

Legal Notice

Information in accordance with the duty to inform pursuant to §5 of the E-Commerce Act, §14 of the Austrian Commercial Code, §63 of the Industrial Code and the duty to disclose pursuant to §25 of the Media Act.

zacweb.net e.U.
Peter Konecny
Körnermarkt 3,
3542 Gföhl,
Österreich

Object of the company: Dienstleistungen in der automatischen Datenverarbeitung und Informationstechnik

VAT-Number: ATU73675917

GLN: 9110026664221

GISA: 31014397

Corporate register number: FN498450s

Corporate register court: Landesgericht Krems

Company location: 3542 Gföhl

Phone: 02716 / 94100

Email: office@zacweb.net

Member of: WKO Niederösterreich, Fachgruppe Unternehmensberatung, Buchhaltung und Informationstechnologie

Laws re. professions: Gewerbeordnung: www.ris.bka.gv.at

Supervisory/Trade authority: Bezirkshauptmannschaft Krems

Job title: Webdesigner, Grafiker, IT-Dienstleister

Awarding country: Österreich

Contact details of the data protection controller

If you have any question about data protection, please find the contact details of the body or person responsible for data protection below:

w.o.

E-Mail: datenschutz@zacweb.net

EU Dispute Resolution

We would like to inform you about the Online Dispute Resolution platform (ODR platform) in accordance with the regulation on Online Dispute Resolution in consumer matters (ODR Regulation).

Consumers have the option of submitting complaints to the European Commission's Online Dispute Resolution platform at

<https://ec.europa.eu/consumers/odr/main/?event=main.home2.show>. You will find the necessary contact details in our imprint above.

However, we would like to note, that we are not willing or obliged to participate in dispute settlement procedures before a consumer arbitration board.

Liability for the Contents of this Website

We are constantly developing the content of this website and strive to provide correct and up-to-date information. Unfortunately, we cannot accept liability for the accuracy of any content on this website. This especially includes content provided by third parties. As a service provider, we are neither obliged to monitor any information you transmit or store, nor to investigate any circumstances that indicate illegal activity.

Due to court- or official orders under the general law, our obligations to remove information or to block the use of information remain unaffected, even if we are not responsible.

If you notice any problematic or illegal content, please contact us immediately so we can remove the illegal content. You will find our contact details in the imprint.

Liability for Links on this Website

Our website contains links to other websites for which we are not responsible. We are not liable for any linked websites, since we have had no knowledge of illegal activities. If we ever become aware of any illegal activity, we will remove any links in question immediately.

If you notice illegal links on our website, please contact us. You will find our contact details in the imprint.

Copyright Notice

All contents of this website (pictures, images, photos, texts, videos) are subject to copyright. Please ask us before distributing, reproducing or using the contents of this website – such as republishing them on other websites. If necessary, we will prosecute the unauthorised use of our website's content.

If you find content on this website that violates copyright, please contact us.

Picture Credits

The pictures, images and graphics on this website are protected by copyright.

The image rights are with:

Fotograf Max Mustermann
Fotografin Pia Musterfrau

All texts are copyrighted.

Source: Created with the [Impressum Generator](#) by AdSimple

Privacy Policy

Privacy Policy Introduction and Overview

We have written this privacy policy (version 01.02.2024-121887810) in order to explain to you, in accordance with the provisions of the [General Data Protection Regulation \(EU\) 2016/679](#) and applicable national laws, which personal data (data for short) we as the controller – and the processors commissioned by us (e.g. providers) – process, will process in the future and what legal options you have. The terms used are to be considered gender-neutral.

In short: We provide you with comprehensive information about any of your personal data we process.

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

If you still have questions, we kindly ask you to contact the responsible body named below or in the imprint, follow the existing links and look at further information on third-party sites. You can of course also find our contact details in the imprint.

Scope

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

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

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

Legal bases

In the following privacy policy, we provide you with transparent information on the legal principles and regulations, i.e. the legal bases of the General Data Protection Regulation, which enable us to process personal data.

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

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

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

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

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

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

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

Contact details of the data protection controller

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

w.o.

E-Mail: datenschutz@zacweb.net

Storage Period

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

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

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

Rights in accordance with the General Data Protection Regulation

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

- According to Article 15 DSGVO, you have the right to information about whether we are processing data about you. If this is the case, you have the right to receive a copy of the data and to know the following information:
 - for what purpose we are processing;
 - the categories, i.e. the types of data that are processed;
 - who receives this data and if the data is transferred to third countries, how security can be guaranteed;
 - how long the data will be stored;
 - the existence of the right to rectification, erasure or restriction of processing and the right to object to processing;
 - that you can lodge a complaint with a supervisory authority (links to these authorities can be found below);
 - the origin of the data if we have not collected it from you;
 - Whether profiling is carried out, i.e. whether data is automatically evaluated to arrive at a personal profile of you.
- You have a right to rectification of data according to Article 16 GDPR, which means that we must correct data if you find errors.
- You have the right to erasure (“right to be forgotten”) according to Article 17 GDPR, which specifically means that you may request the deletion of your data.
- According to Article 18 of the GDPR, you have the right to restriction of processing, which means that we may only store the data but not use it further.
- According to Article 20 of the GDPR, you have the right to data portability, which means that we will provide you with your data in a standard format upon request.
- According to Article 21 DSGVO, you have the right to object, which entails a change in processing after enforcement.

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

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

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

Austria Data protection authority

Manager: Mag. Dr. Andrea Jelinek

Address: Barichgasse 40-42, 1030 Wien

Phone number.: +43 1 52 152-0

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

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

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 if there is another legal permission. This is particularly true when processing is legally required or necessary for the performance of a contractual relationship, and in any case, only to the extent permitted by law. Your consent is in most cases the primary reason for us to process data in third countries. Processing of personal data in third countries such as the USA, where many software providers offer services and have their server locations, may mean that personal data is processed and stored in unexpected ways.

We explicitly point out that, according to the opinion of the European Court of Justice, there is currently only an adequate level of protection for data transfers to the USA if a US company processing personal data of EU citizens in the USA is an active participant in the EU-US Data Privacy Framework. More information can be found 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 anonymized and processed, if applicable. Additionally, US government authorities may potentially have access to individual data. Furthermore, it may occur that collected data is linked with 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 offered.

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

Security of data processing operations

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


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

TLS encryption with https

The terms TLS, encryption and https sound very technical, which they are indeed. We use HTTPS (Hypertext Transfer Protocol Secure) to securely transfer data on the Internet.

This means that the entire transmission of all data from your browser to our web server is secured – nobody can “listen in”.






We have thus introduced an additional layer of security and meet privacy requirements through technology design [Article 25 Section 1 GDPR](#)). With the use of TLS (Transport Layer Security), which is an encryption protocol for safe data transfer on the internet, we can ensure the protection of confidential information.

You can recognise the use of this safeguarding tool by the little lock-symbol , which is situated in your browser's top left corner in the left of the internet address (e.g. examplepage.uk), as well as by the display of the letters https (instead of http) as a part of our web address.

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

Communications

Communications Overview

-  Affected parties: Anyone who communicates with us via phone, email or online form
-  Processed data: e. g. telephone number, name, email address or data entered in forms.
You can find more details on this under the respective form of contact
-  Purpose: handling communication with customers, business partners, etc.
-  Storage duration: for the duration of the business case and the legal requirements
-  Legal basis: Article 6 (1) (a) GDPR (consent), Article 6 (1) (b) GDPR (contract), Article 6 (1) (f) GDPR (legitimate interests)

If you contact us and communicate with us via phone, email or online form, your personal data may be processed.

The data will be processed for handling and processing your request and for the related business transaction. The data is stored for this period of time or for as long as is legally required.

Affected persons

The above-mentioned processes affect all those who seek contact with us via the communication channels we provide.

Telephone

When you call us, the call data is stored in a pseudonymised form on the respective terminal device, as well as by the telecommunications provider that is being used. In addition, data such as your name and telephone number may be sent via email and stored for answering your inquiries. The data will be erased as soon as the business case has ended and the legal requirements allow for its erasure.

Email

If you communicate with us via email, your data is stored on the respective terminal device (computer, laptop, smartphone, ...) as well as on the email server. The data will be deleted as soon as the business case has ended and the legal requirements allow for its erasure.

Online forms

If you communicate with us using an online form, your data is stored on our web server and, if necessary, forwarded to our email address. The data will be erased as soon as the business case has ended and the legal requirements allow for its erasure.

Legal bases

Data processing 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 continue to use it for the purposes of the business case;
- Art. 6 para. 1 lit. b GDPR (contract): For the performance of a contract with you or a processor

such as a telephone provider, or if we have to process the data for pre-contractual activities, such as preparing an offer;

- Art. 6 para. 1 lit. f GDPR (legitimate interests): We want to conduct our customer inquiries and business communication in a professional manner. Thus, certain technical facilities such as email programs, Exchange servers and mobile network operators are necessary to efficiently operate our communications.

Data Processing Agreement (DPA)

In this section, we would like to explain what a Data Processing Agreement is and why it is needed. As the term "Data Processing Agreement" is quite lengthy, we will often only use the acronym DPA here in this text. Like most companies, we do not work alone, but also use the services of other companies or individuals. By involving different companies or service providers, we may pass on personal data for processing. These partners then act as processors with whom we conclude a contract, the so-called Data Processing Agreement (DPA). Most importantly for you to know is that any processing of your personal data takes place exclusively according to our instructions and must be regulated by the DPA.

Who are the processors?

As a company and website owner, we are responsible for any of your data that is processed by us. In addition to the controller, there may also be so-called processors involved. This includes any company or person who processes your personal data. More precisely and according to the GDPR's definition, this means: Any natural or legal person, authority, institution or other entity that processes your personal data is considered a processor. Processors can therefore be service providers such as hosting or cloud providers, payment or newsletter providers or large companies such as Google or Microsoft.

To make the terminology easier to comprehend, here is an overview of the GDPR's three roles:

Data subject (you as a customer or interested party) □ **Controller** (we as a company and contracting entity) □ **Processors** (service providers such as web hosts or cloud providers)

Contents of a Data Processing Agreement

As mentioned above, we have concluded a DPA with our partners who act as processors. First and foremost, it states that the processor processes the data exclusively in accordance with the GDPR. The contract must be concluded in writing, although an electronic contract completion is also considered a "written contract". Any processing of personal data only takes place after this contract is concluded. The contract must contain the following:

- indication to us as the controller
- obligations and rights of the controller
- categories of data subjects
- type of personal data
- type and purpose of data processing

- subject and duration of data processing
- location of data processing






Furthermore, the contract contains all obligations of the processor. The most important obligations are:

- ensuring data security measures
- taking possible technical and organisational measures to protect the rights of the data subject
- maintaining a data processing record
- cooperation with the data protection authority upon request
- performing a risk analysis for any received personal data
- subprocessors may only be appointed with the written consent of the controller

You can see an example of what a DPA looks like at <https://gdpr.eu/data-processing-agreement/>. This link shows a sample contract.

Cookies

Cookies Overview

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

What are cookies?

Our website uses HTTP-cookies to store user-specific data.

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

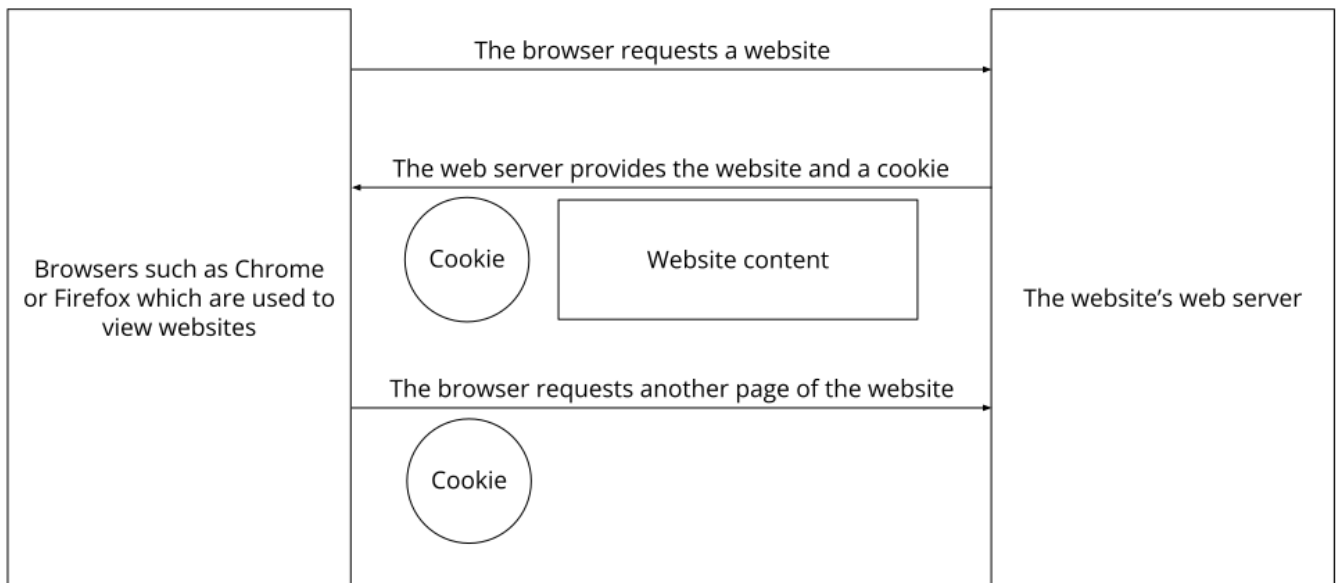
Whenever you surf the Internet, you are using a browser. Common browsers are for example, Chrome, Safari, Firefox, Internet Explorer and Microsoft Edge. Most websites store small text-files in your browser. These files are called cookies.

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

Cookies store certain user data about you, such as language or personal page settings. When you re-open our website to visit again, your browser submits these “user-related” information back to our site. Thanks to cookies, our website knows who you are and offers you the settings you are familiar to. In some browsers, each cookie has its own file, while in others, such as Firefox, all

cookies are stored in one single file.

The following graphic shows a possible interaction between a web browser such as Chrome and the web server. The web browser requests a website and receives a cookie back from the server. The browser then uses this again as soon as another page is requested.



There are both first-party cookies and third-party cookies. First-party cookies are created directly by our site, while third-party cookies are created by partner-websites (e.g. Google Analytics). Each cookie must be evaluated individually, as each cookie stores different data. The expiry time of a cookie also varies from a few minutes to a few years. Cookies are not software programs and do not contain viruses, trojans or other malware. Cookies also cannot access your PC's information.

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

Name: _ga

Value: GA1.2.1326744211.152121887810-9

Purpose: Differentiation between website visitors

Expiry date: after 2 years

A browser should support these minimum sizes:

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

Which types of cookies are there?

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

There are 4 different types of cookies:

Essential cookies

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

Purposive cookies

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

Target-orientated cookies

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

Advertising cookies

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

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

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

Purpose of processing via cookies

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

Which data are processed?

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

Storage period of cookies

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

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

Right of objection – how can I erase cookies?

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

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

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

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

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

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

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

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

Legal basis

The so-called “cookie directive” has existed since 2009. It states that the storage of cookies requires your **consent** (Article 6 Paragraph 1 lit. a GDPR). Within countries of the EU, however, the reactions to these guidelines still vary greatly. In Austria, however, this directive was implemented in Section 165 (3) of the Telecommunications Act (2021). In Germany, the cookie guidelines have not been implemented as national law. Instead, this guideline was largely implemented in Section 15 (3) of the Telemedia Act (TMG).


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


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


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


Customer Data


Customer Data Overview

 Affected parties: Customers or business and contractual partners

 Purpose: Performance of a contract for the provision of agreed services or prior to entering into such a contract, including associated communications.

 Data processed: name, address, contact details, email address, telephone number, payment information (such as invoices and bank details), contract data (such as duration and subject matter of the contract), IP address, order data

 Storage period: the data will be erased as soon as they are no longer required for our business purposes and there is no legal obligation to process them.

 Legal bases: Legitimate interests (Art. 6 Para. 1 lit. f GDPR), Contract (Art. 6 Para. 1 lit. b GDPR)

What is customer data?

In order to be able to offer our services and contractual services, we also process data from our customers and business partners. This data always includes personal data. Customer data is all information that is processed on the basis of contractual or pre-contractual agreements so that the offered services can be provided. Customer data is therefore all the information we collect and process about our customers.

Why do we process customer data?

There are many reasons why we collect and process customer data. The main reason is that we simply need specific data to provide our services. Sometimes for example your email address may be enough. But if you purchase a product or service, we may e. g. also need data such as your name, address, bank details or other contract data. This data will subsequently be used for marketing and sales optimisation so that we can improve our overall service for our customers and clients. Another important reason for data processing is our customer service, which is very important to us. We want you to have the opportunity to contact us at any time with questions about our offers. Thus, we may need certain data such as your email address at the very least.

What data is processed?

Exactly which data is stored can only be shown by putting them in categories. All in all, it always depends on which of our services you receive. In some cases, you may only give us your email address so that we can e. g. contact you or answer your questions. In other instances, you may purchase one of our products or services. Then we may need significantly more information, such as your contact details, payment details and contract details.

Here is a list of potential data we may receive and process:

- Name
- Contact address
- Email address
- Phone number

- Your birthday
- Payment data (invoices, bank details, payment history, etc.)
- Contract data (duration, contents)
- Usage data (websites visited, access data, etc.)
- Metadata (IP address, device information)

How long is the data stored?

We erase corresponding customer data as soon as we no longer need it to fulfill our contractual obligations and purposes, and as soon as the data is also no longer necessary for possible warranty and liability obligations. This can for example be the case when a business contract ends. Thereafter, the limitation period is usually 3 years, although longer periods may be possible in individual cases. Of course, we also comply with the statutory retention requirements. Your customer data will certainly not be passed on to third parties unless you have given your explicit consent.






Legal Basis

The legal basis for the processing of your data is Article 6 Paragraph 1 Letter a GDPR (consent), Article 6 Paragraph 1 Letter b GDPR (contract or pre-contractual measures), Article 6 Paragraph 1 Letter f GDPR (legitimate interests) and in special cases (e. g. medical services) Art. 9 (2) lit. GDPR (processing of special categories).

In the case of protecting vital interests, data processing is carried out in accordance with Article 9 Paragraph 2 Letter c. GDPR. For the purposes of health care, occupational medicine, medical diagnostics, care or treatment in the health or social sectors or for the administration of systems and services in health or social sectors, the processing of personal data takes place in accordance with Art. 9 Para. 2 lit. h. GDPR. If you voluntarily provide data of these special categories, the processing takes place on the basis of Article 9 Paragraph 2 lit. a GDPR.

Web hosting

Web hosting Overview

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

What is web hosting?

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

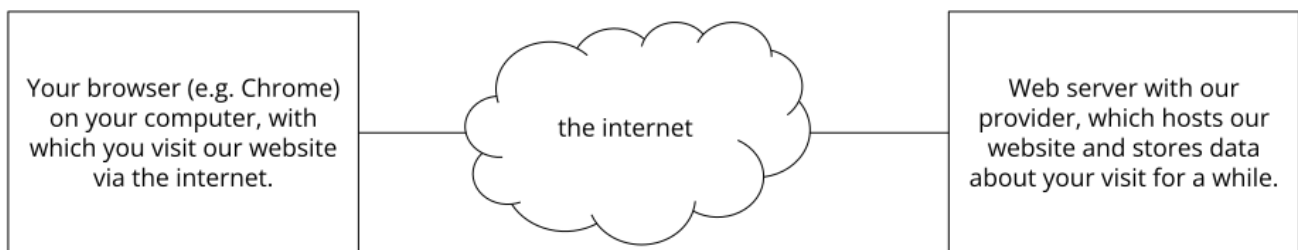
domain we mean example.uk or examplepage.com.

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

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

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

Illustration:



Why do we process personal data?

The purposes of data processing are:

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

Which data are processed?

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

- the full address (URL) of the accessed website (e. g. <https://www.examplepage.uk/examplesubpage.html?tid=121887810>)
- browser and browser version (e.g. Chrome 87)
- the operating system used (e.g. Windows 10)
- the address (URL) of the previously visited page (referrer URL) (e. g. <https://www.examplepage.uk/icamefromhere.html/>)
- the host name and the IP address of the device from the website is being accessed from (e.g.

COMPUTERNAME and 194.23.43.121)

- date and time
- in so-called web server log files

How long is the data stored?

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

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

Legal basis


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


Web Analytics


Web Analytics Privacy Policy Overview

 Affected parties: visitors to the website

 Purpose: Evaluation of visitor information to optimise the website.

 Processed data: Access statistics that contain data such as access location, device data, access duration and time, navigation behaviour, click behaviour and IP addresses. You can find more details on this from the respective web analytics tool directly.

 Storage period: depending on the respective 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, which is known as web analytics, in order to evaluate website visitor behaviour. Thus, data is collected, which the analytic tool provider (also called tracking tool) stores, manages and processes. Analyses of user behaviour on our website are created with this data, which we as the website operator receive. Most tools also offer various testing options. These enable us, to for example test which offers or content our visitors prefer. For this, we may show you two different offers for a limited period of time. After the test (a so-called A/B test) we know which product or content our website visitors find more interesting. For such testing as well as for various other analyses, user profiles are created and the respective data is stored in cookies.

Why do we run Web Analytics?

We have a clear goal in mind when it comes to our website: we want to offer our industry's best website on the market. Therefore, we want to give you both, the best and most interesting offer as

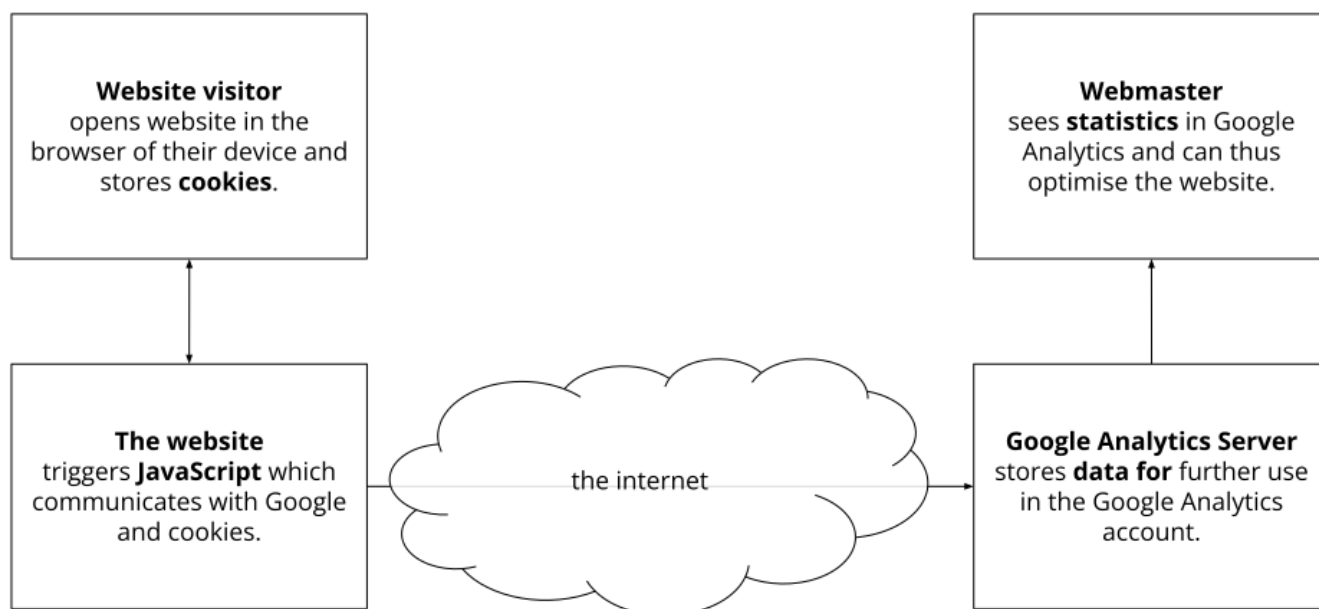
well as comfort when you visit our website. With web analysis tools, we can observe the behaviour of our website visitors, and then improve our website accordingly for you and for us. For example, we can see the average age of our visitors, where they come from, the times our website gets visited the most, and which content or products are particularly popular. All this information helps us to optimise our website and adapt it to your needs, interests and wishes.

Which data are processed?

The exact data that is stored depends on the analysis tools that are being used. But generally, data such as the content you view on our website are stored, as well as e. g. which buttons or links you click, when you open a page, which browser you use, which device (PC, tablet, smartphone, etc.) you visit the website with, or which computer system you use. If you have agreed that location data may also be collected, this data may also be processed by the provider of the web analysis tool.

Moreover, 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 in a pseudonymised form (i.e. in an unrecognisable and abbreviated form). No directly linkable data such as your name, age, address or email address are stored for testing purposes, web analyses and web optimisations. If this data is collected, it is retained in a pseudonymised form. Therefore, it cannot be used to identify you as a person.

The following example shows Google Analytics' functionality as an example for client-based web tracking with JavaScript code.



The storage period of the respective data always depends on the provider. Some cookies only retain data for a few minutes or until you leave the website, while other cookies can store data for several years.

Duration of data processing

If we have any further information on the duration of data processing, you will find it below. We generally only process personal data for as long as is absolutely necessary to provide products and services. The storage period may be extended if it is required by law, such as for accounting purposes for example for accounting.

Right to object

You also have the option and the right to revoke 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 processing by cookies by managing, deactivating or erasing cookies in your browser.

Legal basis

The use of Web Analytics requires your consent, which we obtained with our cookie popup. According to **Art. 6 para. 1 lit. a of the GDPR (consent)**, this consent represents the legal basis for the processing of personal data, such as by collection through Web Analytics tools.






In addition to consent, we have a legitimate interest in analysing the behaviour of website visitors, which enables us to technically and economically improve our offer. With Web Analytics, we can recognise website errors, identify attacks and improve profitability. The legal basis for this is **Art. 6 para. 1 lit. f of the GDPR (legitimate interests)**. Nevertheless, we only use these tools if you have given your consent.

Since Web Analytics tools use cookies, we recommend you to read our privacy policy on cookies. If you want to find out which of your data are stored and processed, you should read the privacy policies of the respective tools.

If available, information on special Web Analytics tools can be found in the following sections.

Matomo Cloud privacy policy

Matomo Cloud Privacy Policy Overview

-  Affected parties: website visitors
-  Purpose: Evaluation of visitor information for website optimisation.
-  Processed data: Access statistics containing data such as access location, device data, access duration and time, navigation behaviour, click behaviour and IP addresses.
-  Storage period: data is retained until no longer required for the service provision. Log file data are erased after a maximum of 30 days.
-  Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is Matomo Cloud?

We use the web analytics software Matomo Cloud on our website. The service provider is the New

Zealand-based company InnoCraft Ltd, 7 Waterloo Quay PO625, 6140 Wellington, New Zealand. Matomo is a privacy-focused web analytics platform that provides accurate statistics on your behavior on our website while taking data protection seriously. We have access to a Matomo dashboard and can utilize various functions for web analytics. Matomo also offers different options to anonymize IP addresses of our website visitors and disable cookies.

Why do we use Matomo Cloud?

Many common analytics tools collect vast amounts of personally identifiable information and may share it with third parties, making data control challenging. Data protection is a significant concern for us, and that's why we chose Matomo, a much more privacy-friendly alternative. However, we also don't want to entirely forego web analytics. Statistics on website behavior help us optimize our service and tailor it to your individual needs.

What data does Matomo Cloud store?

In addition to personal data such as your IP address or information about you (e.g., name, address, birthdate) that you actively provide, Matomo Cloud mainly stores information about your visitor behavior. This usually includes non-personal data like website visitor count, page views, duration of visits, or used search terms. Additionally, technical data such as browser type, your operating system, and screen resolution may be stored. Matomo can also collect information about the website you came from. The collected data is never shared or sold to third parties.

How long and where are the data stored?

Matomo Cloud offers a hosted version where data is stored on dedicated Matomo servers. All data is stored in Europe, even though the main headquarters are in New Zealand.

In general, data at Matomo Cloud is stored as long as required for business purposes.

Unfortunately, exact retention periods cannot be specified here as they depend heavily on individual configurations.

How can I delete my data or prevent data storage?

You have the right and the option to access your personal data, object to its use and processing, and submit a complaint to a state supervisory authority at any time.

In your browser settings, you also have the option to manage, delete, or disable cookies individually. Please note that disabled or deleted cookies may have potential negative impacts on the functionality of our website. Managing cookies varies slightly depending on your browser. Links to instructions for the most popular browsers can be found in the "Cookies" section. If you want to request data deletion, you can also contact us.

Legal Basis

The use of Matomo Cloud requires your consent, which we obtained through our consent management tool (popup). According to Art. 6 para. 1 lit. a GDPR (Consent), this consent constitutes the legal basis for the processing of personal data that may occur during the collection by web






analytics tools.

In addition to consent, we have a legitimate interest in analyzing the behavior of website visitors to improve our technical and economic offerings. With the help of Matomo Cloud, we identify optimization potential for our website and enhance cost-effectiveness. The legal basis for this is Art. 6 para. 1 lit. f GDPR (Legitimate interests). However, we use Matomo Cloud only to the extent that you have given consent.

For more information about the data processed by the use of Matomo Cloud, refer to the Privacy Policy at <https://matomo.org/matomo-cloud-privacy-policy/>. For privacy-related questions, you can email privacy@matomo.org.

Matomo On-Premise Privacy Policy

Matomo On-Premise Privacy Policy Overview

-  Affected parties: website visitors
-  Purpose: Evaluation of visitor information to optimise the website.
-  Processed data: Data such as the number of website visitors, page views, duration of visits, or used search terms. More details can be found below and in the privacy policy of Matomo On-Premise.
-  Storage period: In principle, the data is stored with us for as long as business purposes require.
-  Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is Matomo On-Premise?

We use the privacy-friendly analytics program Matomo On-Premise on our website. In the On-Premise version, Matomo is installed on our own server. This means we act as the operator of the software, and any data we might collect from you is stored directly with us. The data processing thus remains entirely within our control. The tool is developed by the New Zealand-based company InnoCraft Ltd, 7 Waterloo Quay PO625, 6140 Wellington, New Zealand.

Matomo On-Premise is a web analytics platform that takes data privacy seriously while providing accurate statistics on your behavior on our website for us as website operators. A significant difference from other analytics programs is the option of data storage on our own server. Matomo On-Premise also offers various ways to anonymize IP addresses of our website visitors and disable cookies.

Why do we use Matomo On-Premise?

Many common analytics tools collect vast amounts of personally identifiable information and may share it with third parties. This means maintaining control over your data becomes challenging. Data privacy is a significant concern for us, and that's why we opted for Matomo On-Premise, a considerably more privacy-friendly alternative. However, we do not want to completely forego web analytics. After all, with the help of statistics on website behavior, we can optimize our service and tailor it to your individual needs.

What data is stored by Matomo On-Premise?

In addition to personally identifiable information you actively provide, such as your IP address or personal details (e.g., name, address, date of birth), Matomo On-Premise primarily stores information about your visitor behavior. This usually involves non-personal data, such as the number of website visitors, page views, duration of visits, or used search terms. Technical data like browser type, operating system, and screen resolution can also be stored. Matomo On-Premise may collect information about the website from which you accessed ours. The collected data is stored with us and not shared or sold to third parties.

How long and where are the data stored?

Matomo On-Premise is a self-hosted analytics platform, meaning we store all collected data directly on our own servers. Our server is located in Europe, so data is not processed in third countries, i.e., countries outside the scope of the GDPR.

In general, data is stored with us for as long as business purposes require. Unfortunately, we cannot provide precise retention periods at this point, as they strongly depend on our individual configurations. If you want to learn more about our data retention periods and configurations, please feel free to contact us.

How can I delete my data or prevent data storage?

You have the right and the option to access your personally identifiable data at any time and object to its use and processing. You can also file a complaint with a state supervisory authority or with us at any time.

In your browser, you also have the option to manage, delete, or disable cookies individually. Please note that disabled or deleted cookies may have potential negative effects on the functions of our website. The process of managing cookies may vary depending on the browser you use. The respective links to the instructions for the most popular browsers can be found under the "Cookies" section. If you want to request data deletion, you can also contact us.

Legal Basis

The use of Matomo On-Premise requires your consent, which we obtained through our Consent Management Tool (Popup). According to Art. 6 (1) lit. a GDPR (Consent), this consent is the legal basis for the processing of personally identifiable data, as may occur with the collection by web analytics tools.

In addition to consent, we have a legitimate interest in analyzing the behavior of website visitors to technically and economically improve our offerings. By using Matomo On-Premise, we can identify optimization potential for our website and improve efficiency. The legal basis for this is Art. 6 (1) lit. f GDPR (Legitimate Interests). However, we only use Matomo On-Premise to the extent that you have given consent.

If you want to learn more about the data processing by Matomo On-Premise, feel free to contact us. We also recommend Matomo's privacy policy at <https://matomo.org/privacy-policy/>.

Matomo On-Premise (ohne Cookies)

What is Matomo On-Premise (without Cookies)?

We use the privacy-friendly analytics program Matomo On-Premise without the use of cookies on our website. With the On-Premise version, Matomo is installed on our own server. This means we act as the operator of the software, and any potential data we could collect from you is stored directly with us. Thus, data processing remains entirely within our control. The tool is developed by the New Zealand-based company InnoCraft Ltd, 7 Waterloo Quay PO625, 6140 Wellington, New Zealand.

Matomo On-Premise is a web analytics platform that takes data protection seriously and still provides accurate statistics on your behavior on our website. A significant difference from other analytics programs is the option of storing data on our own server. Matomo On-Premise also offers various ways to anonymize IP addresses of our website visitors and disable cookies. We have also opted for cookie deactivation. This means we use Matomo On-Premise for our website without the use of cookies.

Why do we use Matomo On-Premise?

Many common analytics tools collect vast amounts of personally identifiable information and may share it with third parties, making data control challenging. Data protection is a significant concern for us, and that's why we chose Matomo On-Premise without the use of cookies. However, we also don't want to entirely forego web analytics. Statistics on website behavior help us optimize our service and tailor it to your individual needs.

What data does Matomo On-Premise store?

Primarily, Matomo On-Premise stores information about your visitor behavior. This is not personal data but includes information such as website visitor count, page views, duration of visits, or used search terms. Additionally, technical data such as browser type, your operating system, and screen resolution may be stored. Matomo On-Premise can also collect information about the website you came from. The collected data is stored with us and is not shared or sold to third parties.

How long and where are the data stored?

Matomo On-Premise is a self-hosted analytics platform, meaning we store all collected data directly on our own servers. Our server is located in Europe, so data is not processed in third countries, i.e., countries outside the scope of the GDPR.

In general, the data is stored with us as long as required for business purposes. Unfortunately, we cannot provide precise retention periods here as they strongly depend on our individual configurations. If you want to learn more about our data storage duration and configurations, please feel free to contact us.

How can I delete my data or prevent data storage?

You have the right and the option to access your personal data, object to its use and processing,

and submit a complaint to a state supervisory authority or simply to us at any time.






Legal Basis

We have a legitimate interest in analyzing the behavior of website visitors to improve our technical and economic offerings. With the help of Matomo On-Premise, we identify optimization potential for our website and enhance cost-effectiveness. The legal basis for this is Art. 6 para. 1 lit. f GDPR (Legitimate interests).

If you want to know more about the data processing by Matomo On-Premise without cookies, feel free to contact us. We also recommend Matomo's privacy policy at <https://matomo.org/privacy-policy/>.

Email-Marketing

Email Marketing Overview

-  Affected parties: newsletter subscribers
-  Purpose: direct marketing via email, notification of events that are relevant to the system
-  Processed data: data entered during registration, but at least the email address. You can find more details on this in the respective email marketing tool used.
-  Storage duration: for the duration of the subscription
-  Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is Email-Marketing?

We use email marketing to keep you up to date. If you have agreed to receive our emails or newsletters, your data will be processed and stored. Email marketing is a part of online marketing. In this type of marketing, news or general information about a company, product or service are emailed to a specific group of people who are interested in it.

If you want to participate in our email marketing (usually via newsletter), you usually just have to register with your email address. To do this, you have to fill in and submit an online form. However, we may also ask you for your title and name, so we can address you personally in our emails.

The registration for newsletters generally works with the help of the so-called "double opt-in procedure". After you have registered for our newsletter on our website, you will receive an email, via which you can confirm the newsletter registration. This ensures that you own the email address you signed up with, and prevents anyone to register with a third-party email address. We or a notification tool we use, will log every single registration. This is necessary so we can ensure and prove, that registration processes are done legally and correctly. In general, the time of registration and registration confirmation are stored, as well as your IP address. Moreover, any change you make to your data that we have on file is also logged.

Why do we use Email-Marketing?

Of course, we want to stay in contact with you and keep you in the loop of the most important

news about our company. For this, we use email marketing – often just referred to as “newsletters” – as an essential part of our online marketing. If you agree to this or if it is permitted by law, we will send you newsletters, system emails or other notifications via email. Whenever the term “newsletter” is used in the following text, it mainly refers to emails that are sent regularly. We of course don't want to bother you with our newsletter in any way. Thus, we genuinely strive to offer only relevant and interesting content. In our emails you can e.g. find out more about our company and our services or products. Since we are continuously improving our offer, our newsletter will always give you the latest news, or special, lucrative promotions. Should we commission a service provider for our email marketing, who offers a professional mailing tool, we do this in order to offer you fast and secure newsletters. The purpose of our email marketing is to inform you about new offers and also to get closer to our business goals.

Which data are processed?

If you subscribe to our newsletter via our website, you then have to confirm your membership in our email list via an email that we will send to you. In addition to your IP and email address, your name, address and telephone number may also be stored. However, this will only be done if you agree to this data retention. Any data marked as such are necessary so you can participate in the offered service. Giving this information is voluntary, but failure to provide it will prevent you from using this service. Moreover, information about your device or the type of content you prefer on our website may also be stored. In the section “Automatic data storage” you can find out more about how your data is stored when you visit a website. We record your informed consent, so we can always prove that it complies with our laws.

Duration of data processing

If you unsubscribe from our e-mail/newsletter distribution list, we may store your address for up to three years on the basis of our legitimate interests, so we can keep proof your consent at the time. We are only allowed to process this data if we have to defend ourselves against any claims.

However, if you confirm that you have given us your consent to subscribe to the newsletter, you can submit an individual request for erasure at any time. Furthermore, if you permanently object to your consent, we reserve the right to store your email address in a blacklist. But as long as you have voluntarily subscribed to our newsletter, we will of course keep your email address on file.

Withdrawal – how can I cancel my subscription?

You have the option to cancel your newsletter subscription at any time. All you have to do is revoke your consent to the newsletter subscription. This usually only takes a few seconds or a few clicks. Most of the time you will find a link at the end of every email, via which you will be able to cancel the subscription. Should you not be able to find the link in the newsletter, you can contact us by email and we will immediately cancel your newsletter subscription for you.

Legal basis


Our newsletter is sent on the basis of your **consent** (Article 6 (1) (a) GDPR). This means that we are

only allowed to send you a newsletter if you have actively registered for it beforehand. Moreover, we may also send you advertising messages on the basis of Section 7 (3) UWG (Unfair Competition Act), provided you have become our customer and have not objected to the use of your email address for direct mail.


If available – you can find information on special email marketing services and how they process personal data, in the following sections.

Messenger & Communication Introduction


Messenger & Communication Privacy Statement Overview


 Affected parties: website visitors

 Purpose: for contact requests and general communications between yourself and us

 Processed data: Data such as name, address, email address, telephone number, general content data, plus IP address if applicable

You can find more details on this under the respective tools used.

 Storage duration: depends on the messenger & communication functions

 Legal bases: Article 6 paragraph 1 letter a GDPR (consent), Article 6 paragraph 1 letter f GDPR (legitimate interests), Article 6 paragraph 1 sentence 1 letter b. GDPR (contractual or pre-contractual obligations)

What are Messenger & Communication functions?

We offer you various options on our website to communicate with us (e.g. messenger and chat functions, online or contact forms, email, telephone). With the use of these functions, your data will be processed and stored insofar as it is necessary to answer your inquiry and conduct any of our subsequent measures.

In addition to classic means of communication such as email, contact forms or telephone, we also use chats or messengers. The most commonly used messenger function at the moment is WhatsApp, but of course, there are many different providers who offer messenger functions for websites. If content is end-to-end encrypted, it will be indicated in our individual privacy policies or in the privacy policy of the respective provider. End-to-end encryption means that the content of a message is not visible to the provider themselves. However, information about your device, location settings and other technical data can still be processed and stored.

Why do we use Messenger & Communication functions?

The ability to communicate with you is very important to us. After all, we want to keep the conversation with you going and answer any questions you may have about our service as best we can. Needless to say, smooth communication is an important part of our service. With our practical messenger & communication functions, you always have the option to choose the ones you prefer most. In exceptional cases, however, we may not be able to answer certain questions via chat or messenger. This may be the case for internal contractual matters, for example. For matters like these, we recommend you to use other communication options such as email or telephone.

We generally assume our responsibility under data protection law, even if we use the services of

any social media platform. However, the European Court of Justice has decided that in certain cases the operator of the social media platform be jointly responsible alongside us in the scope of Art. 26 GDPR. Should this be the case, we will point it out separately and work on the basis of a relevant agreement. You will find the essence of the agreement for the respective platforms below.

Please note that when using our integrated elements, your data may also be processed outside the European Union, since many providers, such as Facebook Messenger or WhatsApp, 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.

Which data is processed?

Exactly which data is retained and processed depends on the respective messenger & communication function provider. In general, it is data such as your name, address, telephone number, email address and content data such as any information you enter into a contact form. In most cases, information about your device and IP address are also stored. Moreover, data that are transmitted via a messenger & communication function are also stored on the providers' servers.

If you want to know exactly which data is stored and processed by the respective providers and how you can object to the data processing, you please carefully read the respective privacy policy of the company in question.

How long is data stored?

How long data is processed and stored depends primarily on the tools we use. Below you can find out more about the data processing of individual tools. The providers' privacy policies usually state exactly which data is stored and processed and for how long. In general, we only process personal data for as long as necessary to provide our services. When data is stored in cookies, the storage period varies greatly. Data may e.g. be deleted immediately after leaving a website, or they may be stored for several years. Therefore, you should study each individual cookie in detail if you want to know more about data storage. In most cases, you will also find helpful information about individual cookies in the privacy policies of the individual providers.

Right to object

You also have the right and the option to revoke your consent to the use of cookies or third-party providers at any time. This can be done 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 the cookies in your browser. For more information, we recommend you to read the Consent section.

Since cookies may be in use with messenger & communication functions, we recommend you to read our general privacy policy on cookies. To find out exactly which of your data is stored and processed, please read the privacy policies of the respective tools.

Legal Basis

If you have consented to the data processing and storage by integrated messenger & communication functions, this consent is the legal basis for data processing (**Art. 6 Para. 1 lit. a GDPR**). We process your request and manage your data within the framework of contractual or pre-contractual relationships in order to fulfill our pre-contractual and contractual obligations or to answer inquiries. The basis for this is **Art. 6 Para. 1 section 1 lit. b GDPR**. In general, if you have given your consent, your data will also be stored and processed on the basis of our legitimate interest (**Art. 6 Para. 1 lit. f GDPR**) in quick and smooth communication with you or other customers and business partners.

Signal Messenger Privacy Policy

We use the messenger service Signal Messenger on our website. The service provider is the American company Signal Messenger LLC, 650 Castro Street, Suite 120-223 Mountain View, CA 94041, USA.

What is Signal Messenger?

Signal Messaging is an open-source application that allows us to have secure and private communication through text messages, voice, or video calls. The tool was founded in 2014 by Moxie Marlinspike and Stuart Anderson. Signal works on iOS, Android, and desktop. An important feature of Signal is its end-to-end encryption. This encryption ensures that messages or calls can truly only be read, seen, or heard by the parties involved. Even the developers of Signal cannot decrypt the messages.

Why do we use Signal Messenger?

Of course, we want to stay in communication with you. When we had to choose a messenger, our choice quickly fell on Signal Messenger. As the security of data is a major concern for us, we highly appreciate the encrypted communication that the tool offers. Additionally, there are further security settings, such as automatic data deletion or two-factor authentication.

How secure is data transfer with Signal Messenger?

Signal processes data, among other things, in the United States. We would like to point out that, according to the European Court of Justice, there is currently no adequate level of protection for data transfer to the United States. This may involve various risks for the legality and security of data processing.






As a basis for data processing by recipients located in third countries (outside the European Union, Iceland, Liechtenstein, Norway, and particularly in the United States) or for transferring data to those countries, Signal uses standard contractual clauses approved by the EU Commission (= Art. 46. Sec. 2 and 3 GDPR). These clauses obligate Signal to comply with the EU data protection level when processing relevant data even outside the EU. These clauses are based on an implementing decision by the EU Commission. You can find the decision and the clauses here:

https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=en

You can learn more about the data processed through the use of Signal in the Privacy Policy at <https://signal.org/legal/>.

Social Media

Social Media Privacy Policy Overview

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

What is Social Media?

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

Why do we use Social Media?

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

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

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

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

Which data are processed?

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

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

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

Duration of data processing

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

Right to object

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

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

Legal basis


If you have consented to the processing and storage of your data by integrated social media


elements, this consent serves as the legal basis for data processing (**Art. 6 para. 1 lit. a GDPR**). Generally, provided you have given your consent, your data will also be stored and processed on the basis of our legitimate interest (**Art. 6 para. 1 lit. f GDPR**) in maintaining fast and good communication with you and other customers and business partners. Nevertheless, we only use the tools if you have consented. Most social media platforms also set cookies on your browser to store data. We therefore recommend you to read our privacy policy on cookies carefully and to take a look at the privacy policy or cookie policy of the respective service provider.


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

Facebook Privacy Policy


Facebook Privacy Policy Overview


 Affected parties: website visitors

 Purpose: service optimisation

 Processed data: data such as customer data, data on user behaviour, device information and IP address.

You can find more details in the Privacy Policy below.

 Storage period: until the data no longer serves Facebook's purposes

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

What are Facebook tools?

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

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

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

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

call them “Facebook tools”. They include the following:

- Facebook-Pixel
- Social Plugins (e.g. the “Like” or “Share” button)
- Facebook Login
- Account Kit
- APIs (application programming interface)
- SDKs (Software development kits)
- Plattform-integrations
- Plugins
- Codes
- Specifications
- Documentations
- Technologies and Services

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

Why do we use Facebook tools on our website?

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

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

What data is stored by Facebook tools?

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

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

Moreover, not only contact data, but also “event data” is transferred. These data are the

information we receive about you on our website. To give an example, it allows us to see what subpages you visit or what products you buy from us. Facebook does not disclose the obtained information to third parties (such as advertisers), unless the company has an explicit permission or is legally obliged to do so. Also, "event data" can be linked to contact information, which helps Facebook to offer improved, customised adverts. Finally, after the previously mentioned matching process, Facebook deletes the contact data.

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

How long and where are the data stored?

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

How can I erase my data or prevent data retention?

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

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

- 1) Click on settings in the top right side in Facebook.
- 2) Then, click "Your Facebook information" in the left column.
- 3) Now click on "Deactivation and deletion".
- 4) Choose "Permanently delete account" and then click on "Continue to account deletion".
- 5) Enter your password, click on "continue" and then on "Delete account".

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

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

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

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

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

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

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

Legal basis

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

Facebook processes data from you, among other things, in the USA. Facebook respectively 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. More information can be found at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Additionally, Facebook uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Facebook commits to maintaining the European data protection level 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://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

The Facebook Data Processing Term, which references the Standard Contractual Clauses, can be found at <https://www.facebook.com/legal/terms/dataprocessing>.

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

Facebook Social Plugins Privacy Policy

We installed so-called social plugins from Facebook Inc. to our website. You can recognise these

buttons by the classic Facebook logo, the “Like” button (hand with raised thumb) or by a “Facebook plugin” label. A social plugin is a small part of Facebook that is integrated into our page. Each plugin has its own function. The most used functions are the well-known “Like” and “Share” buttons.

Facebook offers the following social plugins:

- “Save” button
- “Like” button, Share, Send and Quote
- Page plugin
- Comments
- Messenger plugin
- Embedded posts and video player
- Group Plugin

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

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

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

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

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

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

Name: dpr

Value: no information

Purpose:This cookie is used to make the social plugins work on our website.

Expiry date: after end of session

Name: fr

Value: 0jiejyh4121887810c2GnlufEJ9..Bde09j...1.0.Bde09j

Purpose:The cookie is also necessary for the plugins to function properly

Expiry date: after 3 months


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


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


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


Gravatar Privacy Policy


Gravatar Privacy Policy Overview

 Affected parties: website visitors

 Purpose: optimising our service

 Processed data: includes your encrypted e-mail address, IP address and our server URL
More details can be found in the privacy policy below.

 Storage period: the data is generally deleted when it is no longer useful for the provider's services.

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

What is Gravatar?

We have integrated the Gravatar plugin from Automattic Inc. (60 29th Street # 343, San Francisco, CA 94110, USA) into our website. Gravatar is automatically activated on all WordPress websites. The function enables user images (avatars) to be displayed in published articles or comments, provided the respective email address is registered at www.gravatar.com.

This function sends data to Gravatar or Automattic Inc. where it gets stored and processed. In this privacy statement we would like to inform you what data this is, how the network uses it and how you can manage or prevent data retention.

Gravatar stands for "Globally Recognized Avatar" which is a globally available avatar (a user picture) that is linked to an email address. The company Gravatar is the world's leading provider for this service. As soon as a user enters their email address which is also registered with www.gravatar.com to a website, the user's previously stored image is automatically displayed with their post or comment.

Why do we use Gravatar on our website?

Anonymity on the internet is a popular topic. An avatar gives people that make posts or comments

a face. Moreover, it makes it easier to be recognised on the web and to make oneself known. Many users enjoy the advantages of user pictures as they want to appear on the web in a personal and authentic manner. Of course, we want to offer you the possibility to display your Gravatar also on our website. Furthermore, we also like to see faces of our commenting users. With the activated Gravatar function, we are expanding the service on our website. After all, we want you to feel comfortable on our website and enable you to receive an extensive and interesting offer.

What data is stored by Gravatar?

When you publish a comment to a blogpost which requires an email address, WordPress checks whether your email address is linked to an avatar on Gravatar. For this, your email address gets encrypted and hashed and sent to Gravatar's or Automattic's servers, together with your IP address and our URL. Then Gravatar will check whether the email address is registered with the platform.

If the email address is registered with Gravatar, the image (gravatar) stored there will be displayed in the published comment. If you have registered your email address with Gravatar and comment on our website, further data will be transmitted to Gravatar, where it will be saved and processed. In addition to IP address and user behaviour data, this includes e.g. your browser type, the unique device identification, your preferred language, the data and time of the page visit, your operating system and information on the mobile network. Gravatar use this information to improve their services and offers and to gain better insight into the use of their service.

The following cookies are set by Automattic when a user enters an email address that is registered with Gravatar, for submitting a comment:

Name: gravatar

Value: 16b3191024acc05a238209d51ffcb92bdd710bd19121887810-7

Purpose: We could not find any exact information about the cookie.

Expiry date: after 50 years

Name: is-logged-in

Value: 1121887810-1

Purpose: This cookie stores the information that the user is logged in via the registered email address.

Expiry date: after 50 years

How long and where is the data retained?

Automattic deletes the collected data either if they are no longer used for their services, or if the company is not legally obliged to keep the data. Web server logs such as IP addresses, browser types and operating systems will be deleted after about 30 days. Until deletion, Automattic use the data to analyse traffic on their own websites (for example all WordPress sites) and to fix potential problems. The data is also stored on Automattic's American servers.

How can I delete my data or prevent data retention?

You have the right to access and delete your personal data at any time. If you have registered with Gravatar with an email address, you can delete your account or email address there at any time.

Since images are only displayed when using an email address registered with Gravatar, and data is therefore transferred to Gravatar, you can prevent transmission of your data to Gravatar by submitting comments or articles on our website with an email address that is not registered with Gravatar.

You can manage, deactivate or delete cookies that may be set in your browser when commenting. Please note that in this case comment functions may no longer be available in their intended scope. Depending on the browser you use, the management of cookies works a little different. You can find the instructions for the most common browsers here:

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

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

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

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

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

Automattic is an active participant in the EU-U.S. Privacy Shield Framework which regulates correct and secure transfer of personal data. You can find more information on this at

<https://www.privacyshield.gov/participant?id=a2zt0000000CbqcAAC> .

You can find more details on the privacy policy and what data is collected by Gravatar at

<https://automattic.com/privacy/> . Moreover, at <https://en.gravatar.com/> you can find general information on Gravatar.

Legal basis

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

Gravatar processes data from you, among other things, in the USA. 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. More information can be found at


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


Additionally, Automattic uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Automattic commits to maintaining the European data protection level 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://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.


You can find out more about the standard contractual clauses and the data that is processed by Automattic in their Privacy Policy at <https://automattic.com/privacy/>. Moreover, you can find general information about Gravatar at <http://gravatar.com/>.

Instagram Privacy Policy


Instagram Privacy Policy Overview


 Affected parties: website visitors

 Purpose: optimising our service

 Processed data: includes data on user behaviour, information about your device and IP address.

More details can be found in the privacy policy below.

 Storage period: until Instagram no longer needs the data for its purposes

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

What is Instagram?

We have integrated functions of Instagram to our website. Instagram is a social media platform of the company Instagram LLC, 1601 Willow Rd, Menlo Park CA 94025, USA. Since 2012, Instagram is a subsidiary company of Facebook Inc. and is a part of Facebook's products. The inclusion of Instagram's contents on our website is called embedding. With this, we can show you Instagram contents such as buttons, photos or videos directly on our website. If you open websites of our online presence, that have an integrated Instagram function, data gets transmitted to, as well as stored and processed by Instagram. Instagram uses the same systems and technologies as Facebook. Therefore, your data will be processed across all Facebook firms.

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

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

Why do we use Instagram on our website?

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

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

What data is stored by Instagram?

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

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

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

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

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

The following cookies were used in our test:

Name: csrftoken

Value: ""

Purpose: This cookie is most likely set for security reasons to prevent falsifications of requests. We could not find out more information on it.

Expiry date: after one year

Name: mid

Value: ""

Purpose: Instagram places this cookie to optimise its own offers and services in- and outside of Instagram. The cookie allocates a unique user ID.

Expiry date: after end of session

Name: fbsr_121887810124024

Value: no information

Purpose: This cookie stores the login request of Instagram app users.

Expiry date: after end of session

Name: rur

Value: ATN

Purpose: This is an Instagram cookie which guarantees functionality on Instagram.

Expiry date: after end of session

Name: urlgen

Value: "{194.96.75.33": 1901};1iEtYv:Y833k2_UjKvXgYe121887810"

Purpose: This cookie serves Instagram's marketing purposes.

Expiry date: after end of session

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

How long and where are these data stored?

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

How can I erase my data or prevent data retention?

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

And this is how an Instagram account can be deleted:

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

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

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

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

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

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

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

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

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

Legal basis

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

Instagram processes data from you, among other things, in the USA. Instagram respectively 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. More information can be found at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Additionally, Instagram uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Instagram commits to maintaining the European data protection level 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://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.


We have tried to give you the most important information about data processing by Instagram. On


<https://help.instagram.com/519522125107875>


you can take a closer look at Instagram's data guidelines.

LinkedIn Privacy Policy


LinkedIn Privacy Policy Overview


 Affected parties: website visitors

 Purpose: optimisation of our service

 Processed data: includes data on user behaviour, information about your device and IP address.

More details can be found in the privacy policy below.

 Storage period: the data is generally deleted within 30 days

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

What is LinkedIn?

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

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

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

Why do we use LinkedIn on our website?

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

our offer.

What data are stored by LinkedIn?

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

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

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

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

Name: bcookie

Value: =2&34aab2aa-2ae1-4d2a-8baf-c2e2d7235c16121887810-

Purpose: This cookie is a so-called "browser ID cookie" and stores your identification number (ID).

Expiry date: after 2 years

Name: lang

Value: v=2&lang=en-gb

Purpose: This cookie saves your default or preferred language.

Expiry date: after end of session

Name: lidc

Value: 1818367:t=1571904767:s=AQF6KNnJ0G121887810...

Purpose: This cookie is used for routing. Routing records how you found your way to LinkedIn and how you navigate through the website.

Expiry date: after 24 hours

Name: rtc

Value: kt0lrv3NF3x3t6xvDgGrZGDKkX

Purpose: No further information could be found about this cookie.

Expiry date: after 2 minutes

Name: JSESSIONID

Value: ajax:1218878102900777718326218137

Purpose: This is a session cookie that LinkedIn uses to maintain anonymous user sessions through the server.

Expiry date: after end of session

Name: bscookie

Value: "v=1&201910230812...

Purpose: This cookie is a security cookie. LinkedIn describes it as a secure browser ID cookie.

Expiry date: after 2 years

Name: fid

Value: AQHj7li23ZBcqAAAA...

Purpose: We could not find any further information about this cookie.

Expiry date: after 7 days

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

How long and where are the data stored?

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

How can I delete my data or prevent data retention?

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

How to access account data in your LinkedIn profile:

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

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

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

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

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

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

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

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

Legal basis

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

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


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

https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847


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

XING Privacy Policy


Xing Privacy Policy Overview


 Affected parties: website visitors

 Purpose: optimising our service

 Processed data: your IP address and browser data, as well as the date and time of your page view

More details can be found in the privacy policy below.

 Storage period: data of Xing users are stored until deletion is requested

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

What is Xing?

On our website we use social plugins by the social media network Xing, by the company Xing SE, Dammtorstrasse 30, 20354 Hamburg, Germany. Their functions allow you to for example share content and follow interesting content on Xing directly via our website, or to log in to Xing via our site. You can recognize the plugins by the company name or the Xing logo. If you open a website that uses a Xing plugin, data can be transmitted to, and saved as well as evaluated by the “Xing server”. In this privacy policy we will inform you on what data this is and how you can manage or prevent data retention.

Xing is a social network with its headquarters in Hamburg. The company specializes in managing professional contacts. That means, that as opposed to other networks, Xing is primarily about professional networking. The platform is often used for job hunting or for companies to find employees. Moreover, Xing offers interesting content on various professional topics. The global counterpart of Xing is the American company LinkedIn.

Why do we use Xing on our website?

Nowadays, there is a flood of social media channels, and we understand that your time is very precious. It is simply not possible for you to closely follow every social media channel of a company. Therefore, we want to make your life as easy as possible and enable you to share or follow interesting content on Xing directly via our website. With these so-called “social plugins” we are expanding the service on our website. Additionally, the data collected by Xing help us to create targeted advertising on the platform. This means that our services are only displayed to people who are genuinely interested in them.

What data is stored by Xing?

As plugins for websites, Xing offers the share, follow and login buttons. As soon as you open a page with an integrated Xing social plugin, your browser will connect to servers in a Xing data centre. Xing claim that upon using the share button, no data that could directly relate to a person is stored. Furthermore, Xing do not save your IP address, neither do any cookies get set upon using the share button. This means that your user behaviour is not analysed. You can find more information at https://dev.xing.com/plugins/share_button/privacy_policy.

With Xing’s other plugins, cookies only get set in your browser if you interact with the plugin or click on it. Personal data such as your IP address, browser data, as well as the date and time of your visit

to Xing may be stored. If you have a XING account and are logged in, the collected data will be assigned to your personal account and matched with the data stored in it.

If you click on the follow or log-in button and are not yet logged in to Xing, the following cookies are set in your browser. Please keep in mind that this is an indicative list and we do not claim for it to be exhaustive:

Name: AMCVS_0894FF2554F733210A4C98C6%40AdobeOrg

Value: 1

Purpose: This cookie is used to create and store identification details for website visitors.

Expiry date: after session end

Name: c_

Value: 157c609dc9fe7d7ff56064c6de87b019121887810-8

Purpose: We were unable to find out more information on this cookie.

Expiry date: after one day

Name: prevPage

Value: wbm%2FWelcome%2Flogin

Purpose: This cookie stores the URL of the previous website you visited.

Expiry date: after 30 minutes

Name: s_cc

Value: true

Purpose: This Adobe Site Catalyst cookie determines whether cookies are generally activated in the browser.

Expiry date: after end of session

Name: s_fid

Value: 6897CDCD1013221C-39DDACC982217CD1121887810-2

Purpose: This cookie is used to identify a unique visitor.

Expiry date: after 5 years

Name: visitor_id

Value: fe59fbe5-e9c6-4fca-8776-30d0c1a89c32

Purpose: The visitor cookie contains a unique visitor ID and a unique identifier for your account.

Expiry date: after 2 years

Name: _session_id

Value: 533a0a6641df82b46383da06ea0e84e7121887810-2

Purpose: This cookie creates a temporary session ID that is used as the in-session user ID. The cookie is vital to provide the functions of Xing.

Expiry date: after end of session

When you are logged in to Xing or are a member of the platform, further personal data will be collected, processed and saved. Xing also passes personal data to third parties if it is either

necessary for its own business purposes, if you have given your consent or if there is a legal obligation.

How long and where is the data stored?

Xing stores data on different servers in various data centres. The company stores this data until you delete it or until you delete your user account. Of course, this only applies to users who are already Xing members.

How can I erase my data or prevent data retention?

You have the right to access and delete your personal data at any time. Even if you are not a Xing member, you can prevent potential data processing via your browser or manage it as you wish. Most data are stored via cookies. Depending on which browser you are using, the settings work a little different. You can find the instructions for the most common browsers here:

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

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

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

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

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

You can also set up your browser to notify you whenever a cookie is about to be placed. Then you can always decide individually whether you want to allow or deny a cookie.

Legal basis


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


We tried to make you familiar with the most important information on data processing by Xing. At <https://privacy.xing.com/en/privacy-policy> you can find out more about data processing by the social media network Xing.

Blogs and Publication Media Introduction

Blogs and Publication Media Privacy Policy Overview

 Affected parties: website visitors

 Purpose: Presentation and optimisation of our service, along with communication between website visitors, as well as security measures and administration

 Data processed: Data such as contact details, IP address and published content.
More details can be found under the tools used.

 Storage duration: depending on the tools used

 Legal basis: Article 6 paragraph 1 letter a GDPR (consent), Article 6 paragraph 1 letter f GDPR (legitimate interests), Article 6 paragraph 1 sentence 1 letter b. GDPR (contract)

What are blogs and publishing media?

We use blogs or other means of communication on our website through which we can communicate with you – and through which you can communicate with us. Your data may also be stored and processed by us. This may be necessary in order for us to display content appropriately, make communication work smoothly and increase security. In this privacy policy, we will show you general information on which of your data may be processed. The exact information on data processing, however, always depends on the tools and functions used. You will find detailed information about data processing in the privacy policies of the individual providers.

Why do we use blogs and publication media?

Our greatest motivation for our website is to offer you interesting and exciting content. At the same time, your opinions and your content are important to us. That's why we want to create a good interactive exchange between you and ourselves. With various blogs and publication options, we can achieve exactly that. You can e. g. post comments about our content, reply to others' comments or, in some cases, make posts yourself.

Which data is processed?

Exactly which data is processed always depends on the communication functions we use. Very often IP address, username and published content are stored. This is done primarily to ensure security protection, prevent spam, and for us to be able to take action against any illegal content. What is more, cookies may also be used for data retention. They are small text files that are stored as information in your browser. You can find more details about the collected and stored data in our individual sections and in the privacy policies of the respective providers.

Duration of data processing

We will inform you below about the duration of data processing, provided we have further information on this. For example, post and comment functions store data until you revoke data storage. In general, personal data is only stored for as long as is absolutely necessary for us to provide you with our services.

Right to object

You also have the right and the option to revoke your consent to the use of cookies or third-party

communication tools at any time. This can be done either via our cookie management tool or via other opt-out functions. For example, you can also prevent data collection through cookies by managing, deactivating or erasing the cookies in your browser.

Since cookies can also be used in publication media, we also recommend 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 this means of communication mainly on the basis of our legitimate interests (Art. 6 Para. 1 lit. f GDPR) in fast and good communication with you or other customers, business partners and visitors. Provided the use serves to process or initiate contractual relationships, the legal basis also extends to Article 6 Paragraph 1 Sentence 1 lit. b. GDPR.

Certain types of processing require your consent – in particular the use of cookies and comment or message functions. Provided you have consented to your data being processed and stored by integrated publication media, this consent is the legal basis for any data processing (Article 6 (1) (a) GDPR). Most communication features we use set cookies in your browser to store data. We therefore recommend you read our privacy policy on cookies carefully and consult the privacy policy or cookie policy of the relevant service provider.

Information on specific tools – if available – can be found in the following sections.

Blog Posts and Comment Functions Privacy Policy

There are various online communication tools that we may use on our website. For example, we use blog posts and comment functions. This gives you the possibility to comment on our content or to write articles. If you make use of this function, your IP address may be stored for security reasons. This is how we protect ourselves from illegal content such as insults, unauthorised advertising or prohibited political propaganda. In order to recognise whether any comments are spam, we can also store and process user information on the basis of our legitimate interests. If we start a survey, we will also store your IP address for the duration of the survey so we can be sure that everyone who takes part only votes once. Moreover, cookies may also be used for storage purposes. All data that we store about you (such as content or information about you) will be stored until you object.

WordPress-Emojis Privacy Policy

In our blog, we also use emojis and smilies. We most probably don't need to explain in more detail what emojis are. After all, you know those smiling, angry or sad faces. They are graphic elements or files that we make available, which are loaded from another server. The service provider for WordPress emojis and smilies is Automattic Inc., 60 29th Street #343, San Francisco, CA 94110, USA. This third-party provider stores your IP address in order to be able to transmit the emoji files to your browser.

Automattic processes data from you, among other things, in the USA. 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. More information can be found at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.


Additionally, Automattic uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Automattic commits to maintaining the European data protection level 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://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

You can find more information about the standard contractual clauses at Automattic at <https://wordpress.com/support/data-processing-agreements/>.


You can find out more about the data that is processed by using WordPress-Emojis in their Privacy Policy at <https://automattic.com/privacy/>.

Content Delivery Networks


Content Delivery Networks Privacy Policy Overview


 Affected parties: website visitors

 Purpose: Service performance optimisation (to increase website loading speeds)

 Processed data: data such as your IP address

You can find more details on this below as well as in the individual Privacy Policies.

 Storage period: most data is stored until it is no longer needed for the provision of the service.

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

What is a Content Delivery Network?

On our website we use a so-called content delivery network or CDN. This helps to load our website quickly and easily, regardless of your location. Moreover, your personal data will also be stored, managed and processed on the respective CDN provider's servers. In the following, we will go into more general detail on this service and the data processing associated with it. You can find detailed information on how your data is handled in the provider's Privacy Policy.

Each content delivery network (CDN) is a network of regionally distributed servers that are connected to each other via the internet. Through this network, website content (especially very large files) can be delivered quickly and smoothly, even when large loading peaks occur. To make this possible, CDNs create a copy of our website on their servers. The website can be delivered quickly because these servers are distributed all around the world. Any data transfer to your

browser is therefore significantly shortened by the CDN.

Why do we use a Content Delivery Network for our website?

A fast loading website is part of our service. Of course, we know how annoying it is when a website loads at a snail's pace. Most of the time, you lose your patience and click away before the website is fully loaded. But of course we want to avoid that. Therefore, to us a fast loading website is an obligatory part of our website offer. With the use of a content delivery network, our website loads significantly faster in your browser. Furthermore, CDNs are particularly helpful when you are abroad, as the website is always delivered from a server in your area.

Which data are processed?

If you access a website or its content and it gets cached in a CDN, the CDN forwards the request to the server closest to you which then delivers the content. Content delivery networks are built in a way that JavaScript libraries can be downloaded and hosted on npm and Github servers. Alternatively, WordPress plugins can also be loaded on most CDNs, provided they are hosted on WordPress.org. Moreover, your browser can send personal data to the content delivery network we use. This includes data such as IP addresses, browser type, browser version, the accessed website or the time and date of the page visit. This data is collected and stored by the CDN. Whether cookies are used for data storage depends on the network that is being used. For more information on this, please read the Privacy Policy of the respective service.

Right to object

If you want to prevent this data transfer altogether, you can use a JavaScript blocker (see for example <https://noscript.net/>) on your computer. However, our website can then of course no longer offer its usual service (such as a fast loading speeds).

Legal basis


If you have consented to the use of a content delivery network, your consent represents the the legal basis for the corresponding data processing. According to **Art. 6 paragraph 1 lit. a (consent)** your consent represents the legal basis for the processing of personal data, as it can occur when collected by a content delivery network.


We also have a legitimate interest in using a content delivery network to optimise our online service and make it more secure. The corresponding legal basis for this is **Art. 6 para. 1 lit. f GDPR (legitimate interests)**. Nevertheless, we only use the tool if you have consented to it.


Provided this information is available, you can find out more about the particular content delivery networks in the following sections.


Cookie Consent Management Platform


Cookie Consent Management Platform Overview

 Affected parties: Website visitors

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

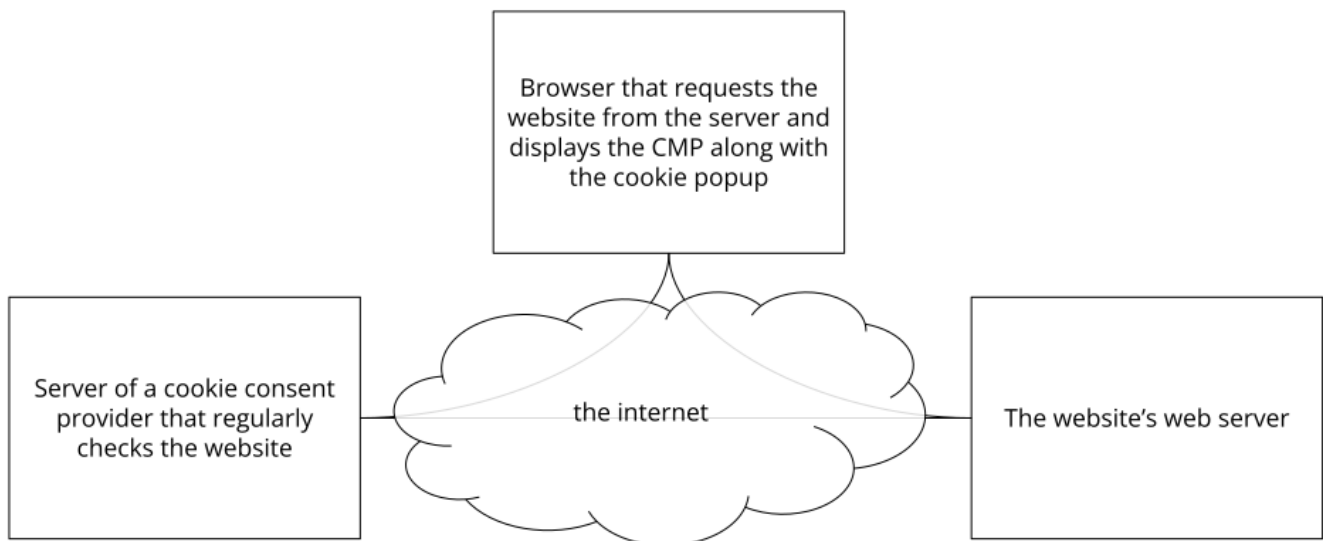
 Processed data: data for managing cookie settings such as IP address, time of consent, type of consent and individual consent. You can find more details on this directly with the tool that is being used.

 Storage period: depends on the tool used, periods of several years can be assumed

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

What is a cookie consent management platform?

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



Why do we use a cookie management tool?

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

Which data are processed?

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

Duration of data processing

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

Right of objection

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


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


Legal basis


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

Security & Anti-spam


Security & Anti-Spam Privacy Policy Overview

 Affected parties: website visitors

 Purpose: for cyber security

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

More details can be found below and in the individual privacy policies.

 Duration of storage: In most cases, data is stored until it is no longer required in order to provide the service

 Legal bases: Article 6 paragraph 1 lit. a GDPR (consent), Article 6 paragraph 1 lit. f GDPR (legitimate interests)

What is Security & Anti-spam software?

So-called security & Anti-spam software can protect you and us from various spam or phishing emails and other potential cyber-attacks. Spam includes advertising emails from mass mailings that you did not sign up for yourself. Such emails are also called data garbage and can also cause costs. Other spam such as phishing emails, on the other hand, are messages that aim to gain trust via fake messages or websites in order to obtain personal information. Anti-spam software usually protects against unwanted spam messages or malicious emails that could inject viruses into our system. We also use general firewall and security systems that protect our devices from unwanted network attacks.

Why do we use Security & Anti-spam software?

We put great importance on our website's security. After all, this is not just about our safety, but also about your safety. Unfortunately, cyber threats are now part of everyday life in the world of IT and the internet. Hackers e. g. often try to steal personal data from IT systems with the help of cyber attacks. And therefore a good defence system is absolutely necessary. A security system monitors all incoming and outgoing connections to our network or computer. In order to achieve even greater security against cyber attacks, we also use other external security services on our devices in addition to standardised security systems. Unauthorised data transmissions are thus better prevented and this is how we protect ourselves from cybercrime.

Which data are processed by Security & Anti-spam software?

The data that is collected and stored of course depends on the respective service. However, we always try to only use programs that collect data very sparingly or only store data that is necessary for the fulfilment of the offered service. In general, the service may store data such as name, address, IP address, email address and technical data such as browser type or browser version. Any performance and log data may also be collected in order to identify possible incoming threats in good time. This data will be processed as part of the provided services and in compliance with applicable laws. This also includes the GDPR for US providers (via the Standard Contractual Clauses). In some cases, security services also work with third parties who may store and/or process data under instructions and in accordance with privacy policies and other security measures. Data is usually stored using cookies.

Duration of data processing

We will inform you below about the duration of data processing, provided we have further information on this. For example, security programs store data until you or we revoke 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 have precise information from the providers about their data storage periods.

Right to object

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

Since cookies may also be used with security services, we recommend you read our 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 security services mainly on the basis of our legitimate interests (Art. 6 Para. 1 lit. f GDPR) in a good security system and protection against various cyber attacks.

Certain data processing requires your consent – in particular, the use of cookies and security functions. If you have agreed to the processing and storage of your data by integrated security services, your consent is the legal basis for data processing (Article 6 (1) (a) GDPR). Most of the services we use set cookies on your browser to store data. We, therefore, recommend you read our privacy policy on cookies carefully and consult the privacy policy or cookie policy of the relevant service provider.

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

Google reCAPTCHA Privacy Policy

Google reCAPTCHA Privacy Policy Overview

-  Affected parties: website visitors
 -  Purpose: Service optimisation and protection against cyber attacks
 -  Processed data: data such as IP address, browser information, operating system, limited location and usage data
- You can find more details on this in the Privacy Policy below.
-  Storage duration: depending on the retained data
 -  Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is reCAPTCHA?

Our primary goal is to provide you an experience on our website that is as secure and protected as possible. To do this, we use Google reCAPTCHA from Google Inc. (1600 Amphitheater Parkway Mountain View, CA 94043, USA). With reCAPTCHA we can determine whether you are a real person from flesh and bones, and not a robot or a spam software. By spam we mean any electronically undesirable information we receive involuntarily. Classic CAPTCHAS usually needed you to solve text or picture puzzles to check. But thanks to Google's reCAPTCHA you usually do have to do such puzzles. Most of the times it is enough to simply tick a box and confirm you are not a bot. With the new Invisible reCAPTCHA version you don't even have to tick a box. In this privacy policy you will find out how exactly this works, and what data is used for it.

reCAPTCHA is a free captcha service from Google that protects websites from spam software and misuse by non-human visitors. This service is used the most when you fill out forms on the Internet. A captcha service is a type of automatic Turing-test that is designed to ensure specific actions on the Internet are done by human beings and not bots. During the classic Turing-test (named after computer scientist Alan Turing), a person differentiates between bot and human. With Captchas, a computer or software program does the same. Classic captchas function with small tasks that are easy to solve for humans but provide considerable difficulties to machines. With reCAPTCHA, you no longer must actively solve puzzles. The tool uses modern risk techniques to distinguish people from bots. The only thing you must do there, is to tick the text field "I am not a robot". However, with Invisible reCAPTCHA even that is no longer necessary. reCAPTCHA, integrates a JavaScript element into the source text, after which the tool then runs in the background and analyses your user behaviour. The software calculates a so-called captcha score from your user actions. Google uses this score to calculate the likelihood of you being a human, before entering the captcha. reCAPTCHA and Captchas in general are used every time bots could manipulate or misuse certain actions (such as registrations, surveys, etc.).

Why do we use reCAPTCHA on our website?

We only want to welcome people from flesh and bones on our side and want bots or spam software of all kinds to stay away. Therefore, we are doing everything we can to stay protected and to offer you the highest possible user friendliness. For this reason, we use Google reCAPTCHA from Google. Thus, we can be pretty sure that we will remain a "bot-free" website. Using reCAPTCHA, data is transmitted to Google to determine whether you genuinely are human. reCAPTCHA thus ensures our website's and subsequently your security. Without reCAPTCHA it could e.g. happen that a bot would register as many email addresses as possible when registering, in order to subsequently "spam" forums or blogs with unwanted advertising content. With reCAPTCHA we can avoid such bot attacks.

What data is stored by reCAPTCHA?

reCAPTCHA collects personal user data to determine whether the actions on our website are made by people. Thus, IP addresses and other data Google needs for its reCAPTCHA service, may be sent to Google. Within member states of the European Economic Area, IP addresses are almost always compressed before the data makes its way to a server in the USA. Moreover, your IP address will

not be combined with any other of Google's data, unless you are logged into your Google account while using reCAPTCHA. Firstly, the reCAPTCHA algorithm checks whether Google cookies from other Google services (YouTube, Gmail, etc.) have already been placed in your browser. Then reCAPTCHA sets an additional cookie in your browser and takes a snapshot of your browser window.

The following list of collected browser and user data is not exhaustive. Rather, it provides examples of data, which to our knowledge, is processed by Google.

- Referrer URL (the address of the page the visitor has come from)
- IP-address (z.B. 256.123.123.1)
- Information on the operating system (the software that enables the operation of your computers. Popular operating systems are Windows, Mac OS X or Linux)
- Cookies (small text files that save data in your browser)
- Mouse and keyboard behaviour (every action you take with your mouse or keyboard is stored)
- Date and language settings (the language and date you have set on your PC is saved)
- All Javascript objects (JavaScript is a programming language that allows websites to adapt to the user. JavaScript objects can collect all kinds of data under one name)
- Screen resolution (shows how many pixels the image display consists of)

Google may use and analyse this data even before you click on the "I am not a robot" checkmark. In the Invisible reCAPTCHA version, there is no need to even tick at all, as the entire recognition process runs in the background. Moreover, Google have not given details on what information and how much data they retain.

The following cookies are used by reCAPTCHA: With the following list we are referring to Google's reCAPTCHA demo version at <https://www.google.com/recaptcha/api2/demo>.

For tracking purposes, all these cookies require a unique identifier. Here is a list of cookies that Google reCAPTCHA has set in the demo version:

Name: IDE

Value: WqTUmlnmv_qXyi_DGNPLESKnRNrpgXoy1K-pAZtAkMbHI-121887810-8

Purpose: This cookie is set by DoubleClick (which is owned by Google) to register and report a user's interactions with advertisements. With it, ad effectiveness can be measured, and appropriate optimisation measures can be taken. IDE is stored in browsers under the domain doubleclick.net.

Expiry date: after one year

Name: 1P_JAR

Value: 2019-5-14-12

Purpose: This cookie collects website usage statistics and measures conversions. A conversion e.g. takes place, when a user becomes a buyer. The cookie is also used to display relevant adverts to users. Furthermore, the cookie can prevent a user from seeing the same ad more than once.

Expiry date: after one month

Name: ANID

Value: U7j1v3dZa1218878100xgZFmiqWppRWKOr

Purpose: We could not find out much about this cookie. In Google's privacy statement, the cookie is mentioned in connection with "advertising cookies" such as "DSID", "FLC", "AID" and "TAID". ANID is stored under the domain google.com.

Expiry date: after 9 months

Name: CONSENT

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

Purpose: This cookie stores the status of a user's consent to the use of various Google services. CONSENT also serves to prevent fraudulent logins and to protect user data from unauthorised attacks.

Expiry date: after 19 years

Name: NID

Value: 0WmuWqy121887810zILzqV_nmt3sDXwPeM5Q

Purpose: Google uses NID to customise advertisements to your Google searches. With the help of cookies, Google "remembers" your most frequently entered search queries or your previous ad interactions. Thus, you always receive advertisements tailored to you. The cookie contains a unique ID to collect users' personal settings for advertising purposes.

Expiry date: after 6 months

Name: DV

Value: gEAABBCjJMXcl0dSAAAANbqc121887810-4

Purpose: This cookie is set when you tick the "I am not a robot" checkmark. Google Analytics uses the cookie personalised advertising. DV collects anonymous information and is also used to distinct between users.

Expiry date: after 10 minutes

Note: We do not claim for this list to be extensive, as Google often change the choice of their cookies.

How long and where are the data stored?

Due to the integration of reCAPTCHA, your data will be transferred to the Google server. Google have not disclosed where exactly this data is stored, despite repeated inquiries. But even without confirmation from Google, it can be assumed that data such as mouse interaction, length of stay on a website or language settings are stored on the European or American Google servers. The IP address that your browser transmits to Google does generally not get merged with other Google data from the company's other services.

However, the data will be merged if you are logged in to your Google account while using the reCAPTCHA plug-in. Google's diverging privacy policy applies for this.

How can I erase my data or prevent data retention?

If you want to prevent any data about you and your behaviour to be transmitted to Google, you must fully log out of Google and delete all Google cookies before visiting our website or use the

reCAPTCHA software. Generally, the data is automatically sent to Google as soon as you visit our website. To delete this data, you must contact Google Support at <https://support.google.com/?hl=en-GB&tid=121887810>.

If you use our website, you agree that Google LLC and its representatives automatically collect, edit and use data.

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

Legal basis

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

We also have a legitimate interest in using Google reCAPTCHA to optimise our online service and make it more secure. The corresponding 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 to it.

Google processes data from you, among other things, in the USA. 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. More information can be found at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Additionally, Google uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Google commits to maintaining the European data protection level 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://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

You can find the Google Ads Data Processing Terms, which refer to the Standard Contractual Clauses, at: <https://business.safety.google/intl/en/adsprocessor/terms/>

You can find out a little more about reCAPTCHA on Google's web developer page at <https://developers.google.com/recaptcha/>. Google goes into the technical development of the reCAPTCHA in more detail here, but you will look in vain for detailed information about data storage and data protection issues. A good overview of the basic use of data by Google can be found in the in-house data protection declaration at <https://policies.google.com/privacy?hl=en-GB>.

hCaptcha Privacy Policy

We use hCaptcha, a security management tool, for our website. The service provider is the American company Intuition Machines Inc., 350 Alabama St, San Francisco, CA 94110, USA.

Intuition Machines processes data from you, among other things, in the USA. Intuition Machines 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. More information can be found at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Additionally, Intuition Machines uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Intuition Machines commits to maintaining the European data protection level 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://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

The Data Processing Agreements, which refer to the standard contractual clauses, can be found at <https://newassets.hcaptcha.com/dpa/IMI.DPA.9.23.21.New.SCCs.pdf>.

You can find out more about the data processed using hCaptcha in the privacy policy at <https://www.hcaptcha.com/privacy>.

Wordfence Privacy Policy

We use Wordfence, a WordPress security plug-in, for our website. The service provider is the American company Defiant, Inc., 1700 Westlake Ave N Ste 200, Seattle, WA 98109, USA.

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


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


The General Data Protection Regulation, which corresponds to the standard contractual clauses, can be found at <https://www.wordfence.com/help/general-data-protection-regulation/>.


You can learn more about the data processed using Wordfence in the Privacy Policy at <https://www.wordfence.com/privacy-policy/>.

Cloud Services


Cloud Services Privacy Policy Overview

 Affected parties: We as the website operator and you as the website visitor

 Purpose: security and data storage

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

More details can be found below and in the individual privacy policies or in the privacy policies of the providers

 Duration of storage: In most cases, data is stored until it is no longer required in order to provide the service

 Legal bases: Article 6 paragraph 1 lit. a GDPR (consent), Article 6 paragraph 1 lit. f GDPR (legitimate interests)

What are cloud services?

As a website operator, cloud services provide us with storage space and computing power via the internet. Data can be transmitted to an external system, where it may be processed and stored via the internet. The relevant cloud provider manages this data. Depending on specific requirements, an individual or a company can choose storage space or computing power. Cloud storage is accessed via an API or via storage protocols. API stands for Application Programming Interface, which is a programming interface that connects software with hardware components.

Why do we use cloud services?

We use cloud services for several reasons. A cloud service offers us the opportunity to store our data securely. In addition, we can access the data from different locations and devices, giving us more flexibility and simplifying our work processes. Cloud storage also saves us costs because we don't have to set up and manage our own infrastructure for data storage and data security. By storing our data centrally in the cloud, we can also expand our application fields and manage our information much better.

As website operator or company, we use cloud services primarily for our own purposes. We e. g. manage our calendar and store documents or other important information in the cloud. However, your personal data may also be stored. This can take place if you provide us with your contact details (e.g. name and email address) while we store our customer data with a cloud provider. Consequently, any of your data we process may also be stored and processed on external servers. Provided we offer certain forms of content by cloud services on our website, cookies can also be set for web analysis and advertising purposes. Furthermore, such cookies retain your settings (e.g. the language used) so you will be provided with your usual web environment next time you visit our website.

Which data is processed by cloud services?

Much of the data we store in the cloud cannot be used to identify you as a person, but some data is personal data as defined by the GDPR. This is often customer data such as name, address, IP address or telephone number or technical device information. Videos, images and audio files may also be stored in the cloud. Exactly how the data is collected and stored depends on the respective service. We only try to use services that handle your data in a very reliable and professional manner. Generally, services such as Amazon Drive, have access to the stored files in order to be able to offer their own service accordingly. For this, however, the services require consent (such as for the right to copy files for security reasons). The data will be processed and handled as part of the provided services and in compliance with applicable laws. This also includes compliance with the GDPR for US providers (via the standard contractual clauses). In some cases, cloud services also cooperate with third parties who may process data under instructions and in accordance with privacy policies and other security measures. At this point we would like to emphasise again that all well-known cloud services (such as Amazon Drive, Google Drive or Microsoft OneDrive) obtain the right to access stored content in order to be able to offer and optimise their own services accordingly.

Duration of data processing

We will inform you below about the duration of data processing, provided we have further information on this. In general, cloud services store data until you or we revoke the data storage or erase the retained data. In general, personal data is only stored for as long as it is necessary for the provision of the respective services. However, it may take up to several months to erase your data from the cloud. This may occur because data is usually not only stored on one server but divided between different servers.

Right to object

You also have the right and the opportunity to revoke your consent to data storage in a cloud at any time. If cookies are used, you also have a right to withdraw your consent. This can be done either via our cookie management tool or via other opt-out functions. For example, you can also prevent data collection through cookies by managing, deactivating or erasing the cookies in your browser. We also recommend 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 policy of the respective cloud provider.

Legal Basis

We use cloud services mainly on the basis of our legitimate interests (Art. 6 Para. 1 lit. f GDPR) in good security and storage systems.


Certain types of processing, in particular the use of cookies and storage functions, require your consent. If you have consented to your data being processed and stored by cloud services, this consent is the legal basis for data processing (Article 6 (1) (a) GDPR). Most of the services we use place cookies in your browser to store data. Thus, we recommend you read our privacy policy on

cookies carefully and study the privacy policy or cookie policy of the relevant service provider.


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

Audio & Video


Audio & Video Privacy Policy Overview


 Affected parties: website visitors

 Purpose: service optimisation

 Processed data: Data such as contact details, user behaviour, device information and IP addresses can be stored.

You can find more details in the Privacy Policy below.

 Storage period: data are retained for as long as necessary for the provision of the service

 Legal bases: 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 to our website. Therefore, you can watch videos or listen to music/podcasts directly via our website. This content is delivered by service providers and is obtained from the respective providers' servers.

Audio and video elements are integrated functional elements of platforms such as YouTube, Vimeo or Spotify. It is usually free of charge to use these portals, but they can also contain paid content. With the integrated elements, you can listen to or view any of their content on our website.

If you use audio or video elements on our website, your personal data may get transmitted to as well as processed and retained by service providers.

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

We of course 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 just giving you a link to a video, we offer you audio and video formats directly on our website. These are entertaining or informative, but ideally they are both. Our service therefore gets expanded and it gets easier for you to access interesting content. In addition to our texts and images, we thus also offer video and/or audio content.

Which data are retained by audio & video elements?

When you visit a page on our website with e.g. an embedded video, your server connects to the service provider's server. Thus, your data will also be transferred to the third-party provider, where it will be stored. Certain 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 device. Most providers also collect information on your web activity. This e.g. includes the session duration, bounce rate, the buttons you clicked or information about the website you are using the service on. This data is mostly stored via cookies

or pixel tags (also known as web beacons). Any data that is pseudonymised usually gets stored in your browser via cookies. In the respective provider's Privacy Policy, you can always find more information on the data that is stored and processed.

Duration of data processing

You can find out exactly how long the data is stored on the third-party provider's servers either in a lower point of the respective tool's Privacy Policy or in the provider's Privacy Policy. Generally, personal data is only processed for as long as is absolutely necessary for the provision of our services or products. This usually also applies to third-party providers. In most cases, you can assume that certain data will be stored on third-party providers' servers for several years. Data can be retained for different amounts of time, especially when stored in cookies. Some cookies are deleted after you leave a website, while others may be stored in your browser for a few years.

Right to object

You also retain the right and the option to revoke your consent to the use of cookies or third-party providers at any time. This can be done either via our cookie management tool or via other opt-out functions. You can e.g. also prevent data retention via cookies by managing, deactivating or erasing cookies in your browser. The legality of the processing up to the point of revocation remains unaffected.


Since the integrated audio and video functions on our site usually also use cookies, we recommend you to 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 the processing and storage of your data by integrated audio and video elements, your consent is considered the legal basis for data processing (**Art. 6 Para. 1 lit. a GDPR**). Generally, your data is also stored and processed on the basis of our legitimate interest (**Art. 6 Para. 1 lit. f GDPR**) in maintaining fast and good communication with you or other customers and business partners. We only use the integrated audio and video elements if you have consented to it.

Vimeo Privacy Policy


Vimeo Privacy Policy Overview


 Affected parties: website visitors

 Purpose: optimising our service

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

You can find more details on this in privacy policy below.

 Storage period: data are generally stored for as long as is necessary 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 Vimeo?

On our website, we use videos of the company Vimeo. This video portal is operated by Vimeo LLC, 555 West 18th Street, New York, New York 10011, USA. With the help of a plug-in, we can display interesting video material directly on our website. Consequently, some of your data may be transmitted to Vimeo. In this privacy policy we want to explain to you what data this is, why we use Vimeo and how you can manage your data or prevent data transmission.

Vimeo is a video platform that was founded in 2004 and introduced video streaming in HD quality in 2007. Since 2015 it has been possible to stream in 4k Ultra HD. The use of the portal is free of charge, but it also contains certain paid content. Compared to the market leader YouTube, Vimeo attaches great importance to valuable content in good quality. On the one hand, the portal offers a lot of artistic content such as music videos and short films. On the other hand, it also offers useful documentaries on a broad spectrum of topics.

Why do we use Vimeo on our website?

The aim of our website is to provide you the best possible content, in the easiest and most accessible way we can. We will only be satisfied with our service, once we have reached that goal. The video service Vimeo supports us in achieving this goal. Vimeo gives us the opportunity to present high quality content to you directly on our website. Instead of us merely giving you a link to an interesting video, you can watch the video here with us. This extends our service and makes it easier for you to access interesting content. Therefore, in addition to our texts and images, we can also offer video content.

What data is stored on Vimeo?

When you open a site on our website that has a Vimeo video embedded to it, your browser will connect to Vimeo's servers, and a data transmission will take place. The data are then collected, stored and processed on Vimeo's servers. Regardless of whether you have a Vimeo account or not, Vimeo collects data about you. This includes your IP address, technical information about your browser type, your operating system or very basic device information. Furthermore, Vimeo store information on what website you use their service on and which actions (web activities) you carry out on our website. These web activities include e.g. session duration, bounce rate or which button you clicked on our site that contains a Vimeo function. Vimeo can track and store these actions using cookies and similar technologies.

If you are logged in as a registered member of Vimeo, more data may be collected, since a bigger number of cookies may already have been set in your browser. Furthermore, your actions on our website are directly linked to your Vimeo account. To prevent this, you must log out of Vimeo while "surfing" our website.

Below we will show you an array of cookies Vimeo sets when you are on a website containing an integrated Vimeo function. This list is not exhaustive and assumes that you do not have a Vimeo account.

Name: player

Value: ""

Purpose: This cookie saves your settings before you play an embedded Vimeo video. This will ensure you to receive your preferred settings again next time you watch a Vimeo video.

Expiry date: after one year

Name: vuid

Value: pl1046149876.614422590121887810-4

Purpose: This cookie collects information about your actions on websites that have a Vimeo video embedded to them.

Expiry date: after 2 years

Note: These two cookies are set every time as soon as you are on a website that has a Vimeo video embedded to it. If you watch the video and click a button such as "share" or "like", additional cookies will be set. These can also be third-party cookies such as `_ga` or `_gat_UA-76641-8` from Google Analytics or `_fbp` from Facebook. The exact cookies that are set depends on your interaction with the video.

The following list will show a selection of cookies that could be placed when you interact with a Vimeo video:

Name: `_abexps`

Value: `%5B%5D`

Purpose: This Vimeo cookie helps Vimeo to remember your settings. For example, this can be a pre-set language, a region or a username. The cookie generally stores data on how you use Vimeo.

Expiry date: after one year

Name: `continuous_play_v3`

Value: `1`

Purpose: This cookie is a first-party cookie from Vimeo. The cookie collects information on how you use Vimeo's service. For example, the cookie stores details on when you pause a video and resume it.

Expiry date: after one year

Name: `_ga`

Value: `GA1.2.1522249635.1578401280121887810-7`

Purpose: This cookie is a third-party cookie from Google. By default, `analytics.js` uses the `_ga` cookie to store the user ID. Thus, it serves to differentiate between website visitors.

Expiry date: after 2 years

Name: `_gcl_au`

Value: `1.1.770887836.1578401279121887810-3`

Purpose: This third-party cookie from Google AdSense is used to improve the efficiency of ads on websites.

Expiry date: after 3 months

Name: `_fbp`

Value: fb.1.1578401280585.310434968

Purpose: This is a Facebook cookie. It is used to display adverts or advertising products from Facebook or other advertisers.

Expiry date: after 3 months

Vimeo use this data to improve their own service, to communicate with you and to implement their own targeted advertising measures. On their website they emphasise that only first-party cookies (i.e. cookies from Vimeo itself) are used for embedded videos, provided you do not interact with the video.

How long and where is the data stored?

Vimeo is headquartered in White Plains, New York (USA). However, their services are offered worldwide. For this, the company uses computer systems, databases and servers in the United States and other countries. Thus, your data may also be stored and processed on servers in America. Vimeo stores the data until the company no longer has an economical reason for keeping it. Then the data will be deleted or anonymised. Vimeo correspond to the EU-U.S. Privacy Shield Framework and are therefore allowed to collect and use information from users within the EU, and to transfer this data to the USA.

How can I erase my data or prevent data retention?

You always have the option to manage cookies in your browser. If you do not want Vimeo to set cookies and collect information about you for example, you can delete or deactivate cookies in your browser settings at any time. These settings vary a little depending on the browser. Please note that after deactivating/deleting cookies, various functions may no longer be fully available. The following instructions show how you can manage or delete cookies in your browser.

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

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

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

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

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

If you are a registered Vimeo member, you can also manage cookies in Vimeo's settings.

Legal basis

If you have consented to the processing and storage of your data by integrated Vimeo elements, this consent is the legal basis for data processing (**Art. 6 para. 1 lit. a GDPR**). Generally, your data is also stored and processed on the basis of our legitimate interest (**Art. 6 para. 1 lit. f GDPR**) to maintain fast and good communication with you or other customers and business partners. Nevertheless, we only use integrated Vimeo elements if you have given your consent. Vimeo also

sets cookies in your browser to store data. We therefore recommend you to read our privacy policy on cookies carefully and to take a look at the privacy policy or the cookie policy of the respective service provider.

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


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

https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847


You can find out more about the use of cookies at Vimeo at https://vimeo.com/cookie_policy. Furthermore, you can find more information on privacy at Vimeo at <https://vimeo.com/privacy>.

YouTube Privacy Policy


YouTube Privacy Policy Overview


 Affected parties: website visitors

 Purpose: optimising our service

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

You can find more details on this in the privacy policy below.

 Storage period: data are generally stored for as long as is necessary for the purpose of the service

 Legal bases: 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 to our website. Therefore, we can show you interesting videos directly on our site. YouTube is a video portal, which has been a subsidiary company of Google LLC since 2006. The video portal is operated by YouTube, LLC, 901 Cherry Ave., San Bruno, CA 94066, USA. When you visit a page on our website that contains an embedded YouTube video, your browser automatically connects to the servers of YouTube or Google. Thereby, certain data are transferred (depending on the settings). Google is responsible for YouTube's data processing and therefore Google's data protection applies.

In the following we will explain in more detail which data is processed, why we have integrated YouTube videos and how you can manage or clear your data.

On YouTube, users can watch, rate, comment or upload videos for free. Over the past few years,

YouTube has become one of the most important social media channels worldwide. For us to be able to display videos on our website, YouTube provides a code snippet that we have integrated to our website.

Why do we use YouTube videos on our website?

YouTube is the video platform with the most visitors and best content. We strive to offer you the best possible user experience on our website, which of course includes interesting videos. With the help of our embedded videos, we can provide you other helpful content in addition to our texts and images. Additionally, embedded videos make it easier for our website to be found on the Google search engine. Moreover, if we place ads via Google Ads, Google only shows these ads to people who are interested in our offers, thanks to the collected data.

What data is stored by YouTube?

As soon as you visit one of our pages with an integrated YouTube, YouTube places at least one cookie that stores your IP address and our URL. If you are logged into your YouTube account, by using cookies YouTube can usually associate your interactions on our website with your profile. This includes data such as session duration, bounce rate, approximate location, technical information such as browser type, screen resolution or your Internet provider. Additional data can include contact details, potential ratings, shared content via social media or YouTube videos you added to your favourites.

If you are not logged in to a Google or YouTube account, Google stores data with a unique identifier linked to your device, browser or app. Thereby, e.g. your preferred language setting is maintained. However, many interaction data cannot be saved since less cookies are set.

In the following list we show you cookies that were placed in the browser during a test. On the one hand, we show cookies that were set without being logged into a YouTube account. On the other hand, we show you what cookies were placed while being logged in. We do not claim for this list to be exhaustive, as user data always depend on how you interact with YouTube.

Name: YSC

Value: b9-CV6ojl5Y121887810-1

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

Expiry date: after end of session

Name: PREF

Value: f1=50000000

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

Expiry date: after 8 months

Name: GPS

Value: 1

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

Expiry date: after 30 minutes

Name: VISITOR_INFO1_LIVE

Value: 95Chz8bagyU

Purpose: This cookie tries to estimate the user's internet bandwidth on our sites (that have built-in YouTube videos).

Expiry date: after 8 months

Further cookies that are placed when you are logged into your YouTube account:

Name: APISID

Value: zILlvClZSkqGsSwI/AU1aZI6HY7121887810-

Purpose: This cookie is used to create a profile on your interests. This data is then used for personalised advertisements.

Expiry 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 also provides safety measures to protect users from unauthorised attacks.

Expiry date: after 19 years

Name: HSID

Value: AcRwpgUik9Dveht0I

Purpose: This cookie is used to create a profile on your interests. This data helps to display customised ads.

Expiry date: after 2 years

Name: LOGIN_INFO

Value: AFmmF2swRQIhALl6aL...

Purpose: This cookie stores information on your login data.

Expiry date: after 2 years

Name: SAPISID

Value: 7oaPxoG-pZsjuuF5/AnUdDUlsj9Ijz2vdM

Purpose: This cookie identifies your browser and device. It is used to create a profile on your interests.

Expiry date: after 2 years

Name: SID

Value: oQfNKjAsI121887810-

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

Expiry date: after 2 years

Name: SIDCC

Value: AN0-TYuqub2JOcDTyL

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

Expiry date: after 3 months

How long and where is the data stored?

The data YouTube receive and process on you are stored on Google's servers. Most of these servers are in America. At <https://www.google.com/about/datacenters/locations/?hl=en> you can see where Google's data centres are located. Your data is distributed across the servers. Therefore, the data can be retrieved quicker and is better protected against manipulation.

Google stores collected data for different periods of time. You can delete some data anytime, while other data are automatically deleted after a certain time, and still other data are stored by Google for a long time. Some data (such as elements on "My activity", photos, documents or products) that are saved in your Google account are stored until you delete them. Moreover, you can delete some data associated with your device, browser, or app, even if you are not signed into a Google Account.

How can I erase my data or prevent data retention?

Generally, you can delete data manually in your Google account. Furthermore, in 2019 an automatic deletion of location and activity data was introduced. Depending on what you decide on, it deletes stored information either after 3 or 18 months.

Regardless of whether you have a Google account or not, you can set your browser to delete or deactivate cookies placed by Google. These settings vary depending on the browser you use. The following instructions will show how to manage cookies in your browser:

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

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

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

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

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

If you generally do not want to allow any cookies, you can set your browser to always notify you when a cookie is about to be set. This will enable you to decide to either allow or permit each individual cookie.

Legal basis

If you have consented processing and storage of your data by integrated YouTube elements, this consent is the legal basis for data processing (**Art. 6 para. 1 lit. a GDPR**). Generally, your data is also stored and processed on the basis of our legitimate interest (**Art. 6 para. 1 lit. f GDPR**) to maintain fast and good communication with you or other customers and business partners.

Nevertheless, we only use integrated YouTube elements if you have given your consent. YouTube also sets cookies in your browser to store data. We therefore recommend you to read our privacy policy on cookies carefully and to take a look at the privacy policy or the cookie policy of the respective service provider.

Google processes data from you, among other things, in the USA. 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. More information can be found at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Additionally, Google uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Google commits to maintaining the European data protection level 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://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

You can find the Google Ads Data Processing Terms, which refer to the Standard Contractual Clauses, at: <https://business.safety.google/intl/en/adsprocessor/terms/>

Since YouTube is a subsidiary company of Google, Google's privacy statement applies to both. If you want to learn more about how your data is handled, we recommend the privacy policy at <https://policies.google.com/privacy?hl=en>.

YouTube Subscribe Button Privacy Policy

We have integrated the YouTube subscribe button to our website, which you can recognise by the classic YouTube logo. The logo shows the words "Subscribe" or "YouTube" in white letters against a red background, with a white "Play" symbol on the left. The button may also be displayed in a different design.

Our YouTube channel consistently offers you funny, interesting or exciting videos. With the built-in "Subscribe" button you can subscribe to our channel directly via our website and do not need to go to YouTube's website for it. With this feature, we want to make it as easy as possible for you to access our comprehensive content. Please note that YouTube may save and process your data.

If you see a built-in subscription button on our page, YouTube sets at least one cookie, according to Google. This cookie stores your IP address and our URL. It also allows YouTube to receive information about your browser, your approximate location and your default language. In our test the following four cookies were placed, without us being logged into YouTube:

Name: YSC

Value: b9-CV6ojl5121887810Y

Purpose: This cookie registers a unique ID, which stores statistics of the viewed video.

Expiry date: after end of session

Name: PEF

Value: f1=50000000

Purpose:This cookie also registers your unique ID. Google uses PEF to get statistics on how you interact with YouTube videos on our website.

Expiry date: after 8 months

Name: GPS

Value: 1

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

Expiry date: after 30 minutes

Name: VISITOR_INFO1_LIVE

Value: 12188781095Chz8bagyU

Purpose: This cookie tries to estimate the user's internet bandwidth on our website (that contain built-in YouTube video).

Expiry date: after 8 months


Note: These cookies were set after a test, thus we do not claim for the list to be exhaustive.


If you are logged into your YouTube account, YouTube may store many of the actions and interactions you make on our website via cookies, to then assign them to your YouTube account. This gives YouTube information on e.g. how long you have been browsing our website, which browser type you use, which screen resolution you prefer or what actions you take.


On the one hand, YouTube uses this data to improve its own services and offers, and on the other hand to provide analyses and statistics for advertisers (who use Google Ads).


Review Platforms Overview

Review Platforms Overview

 Affected parties: Website or rating platform visitors

 Purpose: Feedback on our products and/or services

 Processed data: IP address, email address and name, among other things. You can find more details below or directly on the respective review platforms.

 Storage duration: depends on the respective platform

 Legal bases: Article 6 paragraph 1 lit. a GDPR (consent), Article 6 paragraph 1 lit. f GDPR (legitimate interests),

What are review platforms?

You can rate our products or services on various review platforms. We are registered on some of these platforms so we can get feedback from you, which can help us to optimise our offer. If you rate us via a review platform, the Privacy Policy and the General Terms and Conditions of the respective review service apply. In many instances, you also have to register in order to submit a

review. We may also have rating technologies (widgets) integrated into our website. By using such tools, data is transmitted to the relevant provider, where it is processed and stored.

Many of these integrated programs work on a similar principle. After you have ordered one of our products or used one of our services, you will be asked to submit a review via email or on the website. You will usually be redirected to a review page via a link, where you can quickly and easily create a review. Some review systems also offer an interface to various social media channels in order to make the feedback accessible to more people.

Why do we use review platforms?

Review platforms collect feedback and ratings about our offer. Your ratings help us to quickly receive appropriate feedback. We can use this valuable input to improve our products and/or services much more efficiently. Therefore, on the one hand, ratings help us to optimise our offers. On the other hand, they give you and all our future customers a good overview of the quality of our products and services.

Which data is processed?

If we have your consent, we transmit information about you and the services you have used to the relevant review platform. We do this to ensure that you have genuinely used one of our services. Only then can you give real feedback. The transmitted data is only used to identify the user. The exact data that is stored and processed of course depends on the providers used. Personal data such as IP address, email address or your name are usually also made available to the rating platforms. Specific order information such as the order number of a purchased item will also be forwarded to the appropriate platform after you have submitted your review. If your email address is transmitted, this is done in a form that allows the review platform to send you an email after purchasing a product. In order to integrate your review to our website as well, we also inform the providers that you have accessed our site. The respective review platform that is used is responsible for any personal data collected.

How long and where is the data stored?

You can find out more about the duration of data processing in the relevant Privacy Policy of the provider below, provided we have further information on this. Generally, we only process personal data for as long as is absolutely necessary for the provision of our services and products. Personal data that is mentioned in a review is usually anonymised by the respective platform's employees and is therefore only visible to company administrators. The collected data is stored on the providers' servers, while most providers erase it after the end of the order.

Right to object

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

Legal Basis

If you have agreed that an evaluation platform may be used, the legal basis for the corresponding data processing is this consent. According to Article 6 Paragraph 1 lit. a of the GDPR (consent) represents the legal basis for the processing of personal data, as may occur when it is collected by a review portal.

We also have a legitimate interest in using a review platform to optimise our online service. The corresponding legal basis for this is Article 6 (1) (f) GDPR (legitimate interests). However, we only use any given review platform if you have consented to it.

We hope we could give you the most important general information about data processing at review platforms. You can find further information in the Privacy Policy texts below or in the linked Privacy Policies of the respective companies.

Google Reviews Privacy Policy

We also use the rating platform Google Reviews for our website. The provider of this service is the American company Google Inc. The responsible entity for all Google services in the European area is Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland).

Google processes data from you, among other things, in the USA. 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. More information can be found at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Additionally, Google uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Google commits to maintaining the European data protection level 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://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

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

You can find out more about the data that is processed by Google in their Privacy Policy at <https://policies.google.com/?hl=en>.

Font Awesome Privacy Policy


Font Awesome Privacy Policy Overview


 Affected parties: website visitors

 Purpose: service optimisation

 Processed data: data such as the IP address and loaded icon files

You can find more details on this in the privacy policy below.

 Storage period: data is stored for a few weeks in unidentifiable form

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

What is Font Awesome?

On our website we use Font Awesome by the American company Fonticons (307 S. Main St., Suite 202, Bentonville, AR 72712, USA). Upon your visit to one of our websites, the Font Awesome web font, i.e. the icons, are loaded via the Font Awesome Content Delivery Network (CDN). This way texts, fonts and icons are displayed appropriately on every device. In this privacy policy we will go into more detail on data storage and data processing by this service.

Icons play an increasingly important role on websites. Font Awesome is a web font specifically designed for web designers and web developers. With Font Awesome icons can for example be scaled and coloured as desired using the CSS stylesheet language. Thus, they now replace old picture icons. Font Awesome CDN is the easiest way to load icons or fonts onto your website. To do this, we only had to embed a short line of code into our website.

Why do we use Font Awesome on our website?

Font Awesome enables our websites' content to be depicted better. This eases your navigation on our website, and helps you grasp its content better. The icons can sometimes even be used to replace whole words and save space. This is particularly useful when optimising content specifically for smartphones. The icons are inserted as HTML code instead of as an image, which allows us to edit the icons with CSS exactly as we want. Simultaneously, Font Awesome also lets us improve our loading speed, as it only contains HTML elements and no icon images. All these advantages help us to make our website even clearer, faster and more refined for you.

Which data are stored by Font Awesome?

The Font Awesome Content Delivery Network (CDN) is used to load icons and symbols. CDNs are server networks that are distributed around the world. They make it possible to quickly load files from locations in close proximity. When you open one of our pages, the respective icons will be provided by Font Awesome.

For the web fonts to be loaded, your browser has to connect to the servers of Fonticons, Inc. For this, your IP address will be identified. Font Awesome also collects data on which icon files are downloaded, as well as when they are downloaded. Furthermore, technical data such as your browser version, screen resolution or the time when you accessed the page are also transmitted.

These data are collected and stored for the following reasons:

- to optimise Content Delivery Networks
- to identify and fix technical errors
- to protect CDNs from misuse and attacks
- to calculate fees from Font Awesome Pro customers
- to identify the popularity of icons
- to establish which computer and software you are using

If your browser does not allow web fonts, one of your PC's standard fonts will be used automatically. Moreover, as far as we are currently aware, no cookies will be set. We are keeping in contact with Font Awesome's privacy department and will let you know as soon as we find out more.

How long and where are the data stored?

Font Awesome stores data about the use of the Content Delivery Network also on servers in the United States of America. However, the CDN servers are located all across the world and store user data in your proximity. The data is usually only stored for a few weeks in an identifiable form. Aggregated statistics on the use of the CDNs may also be stored for longer. However, these do not include any personal data.

How can I erase my data or prevent data retention?

As far as we are aware, Font Awesome does not store any personal data via Content Delivery Networks. If you do not want data about the used icons to be stored, you will unfortunately not be able to visit our website. If your browser does not allow web fonts, no data will be transmitted or saved. In this case your computer's default font will be used.

Legal basis

If you have agreed to the use of Font Awesome, your consent is the legal basis for the corresponding data processing. According to **Art. 6 Paragraph 1 lit. a GDPR (consent)** this consent represents the legal basis for personal data processing, as can occur when it is collected by Font Awesome.

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

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

Font Awesome uses standard contractual clauses approved by the EU Commission as basis for data processing by recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway and especially in the USA) or data transfer there (= Art. 46, paragraphs 2 and 3 of the GDPR). These clauses oblige Font Awesome to comply with the EU's level of data protection


when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses here:


https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847


If you want to find out more about Font Awesome and their data handling, we recommend you to read their Privacy Policy at <https://fontawesome.com/privacy> along with the help page at <https://fontawesome.com/help>.

Google Fonts Privacy Policy


Google Fonts Privacy Policy Overview


 Affected parties: website visitors

 Purpose: service optimisation

 Processed data: data such as IP address, CSS and font requests

You can find more details on this in the Privacy Policy below.

 Storage period: Google stores font files for one year

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

What are Google Fonts?

On our website we use Google Fonts, by the company Google Inc. (1600 Amphitheatre Parkway Mountain View, CA 94043, USA).

To use Google Fonts, you must log in and set up a password. Furthermore, no cookies will be saved in your browser. The data (CSS, Fonts) will be requested via the Google domains fonts.googleapis.com and fonts.gstatic.com. According to Google, all requests for CSS and fonts are fully separated from any other Google services. If you have a Google account, you do not need to worry that your Google account details are transmitted to Google while you use Google Fonts. Google records the use of CSS (Cascading Style Sheets) as well as the utilised fonts and stores these data securely. We will have a detailed look at how exactly the data storage works.

Google Fonts (previously Google Web Fonts) is a directory with over 800 fonts that [Google](https://www.google.com) provides its users free of charge.

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

Why do we use Google Fonts on our website?

With Google Fonts we can use different fonts on our website and do not have to upload them to our own server. Google Fonts is an important element which helps to keep the quality of our website high. All Google fonts are automatically optimised for the web, which saves data volume and is an advantage especially for the use of mobile terminal devices. When you use our website, the low data size provides fast loading times. Moreover, Google Fonts are secure Web Fonts. Various image synthesis systems (rendering) can lead to errors in different browsers, operating

systems and mobile terminal devices. These errors could optically distort parts of texts or entire websites. Due to the fast Content Delivery Network (CDN) there are no cross-platform issues with Google Fonts. All common browsers (Google Chrome, Mozilla Firefox, Apple Safari, Opera) are supported by Google Fonts, and it reliably operates on most modern mobile operating systems, including Android 2.2+ and iOS 4.2+ (iPhone, iPad, iPod). We also use Google Fonts for presenting our entire online service as pleasantly and as uniformly as possible.

Which data is stored by Google?

Whenever you visit our website, the fonts are reloaded by a Google server. Through this external cue, data gets transferred to Google's servers. Therefore, this makes Google recognise that you (or your IP-address) is visiting our website. The Google Fonts API was developed to reduce the usage, storage and gathering of end user data to the minimum needed for the proper depiction of fonts. What is more, API stands for „Application Programming Interface“ and works as a software data intermediary.

Google Fonts stores CSS and font requests safely with Google, and therefore it is protected. Using its collected usage figures, Google can determine how popular the individual fonts are. Google publishes the results on internal analysis pages, such as Google Analytics. Moreover, Google also utilises data of its own web crawler, in order to determine which websites are using Google fonts. This data is published in Google Fonts' BigQuery database. Entrepreneurs and developers use Google's webservice BigQuery to be able to inspect and move big volumes of data.

One more thing that should be considered, is that every request for Google Fonts automatically transmits information such as language preferences, IP address, browser version, as well as the browser's screen resolution and name to Google's servers. It cannot be clearly identified if this data is saved, as Google has not directly declared it.

How long and where is the data stored?

Google saves requests for CSS assets for one day in a tag on their servers, which are primarily located outside of the EU. This makes it possible for us to use the fonts by means of a Google stylesheet. With the help of a stylesheet, e.g. designs or fonts of a website can get changed swiftly and easily.

Any font related data is stored with Google for one year. This is because Google's aim is to fundamentally boost websites' loading times. With millions of websites referring to the same fonts, they are buffered after the first visit and instantly reappear on any other websites that are visited thereafter. Sometimes Google updates font files to either reduce the data sizes, increase the language coverage or to improve the design.

How can I erase my data or prevent it being stored?

The data Google stores for either a day or a year cannot be deleted easily. Upon opening the page this data is automatically transmitted to Google. In order to clear the data ahead of time, you have to contact Google's support at <https://support.google.com/?hl=en-GB&tid=121887810>. The only way for you to prevent the retention of your data is by not visiting our website.

Unlike other web fonts, Google offers us unrestricted access to all its fonts. Thus, we have a vast sea of font types at our disposal, which helps us to get the most out of our website. You can find out more answers and information on Google Fonts at <https://developers.google.com/fonts/faq?tid=121887810>. While Google does address relevant elements on data protection at this link, it does not contain any detailed information on data retention.

It proves rather difficult to receive any precise information on stored data by Google.

Legal basis

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

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

Google processes data from you, among other things, in the USA. 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. More information can be found at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Additionally, Google uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Google commits to maintaining the European data protection level 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://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

You can find the Google Ads Data Processing Terms, which refer to the Standard Contractual Clauses, at: <https://business.safety.google/intl/en/adsprocessor/terms/>

You can find more information on which data is generally retained by Google and what this data is used at <https://policies.google.com/privacy?hl=en-GB>.

Google Fonts Local Privacy Policy


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


What are Google Fonts?


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


Online Map Services Introduction

Online Map Services Privacy Policy Overview

 Affected parties: website visitors

 Purpose: Improvement of user experience

 Processed data: the data that is processed depends heavily on the services used. Usually, it is your IP address, location data, search queries and/or technical data. You can find more details on this under the respective tools used.

 Storage duration: depends on the tools used

 Legal bases: Article 6 paragraph 1 lit. a GDPR (consent), Article 6 paragraph 1 lit. f GDPR (legitimate interests)

What are Online Map Services?

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

Why do we use Online Map Services on our website?

Generally speaking, it is imperative for us to offer you a pleasant time on our website. Of course, we know that you will most likely only enjoy your time here if you can easily find your way around and find all the information you need quickly and easily. Therefore, we decided that an online map system may be a significant optimisation of our website's service. After all, you can use the map system to easily view route descriptions, locations or any other points of interest – without leaving our site. Needless to say, it is certainly also very practical that you can easily see where our company headquarters are so that you can find us quickly and safely. As you can see, there are just a lot of advantages – and we clearly consider online map services on our website to be part of our customer service.

What data is stored by Online Map Services?

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

How long and where is the data stored?

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

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

Right to object

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

Legal Basis

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






We also have a legitimate interest in using an online map service to optimise our service on our

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

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

Google Maps Privacy Policy

Google Maps Privacy Policy Overview

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

What is Google Maps?

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

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

Why do we use Google Maps on our website?

The efforts we make on this page have the goal of giving you a useful and meaningful experience on our website. Through the integration of Google Maps, we can offer you essential information on various locations. Therefore, you can spot our office address with one glance. Furthermore, the route directions always show you the best and fastest way to us. You can retrieve the route directions for traveling either by car, by public transport, on foot or by bike. The integration of Google Maps is a part of our customer service.

What data is stored by Google Maps?

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

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

Name: NID

Value: 188=h26c1Ktha7fCQTx8rXgLyATyITJ121887810-5

Purpose: Google uses NID in order to adjust advertisements to your Google searches. With the cookie's help Google "remembers" your most frequently entered search queries or your previous interaction with ads. That way you always receive customised advertisements. The cookie contains a unique ID, which Google uses to collect your personal settings for advertising purposes.

Expiration date: after 6 months

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

How long and where is the data stored?

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

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

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

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

Due to the automatic delete function for location and activity data, which was introduced in 2019, information that is used for determining your location and web or app activity is saved for either 3 or 18 months, depending on your preferred decision, and is deleted thereafter. Furthermore, it is possible to delete this data manually from your browser history via your Google account anytime. If

you want to prevent the determination of your location altogether, you must pause the category “Web and app activity” in your Google account. Click on “Data and personalisation” and then choose the option “Activity controls”. Here you can switch the activities on or off.

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

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

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

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

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

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

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

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

Legal basis

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

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

Google processes data from you, among other things, in the USA. 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. More information can be found at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Additionally, Google uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Google commits to maintaining the European

data protection level 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://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

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

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

Explanation of the terminology used

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

Processor

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Consent

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“consent” of the data subject means any freely given, specific, informed and unambiguous

indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

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

Data concerning health

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

***"Data concerning health"** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;*

Explanation: Health data includes all stored information relating to your own health. It is often data that is also noted in patient files. This includes, for example, which medication you are using, X-rays, your entire medical history or your vaccination statuses.

Personal Data

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

- name
- address
- email address
- postal address

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

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

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

Profiling

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Controller

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Processing

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Personal data breach

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data

transmitted, stored or otherwise processed;

Explanation: For example, a personal data breach can occur in the event of a data leak, i.e. a technical problem or a cyber attack. If the breach results in a risk to the rights and freedoms of individuals, the data controller must immediately report the incident to the supervisory authority, and the data subjects must be informed if the violation poses a high risk to the rights and freedoms of natural persons.

Closing Remarks

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

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

If you have any questions about data protection on our website, please do not hesitate to contact us or the responsible body. We wish you all the best and hope to soon welcome you to our website again.

All texts are copyrighted.

Source: Created with the [Datenschutz Generator](#) by AdSimple