts also automatically transmit information such as language settings, IP address, browser version, browser screen resolution and browser name to the Google servers.

Duration of data processing

How long data is processed is very individual and depends on the web design elements used. If cookies are used, for example, the storage period can be as short as one minute or as long as a few years. Please find out more about this. We recommend that you read our general text section on cookies as well as the data protection declarations of the tools used. There you can usually find out exactly which cookies are used and what information is stored in them. Google font files, for example, are stored for one year. This is to improve the loading time of a website. In principle, data is only stored for as long as is necessary to provide the service. Data can also be stored for longer if required by law.

Right of objection

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

delete. Among web design elements (mostly fonts), however, there is also data that cannot be deleted quite so easily. This is the case when data is automatically collected directly when a page is accessed and transmitted to a third-party provider (such as Google). In this case, please contact the support of the relevant provider. In the case of Google, you can contact support at <https://support.google.com/?hl=de>.

Legal basis

If you have consented to the use of web design tools, the legal basis for the corresponding data processing is this consent. According to Art. 6 para. 1 lit. a GDPR (consent), this consent constitutes the legal basis for the processing of personal data, as may occur when it is collected by web design tools. We also have a legitimate interest in improving the web design on our website. After all, only then can we provide you with an attractive and professional website. The legal basis for this is Art. 6 para. 1 lit. f GDPR (legitimate interests). Nevertheless, we only use web design tools if you have given your consent. We would like to emphasize this again here in any case.


Information on special web design tools - if available - can be found in the following sections.


Online map services Introduction

Online map services Privacy policy summary

 Affected parties: Visitors to the website

 Purpose: Improvement of the user experience

 Processed data: Which data is processed depends heavily on the services used. In most cases, this is IP address, location data, search items and/or technical data. You can find more details on this in the respective tools used.

 Storage duration: depending on the tools used

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

What are online map services?

We also use online map services for our website as an extended service. Google Maps is probably the service you are most familiar with, but there are also other providers that specialize in creating digital maps. Such services make it possible to display locations, route plans or other geographical information directly via our website. With an integrated map service, you no longer have to leave our website to view the route to a location, for example. In order for the online map to work on our website, map sections are integrated using HTML code. The services can then display street maps, the earth's surface or aerial or satellite images.

If you use the integrated map service, data is also transferred to the tool used and stored there. This data may also include personal data.

Why do we use online map services on our website?

Generally speaking, our aim is to offer you a pleasant time on our website. And of course, your time is only pleasant if you can easily find your way around our website and find all the information you need quickly and easily. That's why we thought that an online map system could significantly improve our service on the website. Without leaving our website, you can use the map system to easily view route descriptions, locations or even places of interest. Of course, it is also very practical that you can see at a glance where we are based so that you can find us quickly and safely. As you can see, there are simply many advantages and we clearly regard online map services on our website as part of our customer service.

What data is stored by online map services?

When you open a page on our website that has a built-in online map function, personal data may be transmitted to the respective service and stored there. In most cases, this is your IP address, which can also be used to determine your approximate location. In addition to the IP address, data such as search terms entered and longitude and latitude coordinates are also stored. If you enter an address for route planning, for example, this data is also stored. The data is not stored by us, but on the servers of the integrated tools. You can imagine it like this: You are on our website, but when you interact with a map service, this interaction actually happens on their website. In order for the service to function properly, at least one cookie is usually set in your browser. Google Maps, for example, also uses cookies to record user behaviour in order to optimize its own service and provide personalized advertising. You can find out more about cookies in our "Cookies" section.

How long and where is the data stored?

Each online map service processes different user data. If we have further information, we will inform you about the duration of data processing below in the relevant sections on the individual tools. In principle, personal data is only stored for as long as is necessary for the provision of the service. Google Maps, for example, stores certain data for a specified period of time, while you must delete other data yourself. With Mapbox, for example, the IP address is stored for 30 days and then deleted. As you can see, each tool stores data for different lengths of time. We therefore recommend that you take a close look at the privacy policies of the tools you use.

The providers also use cookies to store data on your user behavior with the map service. You can find more general information on cookies in our "Cookies" section, but you can also find out which cookies may be used in the data protection texts of the individual providers. In most cases, however, this is only an exemplary list and is not complete.

Right of objection

You always have the possibility and also the right to access your personal data and also to object to its use and processing. You can also withdraw the consent you have given us at any time. As a rule, the easiest way to do this is via the cookie consent tool. However, there are also other opt-out tools that you can use. You can also manage, delete or deactivate any cookies set by the providers you use yourself with just a few mouse clicks. However, some functions of the service may then no longer work as usual. How you manage cookies in your browser also depends on the browser you are using. In the section "Cookies" you will also find links to the instructions for the most important browsers.

Legal basis

If you have consented to the use of an online map service, the legal basis for the corresponding data processing is this consent. According to Art. 6 para. 1 lit. a GDPR (consent), this consent constitutes the legal basis for the processing of personal data, as may occur when it is collected by an online map service.


We also have a legitimate interest in using an online map service to optimize our service on our website. The legal basis for this is Art. 6 para. 1 lit. f GDPR (legitimate interests). However, we only ever use an online map service if you have given your consent. We would like to make this clear at this point.


Information on special online map services - if available - can be found in the following sections.

Google Maps privacy policy

Google Maps privacy policy summary

 Affected parties: Visitors to the website

 Purpose: Optimization of our service performance

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

You can find more details below in this privacy policy.

 Storage duration: depending on the stored data

Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (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. With Google Maps we can show you locations better and

so that we can adapt our service to your needs. By using Google Maps, data is transferred to Google and stored on Google servers. We would now like to 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 from Google. With Google Maps, you can search online for exact locations of cities, places of interest, accommodation or businesses using a PC, tablet or app. If companies are represented on Google My Business, further information about the company is displayed in addition to the location. To display directions, map sections of a location can be integrated into 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 on various locations. You can see at a glance where we are based. The directions always show you the best or quickest way to reach us. You can call up the directions for routes by car, public transport, on foot or by bike. For us, providing Google Maps is part of our customer service.

What data is stored by Google Maps?

In order for Google Maps to be able to offer its full service, the company must collect and store data from you. This includes the search terms entered, your IP address and also the latitude and longitude coordinates. If you use the route planner function, the start address you enter is also saved. However, this data storage takes place on the Google Maps websites. We can only inform you about this, but cannot influence it. 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 you with individual, personalized advertising.

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

Name: NID

Wert: 188=h26c1Ktha7fCQTx8rXgLyATyITJ112758054-5

Intended use: NID is used by Google to customize advertisements to your Google searches. With the help of the cookie, Google "remembers" your most frequently entered search queries or your previous interaction with ads. So you always get customized ads. The cookie contains a unique ID that Google uses to collect your personal settings for advertising purposes.

Expiration date: after 6 months

Note: We cannot guarantee the completeness of the stored data. Changes can never be ruled out, especially when using cookies. In order to identify the NID cookie, 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 of the servers are located in America. For this reason, your data is increasingly stored in the USA. You can find out exactly where the Google data centers are located here:

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

Google distributes the data on different data carriers. This means that the data can be accessed more quickly and is better protected against any attempts at manipulation. Each data center also has special emergency programs. If, for example, there are problems with the Google hardware or a natural disaster paralyzes the servers, the data is almost certainly still protected.

Google stores some data for a fixed period of time. For other data, Google only offers the option of deleting 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 or 18 months.

How can I delete my data or prevent data storage?

With the automatic deletion function for location and activity data introduced in 2019, location and web/app activity information is stored for either 3 or 18 months - depending on your decision - and then deleted. 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 from being recorded, you must pause the "Web and app activity" section in your Google account. Click on "Data and personalization" and then on the option "Activity setting". You can switch the activities on or off here.

You can also deactivate, delete or manage individual cookies in your browser. Depending on which browser you use, this always works slightly differently. In the "Cookies" section, you will find the relevant links to the instructions for the most popular browsers.

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

Legal basis

If you have consented to the use of Google Maps, the legal basis for the corresponding data processing is this consent. According to **Art. 6 para. 1 lit. a GDPR (consent)**, this consent constitutes the legal basis for the processing of personal data,

as it may occur when recorded by Google Maps.

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

Google also processes your data in the USA, among other places. Google is an active participant in the EU-US Data Privacy Framework, which regulates the correct and secure transfer of personal data from EU citizens to the USA. You can find more information on this at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Google also uses so-called standard contractual clauses (= Art. 46 (2) and (3) GDPR). Standard Contractual Clauses (SCCs) 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 the EU-US Data Privacy Framework and the standard contractual 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 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: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

The Google Ads Data Processing Terms, which refer to the standard contractual clauses, can be found at <https://business.safety.google/intl/de/adsprocessorterms/>.

If you would like to find out more about Google's data processing, we recommend that you read the company's own privacy policy at <https://policies.google.com/privacy?hl=de>.

Explanation of terms used

We always endeavor to write our privacy policy as clearly and comprehensibly as possible. However, this is not always easy, especially when it comes to technical and legal topics. It often makes sense to use legal terms (such as personal data) or certain technical terms (such as cookies, IP address). However, we do not want to use these without explanation. Below you will find an alphabetical list of important terms used, which we may not have sufficiently addressed in the previous privacy policy. If these terms have been taken from the GDPR and are definitions, we will also quote the GDPR texts here and add our own explanations if necessary.

Processor

Definition according to Article 4 of the GDPR

For the purposes of this Regulation:

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

Explanation: As a company and website owner, we are responsible for all data that we process from you. In addition to controllers, there may also be so-called processors. This includes any company or person that processes personal data on our behalf. In addition to service providers such as tax consultants, processors can therefore also be hosting or cloud providers, payment or newsletter providers or large companies such as Google or Microsoft.

Consent

Definition according to Article 4 of the GDPR

For the purposes of this Regulation:

"Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Explanation: As a rule, such consent is given via a cookie consent tool on websites. You are probably familiar with this. Whenever you visit a website for the first time, you are usually asked via a banner whether you agree or consent to data processing. In most cases, you can also make individual settings and decide for yourself which data processing you allow and which you do not. If you do not give your consent, your personal data may not 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 the purposes of this Regulation:

"personal data" means any information relating to an identified or identifiable person.

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

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

- Name
- Address
- E-mail address
- Postal address
- Telephone 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 much more.

According to the European Court of Justice (ECJ), your **IP address** is also **considered personal data**. IT experts can use your IP address to determine at least the approximate location of your device and subsequently you as the owner of the connection. Therefore, the storage of an IP address also requires a legal basis within the meaning of the GDPR. There are also so-called **"special categories"** of personal data, which are also particularly worthy of 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 (i.e. information on psychological, physical or behavioral characteristics that can identify a person).
- Health data
- Data on sexual orientation or sex life

Profiling

Definition according to Article 4 of the GDPR

For the purposes of this Regulation:

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

Explanation: Profiling involves collecting various pieces of information about a person in order to find out more about them. In the web sector, profiling is often used for advertising purposes or for credit checks. Web or Advertising analysis programs collect data about your behaviour and interests on a website, for example. This results in a special user profile that can be used to target advertising to a specific target group.

Person responsible

Definition according to Article 4 of the GDPR

For the purposes of this Regulation:

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

Explanation: In our case, we are responsible for the processing of your personal data and are therefore the "controller". If we pass on collected data to other service providers for processing, they are "processors". An "order processing contract (AVV)" must be signed for this.

Processing

Definition according to Article 4 of the GDPR

For the purposes of this Regulation:

"processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as the

collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Note: When we refer to processing in our privacy policy, we mean any kind of data processing. As mentioned above in the original GDPR declaration, this includes not only the collection but also the storage and processing of data.

Closing words

Congratulations! If you are reading this, you have really "fought" your way through our entire privacy policy, or at least scrolled this far. As you can see from the scope of our privacy policy, we take the protection of your personal data anything but lightly.

It is important to us to inform you to the best of our knowledge and belief about the processing of personal data. However, we not only want to tell you which data is processed, but also explain the reasons for using various software programs. As a rule, privacy policies sound very technical and legal. However, as most of you are not web developers or lawyers, we wanted to take a different approach in terms of language and explain the facts in simple and clear language. Of course, this is not always possible due to the subject matter. Therefore, the most important terms are explained in more detail at the end of the privacy policy.

If you have any questions about data protection on our website, please do not hesitate to contact us or the responsible office. We wish you a pleasant time and hope to welcome you back to our website soon.

All texts are protected by copyright.

Source: Created with the [Data Protection Generator Austria](#) by AdSimple