

Privacy Policy

Privacy Policy Introduction and Overview

We have written this privacy policy (version 22.10.2023-312427560) 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:

Mosaik Interim GmbH
Schloßstraße 15
74249 Jagsthausen
Tel.: +49 7943 54 39 995

E-Mail: a.muench@mosaik-recruiting.de
Impressum: www.mosaik-recruiting.de/impressum

Storage Period

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

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

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

Rights in accordance with the General Data Protection Regulation

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

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

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

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

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

Baden-Württemberg Data protection authority

State Commissioner for Data Protection: Prof. Dr. Tobias Keber

Address: Königstraße 10a, 70173 Stuttgart

Phone number: 07 11/61 55 41-0

E-mail address: poststelle@lfdi.bwl.de

Website: <https://www.baden-wuerttemberg.datenschutz.de/>

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 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: GA1.2.1326744211.152312427560-9

Purpose: Differentiation between website visitors

Expiry date: after 2 years

A browser should support these minimum sizes:

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

Which types of cookies are there?

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

There are 4 different types of cookies:

Essential cookies

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

Purposive cookies

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

Target-orientated cookies

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

Advertising cookies

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

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

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

Purpose of processing via cookies

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

Which data are processed?

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

Storage period of cookies

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

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

Right of objection – how can I erase cookies?

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

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

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

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

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

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

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

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

Legal basis

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


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


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


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


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.


Registration


Registration Overview

 Affected parties: Anyone who registers to create an account with us, and logs in to use the account.

 Processed data: Personal data such as email address, name, password and other data that is collected during registration, login and account use.

 Purpose: For the provision of our services, as well as to communicate with clients or customers in the scope of our services.

 Storage period: As long as the company account associated with the texts exists, plus a period of usually 3 years.

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

If you register with us and provide any personal data, this data may be processed, possibly along with your IP address. Below you can explore what we mean by the rather broad term “personal data”.

Please only enter the data we need for the registration. In case you are registering on behalf of a third party, please only enter data for which you have the approval of the party you are registering for. If possible, use a secure password that you don't use anywhere else and an email address that you check regularly.

In the following, we will inform you about the exact type of data processing we do. After all, we want you to feel at ease with the services we provide!

What is a registration?

When you register, we retain certain of your data in order to make it easy for you to log in with us online and use your account. An account with us has the advantage that you don't have to re-enter everything every time. It saves time and effort and ultimately prevents any issues with the provision of our services.

Why do we process personal data?

In short, we process personal data to make account registration and usage possible for you. If we didn't do this, you would have to enter all your data each time, wait for our approval and then enter everything again. This strenuous process would probably not only irritate us a little, but also many of our dear clients and customers.

Which data is processed?

Any data that you provided during registration or login and any data that you may enter as part of managing your account data.

During registration, we process the following types of data:

- First name
- Last name
- Email address
- Company name
- Street + house number
- Residence
- Postcode
- Country

During your registration, we process any data you enter, such as your username and password, along with data that is collected in the background such as your device information and IP addresses.

When using your account, we process any data you enter while using the account, as well as any data that is created while you use our services.

Storage time

We store the entered data for at least as long as the account associated with the data exists with us and is in use – and as long as there are contractual obligations between you and us. In case the contract ends, we retain the data until the respective claims get time-barred. Moreover, we store your data as long as we are subject to legal storage obligations, if applicable. Following that, we keep any accounting records (invoices, contract documents, account statements, etc.) of the contract for 10 years (§ 147 AO) and other relevant business documents for 6 years (§ 247 HGB) after accrual.

Right to object

You have registered, entered data and want to revoke the data processing? Not a problem. As you can see above, you retain this right under the General Data Protection Regulation also at and after registration, login or account creation with us. Contact the Data Protection Officer above to exercise your rights. If you already have an account with us, you can easily view and manage your data and texts in your account.

Legal Basis

By completing the registration process, you enter into a pre-contractual agreement with us, with the intention to conclude a contract of use for our platform (although there is no automatic payment obligation). You invest time to enter data and register and in return, we offer you our services after you log on to our system and view your customer account. We also meet our contractual obligations. Finally, we need to be able to email registered users about important changes. Article 6(1)(b) GDPR (implementation of pre-contractual measures, fulfilment of a contract) applies.

Where applicable, we will ask for your consent, e.g. in case you voluntarily provide more data than is absolutely necessary, or in case we may ask you if we may send you advertising. Article 6 paragraph 1 lit. a GDPR (consent) applies in this matter.

We also have a legitimate interest in knowing who our clients or customers are, in order to get in touch if required. We also need to know who is using our services and whether they are being used in accordance with our terms of use, i.e. Article 6(1)(f) GDPR (legitimate interests) applies in this matter.

Note: the following sections are to be ticked by users (as required):

Registration with real names

Since business operations require us to know who our clients or customers are, registration is only possible with your real name (full name) and not with a pseudonym.

Registration with pseudonyms

You can use a pseudonym for the registration, which means you don't have to register with your real name. This ensures that your real name cannot be processed by us.

Storage of the IP address

During registration, login and account use, we store your IP address for security reasons in order to be able to determine legitimate use.

Public Profile

User profiles are publicly visible, i.e. parts of the profiles can also be viewed on the Internet without the need to enter a username and password.

Two Factor Authentication (2FA)


Two Factor Authentication (2FA) offers additional security when logging in, as it prevents you from logging in without a smartphone, for example. This technical measure to secure your account protects you against the loss of data or unauthorised access, even if your username and password were leaked. During your registration process, login or within the account itself you can find out which 2FA is used.

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=312427560>)
- 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.

hosteurope Privacy Policy

We use hosteurope for our website, including a web hosting provider. The provider of this service is the German company Host Europe GmbH, Hansestrasse 111, 51149 Köln, Germany. You can find out more about the data that are processed through the

use of hosteurope in their Privacy Policy at <https://www.hosteurope.de/AGB/Datenschutzerklaerung/>.

Data Processing Agreement (DPA) HostEurope

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have entered into a Data Processing Agreement (DPA) with HostEurope. What exactly a DPA is and especially what must be included in a DPA, you can read in our general section “Data Processing Agreement (DPA)”.


This contract is required by law because HostEurope processes personal data on our behalf. It clarifies that HostEurope may only process data they receive from us according to our instructions and must comply with the GDPR. You can find the link to the Data Processing Agreement (DPA) under <https://www.hosteurope.de/Dokumente/>.

Website Builders Introduction


Website Builders Privacy Policy Overview

 Affected parties: website visitors

 Purpose: service optimisation

 Data processed: The data that is being processed includes but is not limited to technical usage information, browser activity, clickstream activity, session heat maps, contact details, IP addresses or geographic locations. You can find more details in the Privacy Policy below as well as in the providers’ Privacy Policies.

 Storage duration: depends on the provider

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

What are website builders?

We use a modular website builder for our website. This is a special form of Content Management System (CMS). Website builders enable website operators to create websites very easily and without any programming knowledge. In many cases, web hosts also offer website builders. Your personal data may be collected, stored and processed if a website builder is being used. In this Privacy Policy, you will find general information about data that is processed by such modular website builder systems. You can find more information in the respective provider’s Privacy Policy.

Why do we use website builders for our website?

The greatest advantage of modular website builders is their ease of use. We want to offer you a clear, simple and nicely designed website that we can easily operate and maintain by ourselves – without needing any external support. Nowadays website builders offer many helpful functions that we can use even without having any

programming knowledge. This enables us to design our website according to our wishes and therefore, to give you an informative and pleasant experience on our website.

Which data are stored by website builders?

First of all, the exact data that is stored depends on the website builder that is being used. Each provider processes and collects different data from website visitors. However, technical usage information such as users' operating system, browser, screen resolution, language and keyboard settings, hosting provider as well as the date of the website visit are usually collected. Moreover, tracking data (e. g. browser activity, clickstream activities, session heat maps, etc.) may also be processed. The same goes for personal data, since data such as contact information e. g. email address, telephone number (if you have provided it), IP address and geographic location data may also be processed and stored. In the respective provider's Privacy Policy you can find out exactly which of your data is getting stored.

How long and where are the data stored?

Provided that we have any further information on this, we will inform you below about the duration of the data processing associated with the website builder we use. You can find detailed information on this in the provider's Privacy Policy. Generally, we only process personal data for as long as is absolutely necessary to provide our services and products. The provider may store your data according to their own specifications, over which we have no influence.

Right to object

You always retain the right to information, rectification and erasure of your personal data. If you have any questions, you can also contact the responsible parties at the respective website builder system at any time. You can find the corresponding contact details either in our Privacy Policy or on the website of the respective provider.

What is more, in your browser you can clear, disable or manage cookies that providers use for their functions. Depending on the browser you use, this can be done in different ways. Please note, that this may lead to not all functions working as usual anymore.

Legal Bases

We have a legitimate interest in using a website builder system to optimise our online service and present it in an efficient and user-friendly way. The corresponding legal basis for this is Article 6 (1) (f) GDPR (legitimate interests). However, we only use the website builder system if you have consented to it.

If the processing of data is not absolutely necessary for the operation of the website, your data will only be processed on the basis of your consent. This particularly applies to tracking activities. The legal basis for this is Article 6 (1) (a) GDPR.

With this Privacy Policy, we have made you more familiar with the most important general information on data processing. If you want to find out more about this, you will find further information – if available – in the following section or in the Privacy Policy of the provider.

Elementor Privacy Policy

We use the website builder system Elementor for our website. The service provider is the Israeli company Elementor Ltd., located at Rehov Tuval 40, 5252247 Ramat Gan, Israel.

Your data may be transferred to Israel. Israel is outside the scope of the General Data Protection Regulation (GDPR). However, the European Commission has decided, based on Article 45(1) of the GDPR, that Israel provides a level of protection comparable to the GDPR standards. You can view the decision here: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011D0061>

To learn more about the data processed through the use of Elementor, please refer to the privacy policy at <https://elementor.com/about/privacy/>.

WordPress.com Privacy Policy

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

What is WordPress?

The company was founded in 2003 and quickly developed into one of the most famous content management systems (CMS) worldwide. A CMS is a software that helps us design our website and display content beautifully and in an organized manner. The content can include text, audio, and video.

By using WordPress, personal data about you may also be collected, stored, and processed. Typically, mainly technical data such as operating system, browser, screen resolution, or hosting provider are stored. However, personal data such as IP address, geographic data, or contact information may also be processed.

Why do we use WordPress?

Programming is not one of our core competencies. Nevertheless, we want to have a powerful and attractive website that we can manage and maintain ourselves. With a website builder system or a content management system like WordPress, this is possible. With WordPress, we don't need to be programming experts to offer you a beautiful website. Thanks to WordPress, we can quickly and easily operate our website even without technical knowledge. If technical problems arise or we have special requests for our website, we still have our experts who are familiar with HTML, PHP, CSS, and the like.

How secure is the data transfer with WordPress?

WordPress processes data from you, among other things, in the USA. WordPress 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, WordPress 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, WordPress 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 conditions (Data Processing Agreements), which correspond to the standard contractual clauses, can be found at <https://wordpress.com/support/data-processing-agreements/>.

You can learn more about the data processed through the use of WordPress.com in the privacy policy at <https://automattic.com/de/privacy/>.


Data Processing Agreement (DPA) WordPress.com

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have entered into a Data Processing Agreement (DPA) with WordPress.com. What exactly a DPA is and especially what must be included in a DPA, you can read in our general section “Data Processing Agreement (DPA)”.

This contract is required by law because WordPress.com processes personal data on our behalf. It clarifies that WordPress.com may only process data they receive from us according to our instructions and must comply with the GDPR. You can find the link to the Data Processing Agreement (DPA) under <https://wordpress.com/support/data-processing-agreements/>.

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.

Facebook Conversions API Privacy Policy

On our website we use Facebook Conversions API, which is an event tracking tool. The provider of this service is the American company Facebook Inc. The company also has Irish headquarters at 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland.

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>.

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

Facebook Pixel Privacy Policy

We use Facebook's Facebook pixel on our website. For that, we have implemented a code on our website. The Facebook pixel is a segment of a JavaScript code, which, in case you came to our website via Facebook ads, loads an array or functions that enable Facebook to track your user actions. For example, if you buy a product on our website, the Facebook pixel is triggered and stores your actions on our website in one or more cookies. These cookies enable Facebook to match your user data (customer data such as IP address, user ID) with the data of your Facebook account. After that, Facebook deletes your data again. The collected data is anonymous as well as inaccessible and can only be used for ad placement purposes. If you are a Facebook user and you are logged in, your visit to our website is automatically assigned to your Facebook user account.

We exclusively want to show our products or services to persons, who are interested in them. With the aid of the Facebook pixel, our advertising measures can get better adjusted to your wishes and interests. Therefore, Facebook users get to see suitable advertisement (if they allowed personalised advertisement). Moreover, Facebook uses the collected data for analytical purposes and for its own advertisements.

In the following we will show you the cookies, which were set on a test page with the Facebook pixel integrated to it. Please consider that these cookies are only examples. Depending on the interaction that is made on our website, different cookies are set.

Name: _fbp

Value: fb.1.1568287647279.257405483-6312427560-7

Purpose: Facebook uses this cookie to display advertising products.

Expiration date: after 3 months

Name: fr

Value: 0aPf312HOS5Pboo2r..Bdeiuf...1.0.Bdeiuf.

Purpose: This cookie is used for Facebook pixels to function properly.

Expiration date: after 3 months

Name: comment_author_50ae8267e2bdf1253ec1a5769f48e062312427560-3

Value: Name of the author

Purpose: This cookie saves the text and name of a user who e.g. leaves a comment.

Expiration date: after 12 months

Name: comment_author_url_50ae8267e2bdf1253ec1a5769f48e062

Value: https%3A%2F%2Fwww.testseite...%2F (URL of the author)

Purpose: This cookie saved the URL of the website that the user types into a text box on our website.

Expiration date: after 12 months

Name: comment_author_email_50ae8267e2bdf1253ec1a5769f48e062

Value: email address of the author

Purpose: This cookie saves the email address of the user, if they provided it on the website.

Expiration date: after 12 months

Note: The above-mentioned cookies relate to an individual user behaviour. Moreover, especially concerning the usage of cookies, changes at Facebook can never be ruled out.

If you are registered on Facebook, you can change the 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 manage your user based online advertising at

<https://www.youronlinechoices.com/uk/your-ad-choices>. You have the option to

activate or deactivate any providers there.

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>.

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

Privacy Policy for Facebook's Automatic Advanced Matching


Along with Facebook's pixel function, we have also activated Automatic Advanced Matching. This function allows us to send hashed emails, names, genders, cities, states, postcodes and dates of birth or telephone numbers as additional information to Facebook, provided you have made them available to us. This activation gives us the opportunity to customise advertising campaigns even better to persons who are interested in our services or products.


Google Analytics Privacy Policy

Google Analytics Privacy Policy Overview

 Affected parties: website visitors

 Purpose: Evaluation of visitor information to optimise the website.

 Processed data: Access statistics that contain data such as the location of access, device data, access duration and time, navigation behaviour and click behaviour. You can find more details on this in the privacy policy below.

 Storage period: Customizable, GA4 stores data for 14 months by default.

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

What is Google Analytics?

On our website, we use the analytics tracking tool Google Analytics in the Google Analytics 4 (GA4) version provided by the American company Google Inc. For the European region, Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services. Google Analytics collects data about your actions on our website. By combining various technologies such as cookies, device IDs, and login information, you can be identified as a user across different devices. This allows your actions to be analyzed across platforms as well.

For example, when you click on a link, this event is stored in a cookie and sent to Google Analytics. With the reports we receive from Google Analytics, we can better tailor our website and service to your needs. In the following, we will provide more information

about the tracking tool and specifically inform you about the data processed and how you can prevent it.

Google Analytics is a tracking tool used for website traffic analysis. The basis for these measurements and analyses is a pseudonymous user identification number. This number does not include personally identifiable information such as name or address but is used to assign events to a device. GA4 utilizes an event-based model that captures detailed information about user interactions such as page views, clicks, scrolling, and conversion events. Additionally, GA4 incorporates various machine learning features to better understand user behavior and certain trends. GA4 employs modeling through machine learning capabilities, meaning that based on the collected data, missing data can be extrapolated to optimize the analysis and provide forecasts.

In order for Google Analytics to function properly, a tracking code is embedded in the code of our website. When you visit our website, this code records various events that you perform on our website. With GA4's event-based data model, we, as website operators, can define and track specific events to obtain analyses of user interactions. This allows us to track not only general information such as clicks or page views but also specific events that are important for our business, such as submitting a contact form or making a purchase.

Once you leave our website, this data is sent to and stored on Google Analytics servers.

Google processes the data, and we receive reports on your user behavior. These reports can include, among others, the following:

- Audience reports: Audience reports help us get to know our users better and gain a more precise understanding of who is interested in our service.
- Advertising reports: Advertising reports make it easier for us to analyze and improve our online advertising.
- Acquisition reports: Acquisition reports provide helpful information on how we can attract more people to our service.
- Behavior reports: Here, we learn about how you interact with our website. We can track the path you take on our site and which links you click on.
- Conversion reports: Conversion refers to an action you take as a result of a marketing message, such as going from being a website visitor to becoming a buyer or newsletter subscriber. Through these reports, we gain insights into how our marketing efforts resonate with you, with the aim of improving our conversion rate.
- Real-time reports: With real-time reports, we can see what is currently happening on our website. For example, we can see how many users are currently reading this text.

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

- Event-based data model: This model captures specific events that can occur on our website, such as playing a video, making a purchase, or subscribing to our newsletter.

- **Advanced analytics features:** With these features, we can gain a better understanding of your behavior on our website or certain general trends. For example, we can segment user groups, conduct comparative analyses of target audiences, or track your path on our website.
- **Predictive modeling:** Based on the collected data, missing data can be extrapolated through machine learning to predict future events and trends. This can help us develop better marketing strategies.
- **Cross-platform analysis:** Data collection and analysis are possible from both websites and apps. This enables us to analyze user behavior across platforms, provided you have consented to data processing.

Why do we use Google Analytics on our website?

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

The statistically evaluated data gives us a clear picture of the strengths and weaknesses of our website. On one hand, we can optimize our site to make it more easily found by interested people on Google. On the other hand, the data helps us better understand you as a visitor. We know exactly what we need to improve on our website in order to provide you with the best possible service. The data also helps us conduct our advertising and marketing activities in a more personalized and cost-effective manner. After all, it only makes sense to show our products and services to people who are interested in them.

What data is stored by Google Analytics?

With the help of a tracking code, Google Analytics creates a random, unique ID associated with your browser cookie. This way, Google Analytics recognizes you as a new user, and a user ID is assigned to you. When you visit our site again, you are recognized as a “returning” user. All collected data is stored together with this user ID, making it possible to evaluate pseudonymous user profiles.

To analyze our website with Google Analytics, a property ID must be inserted into the tracking code. The data is then stored in the corresponding property. For each newly created property, the default is Google Analytics 4 Property. The data storage duration varies depending on the property used.

Through identifiers such as cookies, app instance IDs, user IDs, or custom event parameters, your interactions, if you have consented, are measured across platforms. Interactions encompass all types of actions you perform on our website. If you also use other Google systems (such as a Google account), data generated through Google Analytics can be linked to third-party cookies. Google does not disclose Google Analytics data unless we, as website operators, authorize it, except when required by law.

According to Google, IP addresses are not logged or stored in Google Analytics 4. However, IP address data is used by Google for deriving location data and is

immediately deleted thereafter. All IP addresses collected from users in the EU are deleted before the data is stored in a data center or on a server.

Since GA4 focuses on event-based data, the tool uses significantly fewer cookies compared to previous versions such as Google Universal Analytics. However, there are still some specific cookies used by GA4. These can include:

Name: _ga

Value: 2.1326744211.152312427560-5

Purpose: By default, analytics.js uses the _ga cookie to store the user ID. It is used to distinguish website visitors.

Expiration: After 2 years

Name: _gid

Value: 2.1687193234.152312427560-1

Purpose: This cookie is also used to distinguish website visitors.

Expiration: After 24 hours

Name: gat_gtag_UA Value: 1

Purpose: Used to reduce the request rate. If Google Analytics is deployed via Google Tag Manager, this cookie will be named dc_gtm .

Expiration: After 1 minute

Note: This list cannot claim to be exhaustive, as Google may change their choice of cookies from time to time. GA4 aims to improve data privacy and offers several options for controlling data collection. For example, we can determine the storage duration ourselves and control data.

Here we provide an overview of the main types of data collected by Google Analytics:

Heatmaps: Google creates heatmaps to show the exact areas you click on. This provides us with information about your interactions on our site.

Session Duration: Google refers to session duration as the time you spend on our site without leaving. If you are inactive for 20 minutes, the session automatically ends.

Bounce Rate: Bounce rate refers to when you view only one page on our website and then leave.

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

Location: IP addresses are not logged or stored in Google Analytics. However, location data is derived shortly before the IP address is deleted.

Technical Information: Technical information includes your browser type, internet service provider, and screen resolution, among others.

Source of Origin: Google Analytics is interested in the website or advertisement that brought you to our site.

Additional data may include contact information, reviews, media playback (e.g., if you play a video on our site), sharing of content via social media, or adding to favorites. This list is not exhaustive and serves only as a general guide to the data storage by Google Analytics.

Where and how long are the data stored?

Google has servers distributed worldwide. You can find precise information about the locations of Google data centers at:

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

Your data is distributed across multiple physical storage devices. This ensures faster access to data and better protection against manipulation. Each Google data center has emergency programs in place for your data. In the event of hardware failure or natural disasters, the risk of service interruption at Google remains low.

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

- 2 months: This is the shortest storage period.
- 14 months: By default, data is stored in GA4 for 14 months.
- 26 months: Data can also be stored for 26 months.
- Data is only deleted manually.

In addition, there is also the option for data to be deleted only if you do not visit our website within the selected time period. In this case, the retention period is reset every time you revisit our website within the defined time frame.

Once the defined period has expired, the data is deleted once a month. This retention period applies to data linked to cookies, user identification, and advertising IDs (e.g., cookies from the DoubleClick domain). Report results are based on aggregated data and are stored independently of user data. Aggregated data is a combination of individual data into larger units.

How can I delete my data or prevent data storage?

Under the data protection laws of the European Union, you have the right to access, update, delete, or restrict your data. By using the browser add-on to deactivate Google Analytics JavaScript (analytics.js, gtag.js), you can prevent Google Analytics 4 from using your data. You can download and install the browser add-on at:

<https://tools.google.com/dlpage/gaoptout?hl=en> Please note that this add-on only disables data collection by Google Analytics.

If you want to disable, delete, or manage cookies in general, you can find the respective instructions for the most common browsers in the “Cookies” section.

Legal basis

The use of Google Analytics requires your consent, which we obtained through our cookie popup. According to **Art. 6(1)(a) of the GDPR**, 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 also have a legitimate interest in analyzing the behavior of website visitors to improve our offering technically and economically. By using Google Analytics, we can identify website errors, detect attacks, and improve efficiency. The legal basis for this is **Art. 6(1)(f) of the GDPR** (legitimate interests). However, we only use Google Analytics if you have given your consent.

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/>

We hope we have provided you with the most important information regarding the data processing by Google Analytics. If you want to learn more about the tracking service, we recommend the following links:

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

If you want to learn more about data processing, you can refer to the Google Privacy Policy at: <https://policies.google.com/privacy?hl=en>.

Data Processing Agreement (DPA) Google Analytics

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have entered into a Data Processing Agreement (DPA) with Google Analytics. What exactly a DPA is and especially what must be included in a DPA, you can read in our general section "Data Processing Agreement (DPA)".

This contract is required by law because Google Analytics processes personal data on our behalf. It clarifies that Google Analytics may only process data they receive from us according to our instructions and must comply with the GDPR. You can find the link to the Data Processing Terms under

<https://business.safety.google/intl/en/adsprocessor/terms/>.

Google Analytics Reports on demographic characteristics and interests

We have turned on Google Analytics' functions for advertising reports. These reports on demographic characteristics and interests contain details about age, gender and interests. Through them we can get a better picture of our users – without being able to allocate any data to individual persons. You can learn more about advertising functions at [auf](#)

https://support.google.com/analytics/answer/3450482?hl=en&utm_id=ad.

You can terminate the use of your Google Account's activities and information in "Ads Settings" at <https://adssettings.google.com/authenticated> via a checkbox.

Google Analytics e-commerce Measurement

We also use the e-commerce measurement function of the web analysis tool Google Analytics for our website. This allows us to analyse very precisely how you and all our other customers interact with our website. E-commerce measurement is all about purchasing behaviour. Based on the data obtained, we can adapt and optimise our service to your wishes and expectations. With this data we can also use our online advertising measures in a more targeted manner, to only show our advertising to people who are interested in our products or services. The e-commerce measurement function records e. g. which orders were placed, how much time you took to decide on purchasing a product, the average order value or the shipping costs. All this data can be recorded and stored under a specific ID.

Google Analytics Google Signals Privacy Policy

We have activated Google signals in Google Analytics. Through this, any existing Google Analytics functions (advertising reports, remarketing, cross-device reports and reports on interests and demographic characteristics) are updated, to result in the summary and anonymisation of your data, should you have permitted personalised ads in your Google Account.

The special aspect of this is that it involves cross-device tracking. That means your data can be analysed across multiple devices. Through the activation of Google signals, data is collected and linked to the Google account. For example, it enables Google to recognise when you look at a product on a smartphone and later buy the product on a laptop. Due to activating Google signals, we can start cross-device remarketing campaigns, which would otherwise not be possible to this extent. Remarketing means, that we can show you our products and services across other websites as well.

Moreover, further visitor data such as location, search history, YouTube history and data about your actions on our website are collected in Google Analytics. As a result, we receive improved advertising reports and more useful information on your interests and demographic characteristics. These include your age, the language you speak, where you live or what your gender is. Certain social criteria such as your job, your marital status or your income are also included. All these characteristics help Google Analytics to define groups of persons or target audiences.

Those reports also help us to better assess your behaviour, as well as your wishes and interests. As a result, we can optimise and customise our products and services for you. By default, this data expires after 26 months. Please consider, that this data is only collected if you have agreed to personalised advertisement in your Google Account. The retained information is always exclusively summarised and anonymous data, and never any data on individual persons. You can manage or delete this data in your Google Account.

Google Analytics in Consent Mode

Depending on your consent, Google Analytics will process your personal data in the so-called “consent mode”. You can choose whether or not you want to accept Google Analytics cookies, and thus which of your data Google Analytics may process. The retained data is mainly used to measure user behaviour on the website, to serve targeted advertising and to provide us with web analysis reports. Usually, you would consent to Google’s data processing via a cookie consent tool. If you do not consent to data processing, only aggregated data will be collected and processed. This means that data cannot be assigned to individual users and therefore no user profile will be created for you. You also have the option to only agree to statistical measurement, meaning that none of your personal data will be processed and used for advertising or advertising measurement sequences.

Google Analytics IP Anonymisation

We implemented Google Analytics’ IP address anonymisation to this website. Google developed this function, so this website can comply with the applicable privacy laws and the local data protection authorities’ recommendations, should they prohibit the retention of any full IP addresses.

The anonymisation or masking of IP addresses takes place, as soon as they reach Google Analytics’ data collection network, but before the data would be saved or processed.

You can find more information on IP anonymisation at <https://support.google.com/analytics/answer/2763052?hl=en>.

Google Analytics without Cookies

We use Google Analytics (GA for short) on our website, but without setting cookies in your browser. Above, we have already explained what cookies are. Whether you remember the explanations or not – here is very brief information specifically related

to GA: Cookies are used to store helpful data for GA in your device's browser. Since cookies are no longer used, none of your personal data is stored in cookies and thus no user profile is created on you. Although Google Analytics can conduct various measurements and web analyses, the data collected for this purpose is only stored on Google's servers, and thus your privacy is considerably more respected and protected.

Google Remarketing Privacy Policy

We use Google Remarketing, an advertising analysis tool, for our website. The provider of this service is the American company Google Inc. The entity responsible for all Google services in Europe is the company 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.

Google holds a contract on commissioned processing in accordance with Art. 28 DSGVO, which acts as the data protection law basis for our customer relationship with Google. This refers to the EU standard contractual clauses in terms of content. Here you can find the order processing conditions: <https://business.safety.google/intl/en/adsprocessor/terms/>


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

Google Site Kit Privacy Policy

Google Site Kit Privacy Policy Overview


 Affected parties: website visitors

 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. More details can be found below and in Google Analytics' privacy policy.

 Storage period: depending on the properties used

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

What is Google Site Kit?

We have integrated the WordPress plugin Google Site Kit of the American company Google Inc. to our website. For Europe, Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services. With Google Site Kit, we can quickly and easily view statistics of various Google products such as Google Analytics directly on our WordPress dashboard. The in Google Site Kit integrated tools also collect your personal data. In this privacy policy we will explain why we use Google Site Kit, how long and where your data is stored, and which other privacy policies may be relevant to you in this context.

Google Site Kit is a plugin for the WordPress content management system. With this plugin we can view important website analysis statistics directly in our dashboard. These are statistics that are collected by other Google products – primarily by Google Analytics. In addition to Google Analytics, the services Google Search Console, Page Speed Insight, Google AdSense, Google Optimize and Google Tag Manager can also be linked to Google Site Kit.

Why do we use Google Site Kit on our website?

As a service provider, it is our job to offer you the best possible experience on our website. You should feel comfortable on our website. Moreover, you should be able to quickly and easily find exactly what you are looking for. Statistical evaluations help us to get to know you better and to adapt our offer to your wishes and interests. We use various Google tools for these evaluations. Site Kit makes our work a lot easier because we can view and analyse the statistics of Google products on its dashboard. Therefore, we must no longer register for using the respective tools. Site Kit always provides a good overview of the most important analysis data.

What data are stored by Google Site Kit?

If you have consented to the use of tracking tools in the cookie notice (also called script or banner), cookies will be set by Google products such as Google Analytics. Also, on about you, such as your user behaviour, will be sent to Google, where it is stored and processed. This also includes personal data such as your IP address.

You can find more detailed information on the individual services in the respective separate sections of this privacy policy. In our privacy policy on Google Analytics for example, you will be able to view information on the exact types of data that are collected. You will also learn how long Google Analytics stores, manages and processes

data, what cookies can be used and how you can prevent data retention. We also have respective comprehensive privacy policies for other Google services such as Google Tag Manager or Google AdSense.

In the following, we will show you exemplary Google Analytics cookies that may be set in your browser if you have consented to Google's data processing. Please note that this list contains only a selection of potential cookies:

Name: _ga

Value:2.1326744211.152312427560-2

Purpose:Usually analytics.js uses the _ga cookie to store the user ID. Therefore, it can differentiate between website visitors.

Expiry date: after 2 years

Name: _gid

Value:2.1687193234.152312427560-7

Purpose: This cookie does also differentiate between website visitors.

Expiry date: after 24 hours

Name: _gat_gtag_UA_<property-id>

Value: 1

Purpose: This cookie is used to lower the request rate.

Expiry date: after 1 minute

How long and where are the data stored?

Google stores the collected data on its own servers, which are distributed all around the world. Most servers are in the United States, so your data may likely be stored there. At <https://www.google.com/about/datacenters/inside/locations/?hl=uk> you can see exactly where the company provides servers.

Data that is collected by Google Analytics is stored for a standard period of 26 months. After this time, your user data will be deleted. This retention period applies to any data linked to cookies, user identification and advertising IDs.

How can I delete my data or prevent data retention?

You always reserve the right to either receive information about your data, or to have your data deleted, rectified, or reduced. You can also deactivate, delete, or manage cookies in your browser at any time. In the following we will show you the respective instructions to do this in the most common browsers:

[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](#)

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

Legal basis

The use of Google Site Kit requires your consent, which we obtained via our cookie popup. According to **Art. 6 para. 1 lit. a GDPR (consent)**, this consent is the legal basis for processing personal data, such as when it is collected by web analytics tools.

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

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/>


To find out more about data processing by Google, we recommend Google's comprehensive privacy policy at <https://policies.google.com/privacy?hl=en-GB>


Google Tag Manager Privacy Policy

Google Tag Manager Privacy Policy Overview

 Affected parties: website visitors

 Purpose: Organisation of individual tracking tools

 Processed data: Google Tag Manager itself does not store any data. The data record tags of the web analytics tools used.

 Storage period: depending on the web analytics tool used

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

What is Google Tag Manager?

We use Google Tag Manager by the company Google Inc. (1600 Amphitheatre Parkway Mountain View, CA 94043, USA) for our website.

This Tag Manager is one of Google's many helpful marketing products. With it, we can centrally integrate and manage code sections of various tracking tools, that we use on our website.

In this privacy statement we will explain in more detail, what Google Tag Manager does, why we use it and to what extent your data is processed.

Google Tag Manager is an organising tool with which we can integrate and manage website tags centrally and via a user interface. Tags are little code sections which e.g. track your activities on our website. For this, segments of JavaScript code are integrated to our site's source text. The tags often come from Google's intern products, such as Google Ads or Google Analytics, but tags from other companies can also be integrated and managed via the manager. Since the tags have different tasks, they can collect browser data, feed marketing tools with data, embed buttons, set cookies and track users across several websites.

Why do we use Google Tag Manager for our website?

Everybody knows: Being organised is important! Of course, this also applies to maintenance of our website. In order to organise and design our website as well as possible for you and anyone who is interested in our products and services, we rely on various tracking tools, such as Google Analytics.

The collected data shows us what interests you most, which of our services we should improve, and which other persons we should also display our services to. Furthermore, for this tracking to work, we must implement relevant JavaScript Codes to our website. While we could theoretically integrate every code section of every tracking tool separately into our source text, this would take too much time and we would lose overview. This is the reason why we use Google Tag Manager. We can easily integrate the necessary scripts and manage them from one place. Additionally, Google Tag Manager's user interface is easy to operate, and requires no programming skills. Therefore, we can easily keep order in our jungle of tags.

What data is stored by Google Tag Manager?

Tag Manager itself is a domain that neither uses cookies nor stores data. It merely functions as an “administrator“ of implemented tags. Data is collected by the individual tags of the different web analysis tools. Therefore, in Google Tag Manager the data is sent to the individual tracking tools and does not get saved.

However, with the integrated tags of different web analysis tools such as Google Analytics, this is quite different. Depending on the analysis tool used, various data on your internet behaviour is collected, stored and processed with the help of cookies. Please read our texts on data protection for more information on the particular analysis and tracking tools we use on our website.

We allowed Google via the account settings for the Tag Manager to receive anonymised data from us. However, this exclusively refers to the use of our Tag Manager and not to your data, which are saved via code sections. We allow Google and others, to receive selected data in anonymous form. Therefore, we agree to the anonymised transfer of our website data. However, even after extensive research we could not find out what summarised and anonymous data it is exactly that gets transmitted. What we do know is that Google deleted any info that could identify our website. Google combines the data with hundreds of other anonymous website data and creates user trends as part of benchmarking measures. Benchmarking is a process of comparing a company’s results with the ones of competitors. As a result, processes can be optimised based on the collected information.

How long and where is the data stored?

When Google stores data, this is done on Google’s own servers. These servers are located all over the world, with most of them being in America. At <https://www.google.com/about/datacenters/inside/locations/?hl=en> you can read in detail where Google’s servers are.

In our individual data protection texts on the different tools you can find out how long the respective tracking tools store your data.

How can I delete my data or prevent data retention?

Google Tag Manager itself does not set any cookies but manages different tracking websites’ tags. In our data protection texts on the different tracking tools you can find detailed information on how you can delete or manage your data.

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

Legal basis

The use of the Google Tag Manager requires your consent, which we obtained via our cookie popup. According to **Art. 6 para. 1 lit. a GDPR (consent)**, this consent is the legal basis for personal data processing, such as when it is collected by web analytics tools.

In addition to consent, we have a legitimate interest in analysing the behaviour of website visitors and thus technically and economically improving our offer. With the help of Google Tag Managers we can also improve profitability. The legal basis for this is **Art. 6 para. 1 lit. f GDPR (legitimate interests)**. We only use Google Tag Manager if you have given us your consent.

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/>


If you want to learn more about Google Tag Manager, we recommend their FAQs at <https://support.google.com/tagmanager/?hl=en#topic=3441530>.


MonsterInsights Privacy Policy

MonsterInsights Privacy Policy Summary

 Affected parties: website visitors

 Purpose: Evaluation of visitor information for website optimisation.

 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 below or in Google Analytics' privacy policy.

 Storage period: depending on the respective Google Analytics properties used

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

What is MonsterInsights?

On our website, we use the “Google Analytics Plugin for WordPress” by the American company MonsterInsights LCC (7732 Maywood Crest Dr, West Palm Beach, Florida, 33412, USA). The plugin is usually simply called MonsterInsights. With the help of this plugin, your user data can be stored, managed and processed by Google Analytics. If you click on a link for instance, Google Analytics stores this click via the integrated plugin and creates informative web analyses with the collected data. In this privacy policy, we will go into more detail on MonsterInsights and inform you which of your data is retained where and how.

MonsterInsights uses the Google Analytics Reporting API to collect data about our website and visitor behaviour. These data are evaluated and then appear as diagrams, graphics and tables directly on our WordPress dashboard. Moreover, for the plugin to work, a Google Analytics tracking code must be integrated into our WordPress page. The plugin offers functions such as page analyses, statistics or ads tracking. With the help of this plugin, we can set up functions such as event tracking, eCommerce tracking or outbound link tracking for our website. This can be done very easily and without any programming knowledge. With MonsterInsights, we can see all important statistics in a single place directly on our dashboard.

Why do we use MonsterInsights?

MonsterInsights makes using Google Analytics a lot easier for us, as we can see the most important analyses on our dashboard right away and don't always have to switch to Google Analytics. Google Analytics provides us with important data about visitor behaviour on our website. With the help of this data, we can adapt our website and our offer better to your wishes. We use the statistics we obtain to make our website more interesting and to target our advertisements.

Which data are stored by MonsterInsights and Google Analytics?

Upon installation of the MonsterInsights plugin, a Google Analytics tracking code was integrated into our WordPress website. This is used by Google Analytics to create a random, unique ID which is linked to your browser cookie. This helps to identify you as a new visitor to our website. If you visit again, you will be recognised as a so-called “recurring” user. Subsequently, all collected data will be stored with the user ID, whereafter pseudonymous user profiles will be created and evaluated. Your actions on our website are stored in cookies and app instance IDs. If you are using other Google services, the generated data may also be linked to third-party cookies.

All tracking is carried out and retained by Google Analytics. MonsterInsights forwards all data directly to Google Analytics in order to process them on behalf of MonsterInsights. Google will only pass on this data if we allow so or if it is required by the law. MonsterInsights does not use its own cookies to store data, but the code added by MonsterInsights loads Google Analytics, which will set cookies.

For instance, it is recorded which website you came to us from, which buttons and links you click, how long you stay on a certain page for and when you leave the site again.

Furthermore, your IP address is shown and stored in abbreviated form so it will not be possible to assign it to you as a person. Your location may also be approximately determined via your IP address, and technical information such as your device type, browser type, Internet provider or your screen resolution may also be retained.

If you want to know more about data retention and data processing, we recommend you to read our general privacy policy for Google Analytics.

How long and where are the data stored?

MonsterInsights does not store the collected data, but forwards them to Google Analytics. There, the data will be retained on Google's servers. These servers are distributed around the world, but most are located in the United States. At the link <https://www.google.com/about/datacenters/locations/> you can see exactly at which locations data centres can be found. By default, your data is stored by Google for 26 months, but you can also choose different retention periods. Also, please take a look at our Google Analytics privacy policy. The retention period applies to data linked to cookies, user identification and advertising ID. Furthermore, web analyses that appear as reports are generated by aggregated data and are stored independently of your user data.

How can I erase my data or prevent data retention?

You reserve the right to information, rectification, erasure and restriction of your data at any time. If you download and install the browser add-on <https://tools.google.com/dlpage/gaoptout?hl=en-GB>, you can prevent Google Analytics from using your data by deactivating Google Analytics JavaScript.

However, you can also deactivate, manage or delete cookies via your browser. In the following, we will show you the instructions to do this for the most common browsers:

[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](#)

Legal basis

The use of MonsterInsights requires your consent, which we obtained via our cookie popup. According to **Art. 6 para. 1 lit. a GDPR (consent)**, this consent is the legal basis for personal data processing, such as when it is collected by web analytics tools.

In addition to consent, we have legitimate interest in analysing the behaviour of website visitors, and thus technically and economically improving our offer. With the

help of MonsterInsights, we can recognise website errors, identify attacks and improve profitability. The legal basis for this is **Art. 6 para. 1 lit.f GDPR (legitimate interests)**. We only use MonsterInsights if you have given your consent.


MonsterInsights 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.

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


If you want to learn more about the WordPress plugin MonsterInsights, we recommend the website <https://www.monsterinsights.com/>. For more information about Google Analytics' data processing, we recommend you to read our Google Analytics privacy policy, as well as Google's information page at <https://support.google.com/analytics/answer/6004245?hl=en> and Google Analytics' Terms of Service site at <https://marketingplatform.google.com/about/analytics/terms/gb/>.


WP Statistics Privacy Policy

WP Statistics 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 anonymised IP addresses, duration of the website visit or your click behaviour.

 Storage period: the data are stored until they are no longer required for the intended purposes

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

What is WP Statistics?

On our website we use the analysis plugin WP Statistics. This plugin has been developed by the American software company Veronalabs (5460 W Main St, Verona, NY 13478, United States). The plugin allows us to receive simple statistics on how you as a user interact with our website. In this privacy policy we will go into more detail about the analysis tool and show you where and for how long your data is stored.

This plugin is an analysis software which was specially developed for websites that use the WordPress content management system. WordPress helps us to easily edit our website even without any programming knowledge. WP Statistics may for example collect data about how long you stay on our website, what subpages you visit, how many visitors are on our website or which website led you to us. Furthermore, WP Statistics does not set any cookies and you cannot be personally identified by the collected data.

Why do we use WP Statistics?

With the help of WP Statistics, we obtain simple statistics that help us to continuously improve and make our website even more interesting for you. Our website and the content, products and/or services offered on it should meet your needs and demands as closely as possible. In order to achieve this goal, we of course have to find out where there is room for improvements and changes. The statistics obtained help us to get one step closer to this goal.

Which data is stored by WP Statistics?

WP Statistics does not set any cookies and the collected data are only used to generate anonymised statistics on the use of our website. WP Statistics also anonymises your IP address. You cannot be identified as a person.

WP Statistics collects visitor data when your web browser connects to our web server. These data are then stored in our server's database. The retained data may for example be:

- the address (URL) of the accessed website
- browser and browser version
- the operating system used
- the address (URL) of the previously visited page (referrer URL)
- the hostname and IP address of the device from which our website was accessed
- date and time
- information on the country/city
- number of visitors that come from a search engine
- duration of the website stay
- clicks on the website

Your data will not be passed on or sold.

How long and where are the data stored?

All data is retained locally on our web server. Your data will be stored on our web server until it is no longer needed for the purposes listed above.

How can I erase my data or prevent data retention?

You have the right to information, rectification, deletion or restriction of the processing of your personal data at any time. Moreover, you can revoke your consent to the data processing anytime.

Legal basis

The use of WP Statistics requires your consent, which we obtained via our cookie popup. According to **Art. 6 para. 1 lit. a GDPR (consent)**, this consent represents the legal basis for personal data processing, such as when it is collected by web analytics tools.

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


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. Data processing is mainly done by WP Statistics. This can lead to data not being anonymously processed and stored. Furthermore, US government authorities may get access to individual data. This data may also get linked to data from other possible WP Statistics services that you have a user account with.


We have now given you the most important information about data processing by WP Analytics. Your data is handled very carefully, as the plugin does not use cookies and the data for statistical analyses are stored locally on our web server. If you want to learn more about WP Analytics, you can view the company's privacy policy at <https://wp-statistics.com/privacy-and-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.

MailPoet Privacy Policy


We use MailPoet on our website, which is a service for our email marketing. The service provider is the Irish company Aut O'Mattic A8C Ireland Ltd, Grand Canal Dock, 25 Herbert Pl, Dublin, D02 AY86, Ireland.


You can find out more about the data that is processed through the use of MailPoet in the privacy policy at <https://automattic.com/privacy/>.

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.

Facebook Messenger Privacy Policy

We use the instant messaging service Facebook Messenger on our website. The service provider is the American company Meta Platforms Inc. For the European area, the company Meta Platforms Ireland Limited (4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland) is responsible.

What is Facebook Messenger?

Facebook Messenger is a chat messaging feature developed by Facebook, allowing you to send and receive text messages, voice and video calls, photos, and other media files to other Facebook users.

When you use Facebook Messenger, your personal data is also processed on Facebook servers. This includes not only your phone number and chat messages but also sent photos, videos, profile data, your address, or your location.

Why do we use Facebook Messenger?

We want to stay in touch with you, and this works best through messaging services like Facebook Messenger. On one hand, because the service works flawlessly, and on the other hand, because Facebook is still one of the most well-known social media platforms. The service is practical and allows for uncomplicated and fast communication with you.

How secure is data transfer with Facebook Messenger?

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>.

You can learn more about the data processed through the use of Facebook in the Privacy Policy at <https://www.facebook.com/about/privacy>.

WhatsApp Privacy Policy

We use the instant messaging service WhatsApp on our website. The service provider is the American company WhatsApp Inc., a subsidiary of Meta Platforms Inc. (formerly Facebook Inc. until October 2021). For the European region, the responsible company is WhatsApp Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland.

What is WhatsApp?

We probably don't need to introduce WhatsApp to you in detail. The likelihood that you use this well-known messaging service on your smartphone is relatively high. For many years, there have been voices criticizing WhatsApp or its parent company Meta Platforms regarding their handling of personal data. The main criticism in recent years has been the merging of WhatsApp user data with Facebook. In response, Facebook adjusted its terms of service in 2021. Facebook stated that, as of 2021, no personal data from WhatsApp users is currently being shared with Facebook.

However, if you use WhatsApp and have consented to the data processing, various personal data about you will be processed by WhatsApp. This includes your phone number, chat messages, sent photos, videos, and profile data. Photos and videos are supposed to be stored only temporarily, and all messages and calls are encrypted end-to-end. Therefore, they should not be accessible by Meta itself. In addition, information from your address book and other metadata are stored by WhatsApp.

Why do we use WhatsApp?

We want to stay in touch with you, and the best way to do that is via WhatsApp. On the one hand, because the service works flawlessly, and on the other hand, because WhatsApp is still the most widely used instant messaging tool worldwide. The service is practical and enables uncomplicated and quick communication with you.

How secure is data transfer with WhatsApp?

WhatsApp processes data from you, among other things, in the USA. WhatsApp 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, WhatsApp 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, WhatsApp 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.


Information on data transfers at WhatsApp, which comply with the standard contractual clauses, can be found at <https://www.whatsapp.com/legal/business-data-transfer-addendum-20210927>


We hope we have provided you with the most important information about the use and data processing by WhatsApp. You can learn more about the data processed through the use of WhatsApp in their Privacy Policy at <https://www.whatsapp.com/privacy>.

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 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: 0jiejy4312427560c2GnlufEJ9..Bde09j...1.0.Bde09j

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

Expiry date: after 3 months

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

If you are registered with Facebook, you can change your settings for advertisements yourself at

https://www.facebook.com/ads/preferences/?entry_product=ad_settings_screen. If

you are not a Facebook user, you can go to

<https://www.youronlinechoices.com/uk/your-ad-choices/> and manage your usage-based online advertising. There you have the option to deactivate or activate providers.

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

Facebook Fanpage Privacy Policy

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

Facebook 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>.


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

Instagram Privacy Policy


Instagram Privacy Policy Overview

 Affected parties: website visitors

 Purpose: optimising our service

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

More details can be found in the privacy policy below.

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

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

What is Instagram?

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

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

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

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

Why do we use Instagram on our website?

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

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

What data is stored by Instagram?

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

Facebook distinguishes between customer data and event data. We assume this is also the case for Instagram. Customer data are for example names, addresses, phone numbers and IP addresses. These data are only transmitted to Instagram, if they have been "hashed" first. Thereby, a set of data is transformed into a string of characters,

which encrypts any contact data. Moreover, the aforementioned “event data” (data on your user behaviour) is transmitted as well. It is also possible, that contact data may get combined with event data. The collected data data is matched with any data Instagram already has on you.

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

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

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

The following cookies were used in our test:

Name: csrftoken

Value: “”

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

Expiry date: after one year

Name: mid

Value: “”

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

Expiry date: after end of session

Name: fbsr_312427560124024

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_UjKvXgYe312427560”

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 plugin. 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-c2e2d7235c16312427560-

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=AQF6KNnJ0G312427560...

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:3124275602900777718326218137

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.


Data Processing Agreement (DPA) LinkedIn

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have entered into a Data Processing Agreement (DPA) with LinkedIn. What exactly a DPA is and especially what must be included in a DPA, you can read in our general section "Data Processing Agreement (DPA)".


This contract is required by law because LinkedIn processes personal data on our behalf. It clarifies that LinkedIn may only process data they receive from us according to our instructions and must comply with the GDPR. You can find the link to the Data Processing Agreement (DPA) under <https://www.linkedin.com/legal/l/dpa?>

TikTok Privacy Policy

TikTok 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: varies depending on settings

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

What is TikTok?

On our website, we use TikTok integration. The service provider is the Chinese company Beijing Bytedance Technology Ltd. For the European region, the responsible entity is the Irish company TikTok Technology Limited, 10 Earlsfort Terrace, Dublin, D02 T380, Ireland. TikTok is a popular social media platform, especially among young people, where users can create, share, and view short video clips.

In this privacy policy, we inform you about the data processed by TikTok, how long the data is stored, and how you can manage your privacy settings.

Why do we use TikTok on our website?

We have incorporated TikTok into our website so that you can watch TikTok videos if you wish and potentially interact with the videos. TikTok is known for its funny and creative content, and naturally, we don't want to withhold such content from you. After all, we also enjoy watching creative TikTok videos ourselves.

What data is processed by TikTok?

When you watch TikTok videos on our website or interact with them, TikTok may collect information about your usage behavior and your device. This may include data such as your IP address, browser type, operating system, location, and other technical information. TikTok may also use cookies and similar technologies to collect information and personalize your user experience.

If you have a TikTok account, additional information may be collected and processed. This includes user information (such as name, birthdate, or email address) and data about your communication with other TikTok users.

How long and where are the data stored?

The storage duration and locations of the data collected by TikTok can vary significantly and are subject to TikTok's privacy policies. TikTok may also store data on servers in the United States and other countries. The storage duration typically complies with applicable legal requirements and internal policies. However, we have not been able to determine the exact duration of data storage. We will inform you as soon as we have more information on this matter.

How can I delete my data or prevent data storage?

If you have a TikTok account, you can manage your privacy settings directly on TikTok. For example, in the settings of your TikTok account, you can specify which information can be shared and which cannot. Additionally, you can manage and disable cookies in your web browser to limit data collection. This is also possible without a TikTok account. However, please note that this may affect the functionality of our website and your TikTok experience.

Legal basis

If you have consented to TikTok processing and storing your data, this consent serves as the legal basis for data processing (Art. 6 para. 1 lit. a GDPR). In general, your data is also stored and processed based on our legitimate interest (Art. 6 para. 1 lit. f GDPR) in effective and efficient communication with you or other customers and business partners. However, we only use embedded social media elements if you have given your consent. TikTok may also set cookies in your browser to store data. Therefore, we recommend that you read our cookie privacy text carefully and view the privacy policy or cookie policies of the respective service provider.

TikTok processes data from you, including in the United States. We would like to inform you that, according to the opinion of the European Court of Justice, there is currently no adequate level of protection for data transfer to the United States. This may entail various risks for the legality and security of data processing.

As the basis for data processing with recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, especially in the United States) or data transfers to such countries, TikTok uses so-called Standard Contractual Clauses (= Art. 46 para. 2 and 3 GDPR). Standard Contractual Clauses (SCC) are model templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the United States). Through these clauses, TikTok commits to maintaining the European level of data protection when processing your relevant data, even when the data is stored, processed, and managed in the United States. These clauses are based on an implementing decision by the EU Commission. You can find the decision and the corresponding Standard Contractual Clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=en

For more information about TikTok's privacy policy and data collection by TikTok, please visit the TikTok website at <https://www.tiktok.com/legal/page/eea/privacy-policy/en> and the general information about TikTok at <https://www.tiktok.com/en/>.

Online Marketing


Online Marketing Privacy Policy Overview

 Affected parties: visitors to the website

 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. Personal data such as name or email address may also be processed. You can find more details on this from the respective Online Marketing tool.

 Storage period: depending on the Online Marketing tools used

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

What is Online Marketing?

Online Marketing refers to all measures that are carried out online to achieve marketing goals, such as increasing brand awareness or doing business transactions. Furthermore, our Online Marketing measures aim to draw people's attention to our website. In order to be able to show our offer to many interested people, we do Online Marketing. It mostly is about online advertising, content marketing or search engine optimisation. For this, personal data is also stored and processed, to enable us to use Online Marketing efficiently and targeted. On the one hand, the data help us to only show our content to people who are interested in it. On the other hand, it helps us to measure the advertising success of our Online Marketing measures.

Why do we use Online Marketing tools?

We want to show our website to everyone who is interested in our offer. We are aware that this is not possible without conscious measures being taken. That is why we do Online Marketing. There are various tools that make working on our Online Marketing measures easier for us. These also provide suggestions for improvement via data. Thus, we can target our campaigns more precisely to our target group. The ultimate purpose of these Online Marketing tools is to optimise our offer.

Which data are processed?

For our Online Marketing to work and to measure its success, user profiles are created and data are e.g. stored in cookies (small text files). With the help of this data, we can not only advertise in the traditional way, but also present our content directly on our website in the way you prefer. There are various third-party tools that offer these functions and thus collect and store your data accordingly. The aforementioned cookies e.g. store the pages you visit on our website, how long you view these pages, which links or buttons you click or which website you came from. What is more, technical information may also be stored. This may include e.g. your IP address, the browser and device you use to visit our website or the time you accessed our website as well as the time you left. If you have agreed for us to determine your location, we can also store and process it.

Your IP address is stored in pseudonymised form (i.e. shortened). What is more, distinct data that directly identify you as a person, such as your name, address or email address, are only stored in pseudonymised for advertising and Online Marketing purposes. With

this data we cannot identify you as a person and only retain the pseudonymised information that is stored in your user profile.

Under certain circumstances, cookies may also be utilised, analysed and used for advertising purposes on other websites that use the same advertising tools. Thus, your data may then also be stored on the servers of the respective provider of the advertising tool.

In rare exceptions, unique data (name, email address, etc.) may also be stored in the user profiles. This can happen, if you are for example a member of a social media channel that we use for our Online Marketing measures and if the network connects previously received data with the user profile.

We only ever receive summarised information from the advertising tools we use that do store data on their servers. We never receive data that can be used to identify you as an individual. What is more, the data only shows how well-placed advertising measures have worked. For example, we can see what measures have caused you or other users to visit our website and purchase a service or product. Based on these analyses we can improve our advertising offer in the future and adapt it more precisely to the needs and wishes of people who are interested.

Duration of data processing

Below we will inform you on the duration of data processing, provided we have this information. In general, we only process personal data for as long as is absolutely necessary to provide our services and products. Data stored in cookies are retained for different lengths of time. Some cookies are deleted after you leave a website, while others may be stored in your browser for a number of years. However, in the respective privacy policies of the respective provider, you will usually find detailed information on the individual cookies this provider uses.

Right of withdrawal

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 for example also prevent data collection by cookies if you manage, deactivate or erase cookies in your browser. The legality of the processing remains unaffected to the point of revocation.

Since Online Marketing tools usually use cookies, 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, you should read the privacy policies of the respective tools.

Legal basis

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


Moreover, we have a legitimate interest in measuring our online marketing activities in anonymised form, in order to use this data for optimising our offer and our Marketing. The corresponding legal basis for this is **Art. 6 para. 1 lit. f GDPR (legitimate interests)**. Nevertheless, we only use these tools if you have given your consent.


Information on special online marketing tools can be found in the following sections, provided this information is available.


Google Ads (Google AdWords) Conversion Tracking Privacy Policy

Google Ads (Google AdWords) Conversion Tracking Privacy Policy Overview

 Affected parties: visitors to the website

 Purpose: economic success and service optimisation.

 Processed data: Access statistics that contain data such as access location, device data, access duration and time, navigation behaviour, click behaviour and IP addresses. Personal data such as name or email address may also be processed.

 Storage period: Conversion cookies usually expire after 30 days and do not transmit any personal data

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

What is Google Ads conversion tracking?

We use Google Ads (previously Google AdWords) as an online marketing measure, to advertise our products and services. Thus, we want to draw more people's attention on the internet to the high quality of our offers. As part of our advertising measures with Google Ads, we use the conversion tracking of Google LLC., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA ("Google") on our website. With the aid of this free tracking tool we can tailor our advertising offer better to your interests and needs. In the following article we will explain, why we use conversion tracking, what data gets saved and how you can prevent this data retention.

Google Ads (previously Google AdWords) is the internal online advertising system of the company Google LLC. We are convinced of our offer's quality and would like as many people as possible to discover our website. For this, Google Ads offers the best platform within the online environment. Of course, we also want to get an overview of the cost-benefit factor of our advertising campaigns. Thence, we use Google Ads' conversion tracking tool.

But what is a conversion actually? A conversion occurs, when you turn from an interested visitor into an acting website visitor. This happens every time you click on our ad and then make another action, such as paying a visit to our website. With Google's conversion tracking tool, we can understand what happens after a user clicks

our Google ad. It shows us for instance if products get bought, services are used or whether users have subscribed to our newsletter.

Why do we use Google Ads conversion tracking on our website?

We use Google Ads to show our offer also across other websites. Our aim is for our advertising campaigns to reach only those people, who are interested in our offers. With the conversion tracking tool, we see what keywords, ads, ad groups and campaigns lead to the desired customer actions. We see how many customers interact with our ads on a device, to then convert. With this data we can calculate our cost-benefit-factor, measure the success of individual ad campaigns and therefore optimise our online marketing measures. With the help of the obtained data we can give our website a more interesting design and customise our advertising offer better to your needs.

What data is stored with Google Ads conversion tracking?

For a better analysis of certain user actions, we have integrated a conversion tracking tag, or code snippet to our website. Therefore, if you click one of our Google ads, a Google domain stores the cookie "conversion" on your computer (usually in the browser) or on your mobile device. Cookies are little text files that save information on your computer.

Here are data of the most significant cookies for Google's conversion tracking:

Name: Conversion

Value: EhMI_aySuoyv4gIVled3Ch0llweVGAEgt-mr6aXd7dYISAGQ312427560-3

Purpose: This cookie saves every conversion you make on our website after you came to us via a Google ad.

Expiry date: after 3 months

Name: _gac

Value:

1.1558695989.EAlalQobChMliOmEgYO04gIVj5AYCh2CBAPrEAAAYASAAEgIYQfD_BwE

Purpose: This is a classic Google Analytics Cookie that records various actions on our website.

Expiry date: after 3 months

Note: The cookie _gac only appears in connection with Google Analytics. The above list does not claim to be exhaustive, as Google repeatedly change the cookies they use for analytical evaluation.

As soon as you complete an action on our website, Google identifies the cookie and saves your action as a so-called conversion. For as long as you surf our website, provided the cookie has not expired, both Google and us can determine that you found your way to us via a Google ad. Then, the cookie is read and sent back to Google Ads, together with the conversion data. Moreover, other cookies may also be used for measuring conversions. Google Ads' conversion tracking can be fine-tuned and

improved with the aid of Google Analytics. Furthermore, ads which Google displays in various places across the web, might be placed under our domain with the name “_gads” or “_gac”.

Since September 2017, analytics.js retains various campaign information with the _gac cookie. This cookie stores data, as soon as you open one of our sites that has been set up for Google Ads’ auto-tagging. In contrast to cookies that are placed for Google domains, Google can only read these conversion cookies when you are on our website. We do neither collect nor receive any personal data. We do obtain a report with statistical evaluations by Google. With the help thereof, we can not only see the total number of users who clicked our ad, but also what advertising measures were well received.

How long and where is the data stored?

At this point we want to reiterate, that we have no influence on how Google use the collected data. According to Google, the data are encrypted and stored on a secure server. In most cases, conversion cookies expire after 30 days, and do not transmit any personalised data. The cookies named “conversion” and “_gac” (which is used with Google Analytics) have an expiry date of 3 months.

How can I erase my data or prevent data retention?

You have the possibility to opt out of Google Ads’ conversion tracking. The conversion tracking can be blocked by deactivating the conversion tracking cookie via your browser. If you do this, you will not be considered for the statistic of the tracking tool. You can change the cookie settings in your browser anytime. Doing so, works a little different in every browser. Hence, in the following you will find an instruction on 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 potential cookie is about to be set. This lets you decide upon permitting or denying the cookie’s placement. By downloading and installing the browser plugin at <https://support.google.com/ads/answer/7395996> you can also deactivate all “advertising cookies”. Please consider that by deactivating these cookies, you cannot prevent all advertisements, only personalised ads.

Legal basis

If you have consented to the use of Google Ads Conversion Tracking, your consent is the legal basis for the corresponding data processing. According to **Art. 6 para. 1 lit. a GDPR (consent)**, this consent is the legal basis for personal data processing, as may be done when collected by Google Ads Conversion Tracking.

We also have legitimate interest in using Google Ads Conversion Tracking to optimise our online service and marketing measures. The corresponding legal basis for this is **Art. 6 para. 1 lit. f GDPR (legitimate interests)**. Nevertheless, we only use Google Ads Conversion Tracking if you have consented 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/>


If you would like to find out more about data protection at Google, we recommend Google's privacy policy at: <https://policies.google.com/privacy?hl=en-GB>.


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).


Real Cookie Banner Privacy Policy


We use the consent management tool Real Cookie Banner on our website. The service provider is the German company devowl.io GmbH, located at Tannet 12, 94539 Grafing, Germany.


To learn more about the data processed through the use of Real Cookie Banner, please refer to the privacy policy at <https://devowl.io/privacy-policy/>.

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 not 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-312427560-8

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: U7j1v3dZa3124275600xgZFmiqWppRWKOr

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: 0WmuWqy312427560zILzqV_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: gEAABBCjJMXcl0dSAAAANbqc312427560-4

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=312427560>.

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>.

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/>.

Payment providers


Payment Providers Privacy Policy Overview


 Affected parties: visitors to the website

 Purpose: To enable and optimise the payment process on our website

 Processed data: data such as name, address, bank details (account number, credit card number, passwords, TANs, etc.), IP address and contract data

You can find more details on this directly from the payment provider tool that is being used.

 Storage period: depending on the payment provider that is being used

 Legal basis: Art. 6 paragraph 1 lit. b GDPR (performance of a contract)

What is a payment provider?

On our website we use online payment systems, which enable us as well as you to have a secure and smooth payment process available. Among other things, personal data may also be sent to the respective payment provider, where it may also be stored and processed. Payment providers are online payment systems that enable you to place an order via online banking. The payment processing is carried out by the payment provider of your choice. We will then receive information about the payment. This method can be used by any user who has an active online banking account with a PIN and TAN. There are hardly any banks that do not offer or accept such payment methods.

Why do we use payment providers on our website?

With both our website and our embedded online shop, we of course want to offer you the best possible service, so you can feel comfortable on our site and take advantage of our offers. We know that your time is valuable and that payment processing in particular has to work quickly and smoothly. Thus, we offer various payment providers. You can choose your preferred payment provider and pay in the usual way.

Which data are processed?

What exact data that is processed of course depends on the respective payment provider. However, generally data such as name, address, bank details (account number, credit card number, passwords, TANs, etc.) do get stored. This data is necessary for carrying out any transactions. In addition, any contract data and user data, such as when you have visited our website, what content you are interested in or which sub-pages you have clicked, may also be stored. Most payment providers also store your IP address and information about the computer you are using.

Your data is usually stored and processed on the payment providers' servers. We, so the website operator, do not receive this data. We only get information on whether the payment has gone through or not. For identity and credit checks, it may happen for payment providers to forward data to the appropriate body. The business and privacy policy principles of the respective provider always apply to all payment transactions. Therefore, please always take a look at the general terms and conditions and the privacy policy of the payment provider. You e.g. also have the right to have data erased or rectified at any time. Please contact the respective service provider regarding your rights (right to withdraw, right of access and individual rights).

Duration of data processing

Provided we have further information on this, we will inform you below about the duration of the processing of your data. In general, we only process personal data for as long as is absolutely necessary for providing our services and products. This storage period may be exceeded however, if it is required by law, for example for accounting purposes. We keep any accounting documents of contracts (invoices, contract documents, account statements, etc.) for 10 years (Section 147 AO) and other relevant business documents for 6 years (Section 247 HGB).

Right to object

You always have the right to information, rectification and erasure of your personal data. If you have any questions, you can always contact the person that is responsible for the respective payment provider. You can find contact details for them either in our respective privacy policy or on the relevant payment provider's website.

You can erase, deactivate or manage cookies in your browser, that payment providers use for their functions. How this works differs a little depending on which browser you are using. Please note, however, that the payment process may then no longer work.

Legal basis

For the processing of contractual or legal relationships (**Art. 6 para. 1 lit. b GDPR**), we offer other payment service providers in addition to the conventional banking/credit institutions. In the privacy policy of the individual payment providers (such as Amazon Payments, Apple Pay or Discover) you will find a detailed overview of data processing and data storage. In addition, you can always contact the responsible parties should you have any questions about data protection issues.


Provided it is available, you can find information on the special payment providers in the following sections.

Stripe Privacy Policy


Stripe Privacy Policy Overview


 Affected parties: website visitors

 Purpose: optimising the payment process on our website

 Processed data: data such as name, address, bank details (account number, credit card number, passwords, TANs, etc.), IP address and contract data

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

 Storage period: data is stored until the collaboration with Stripe is terminated

 Legal basis: Art. 6 para. 1 lit. b GDPR (contract processing), Art. 6 para. 1 lit. a GDPR (consent)

What is Stripe?

On our website we use a payment tool by Stripe, an American technology company and online payment service. Stripe Payments Europe (Europe Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Ireland) is responsible for customers within the EU. Therefore, if you choose Stripe as your payment method, your payment will be processed via Stripe Payments. Hence, the data required for the payment process is forwarded to Stripe where it is then stored. In this privacy policy we will give you an overview of Stripe's data processing and retention. Moreover, we will explain why we use Stripe on our website.

The technology company Stripe offers payment solutions for online payments. Stripe enables us to accept credit and debit card payments in our webshop while it handles the entire payment process. A major advantage of Stripe is that you never have to leave our website or shop during the payment process. Moreover, payments are processed very quickly via Stripe.

Why do we use Stripe on our website?

We of course want to offer the best possible service with both our website and our integrated online shop. After all, we would like you to feel comfortable on our site and take advantage of our offers. We know that your time is valuable and therefore, payment processing in particular must work quickly and smoothly. In addition to our other payment providers, with Stripe we have found a partner that guarantees secure and fast payment processing.

What data are stored by Stripe?

If you choose Stripe as your payment method, your personal data (transaction data) will be transmitted to Stripe where it will be stored. These data include the payment method (i.e. credit card, debit card or account number), bank sort code, currency, as

well as the amount and the payment date. During a transaction, your name, email address, billing or shipping address and sometimes your transaction history may also be transmitted. These data are necessary for authentication. Furthermore, Stripe may also collect relevant data for the purpose of fraud prevention, financial reporting and for providing its services in full. These data may include your name, address, telephone number as well as your country in addition to technical data about your device (such as your IP address).

Stripe does not sell any of your data to independent third parties, such as marketing agencies or other companies that have nothing to do with Stripe. However, data may be forwarded to internal departments, a limited number of Stripe's external partners or for legal compliance reasons. What is more, Stripe uses cookies to collect data. Here is a selection of cookies that Stripe may set during the payment process:

Name: m

Value: edd716e9-d28b-46f7-8a55-e05f1779e84e040456312427560-5

Purpose: This cookie appears when you select your payment method. It saves and recognises whether you are accessing our website via a PC, tablet or smartphone.

Expiry date: after 2 years

Name: __stripe_mid

Value: fc30f52c-b006-4722-af61-a7419a5b8819875de9312427560-1

Purpose: This cookie is required for carrying out credit card transactions. For this purpose, the cookie stores your session ID.

Expiry date: after one year

Name: __stripe_sid

Value: 6fee719a-c67c-4ed2-b583-6a9a50895b122753fe

Purpose: This cookie also stores your ID. Stripe uses it for the payment process on our website.

Expiry date: after end of the session

How long and where are the data stored?

Generally, personal data are stored for the duration of the provided service. This means that the data will be stored until we terminate our cooperation with Stripe. However, in order to meet legal and official obligations, Stripe may also store personal data for longer than the duration of the provided service. Furthermore, since Stripe is a global company, your data may be stored in any of the countries Stripe offers its services in. Therefore, your data may be stored outside your country, such as in the USA for example.

How can I erase my data or prevent data retention?

Please note that when you use 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 must not simply be transferred to, as well as stored and processed in insecure third countries, unless there are suitable

guarantees (such as EU standard contractual clauses) between us and the respective non-European service provider.

You always reserve the right to information, correction and deletion of your personal data. Should you have any questions, you can contact the Stripe team at <https://support.stripe.com/contact/email>.

You can erase, deactivate or manage cookies in your browser that Stripe uses for its functions. This works differently depending on which browser you are using. Please note, however, that if you do so the payment process may no longer work. 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](#)

Legal basis

For the processing of contractual or legal relationships (**Art. 6 para. 1 lit. b GDPR**), we offer the payment service provider Sofortüberweisung in addition to the conventional bank/credit institutions. Successful use of the service also requires your consent (**Art. 6 para. 1 lit. a GDPR**), provided the use of cookies is necessary for it.

Stripe processes data from you, among other things, in the USA. Stripe 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, Stripe 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, Stripe 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 now given you a general overview of Stripe's data processing and retention. If you want more information, Stripe's detailed privacy policy at <https://stripe.com/privacy> is a good source.

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.

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-CV6ojl5Y312427560-1

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: zLLvClZSkqGsSwl/AU1aZI6HY7312427560-

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: AFmmF2swRQlhALI6aL...

Purpose: This cookie stores information on your login data.

Expiry date: after 2 years

Name: SAPISID

Value: 7oaPxoG-pZsJuuF5/AnUdDUIsJ9iJz2vdM

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: oQfNKjAsI312427560-

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-CV6ojI5312427560Y

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

Expiry date: after end of session

Name: PREF

Value: f1=50000000

Purpose: This cookie also registers your unique ID. Google uses PREF 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: 31242756095Chz8bagyU

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/adsprocessor/terms/>.

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

ProvenExpert Privacy Policy


We also use the rating platform ProvenExpert for our website. The provider of this service is the German company Expert Systems AG, Quedlinburger Strasse 1, 10589 Berlin, Germany. You can find out more about the data that is processed through the use of ProvenExpert in their Privacy Policy at <https://www.provenexpert.com/en-gb/privacy-policy/>.

Web Design Introduction

Web Design Privacy Policy Overview


 Affected parties: website visitors

 Purpose: improvement of user experience

 Processed data: depends heavily on the services used. Usually, data such as IP address, technical data, language settings, browser version, screen resolution

and browser name are processed. You can find more details directly with the respective web design tools.

 Storage duration: depends on the tools used

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

What is web design?

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

Why do we use web design tools?

The way you absorb information on a website depends very much on its structure, functionality and visual perception. Therefore, good and professional web design has become increasingly important for us. We are constantly working on improving our site as a way of further extending our services for you as a website visitor. Furthermore, a beautiful and functioning website also has economic advantages for us. Needless to say, you will only visit it and take advantage of our offers if you feel completely at ease.

What data is stored by web design tools?

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

Duration of data processing

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

Right to object

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

Legal Basis

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

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

Adobe Fonts Privacy Policy

We use Adobe's Typekit fonts on our website, which is a web font hosting service. The provider of this service is the American company Adobe Inc. The Irish company Adobe Systems Software Ireland Companies, 4-6 Riverwalk, Citywest Business Campus, Dublin 24, Ireland, is responsible for the European region.

Adobe processes data from you, among other things, in the USA. Adobe 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, Adobe 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, Adobe 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 at Adobe at <https://www.adobe.com/uk/privacy/eudatatransfers.html>.

You can find out more about the data processed by using Adobe Fonts in the Privacy Policy at <https://www.adobe.com/de/privacy.html>.

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>.

Font Awesome Lokal Privacy Policy

We use the Font Awesome Local font and icon toolkit for our website. The service provider is the American company Fonticons, Inc, 307 S Main St Ste 202 Bentonville, AR, 72712-9214, USA.

We have embedded the Font Awesome fonts locally, i.e. on our web server – not on Font Awesome's servers. As a result, there is no connection to Font Awesome servers and thus no data transfer or storage to this company.

You can find out more about the data that is processed by Font Awesome Lokal in their Privacy Policy at <https://fontawesome.com/privacy>.

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/fonts) 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=312427560>. 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=312427560>. 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/adsprocessorterms/>

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=h26c1Ktha7fCQTx8rXgLyATyITJ312427560-5

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>.

Online Booking Systems Introduction


Online Booking Systems Privacy Policy Overview

 Affected parties: website visitors

 Purpose: improvement of user experience and organisation

 Processed data: depends heavily on the services used. Usually, data such as IP address, contact and payment details and/or technical data is processed. You can get more details on this directly from 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 is an online booking system?

We use one or more booking systems which enable you to make bookings via our website. That way e.g. appointments can easily be created online. A booking system is a software application integrated into our website that displays available resources (such as available appointments) and allows you to book – and usually, also pay – directly online. You've probably already come across many such booking systems from the restaurant or hotel industry. However, such systems are actually used in a wide variety of industries. Depending on the tool and settings, booking systems can be used both by us internally, as well as by customers like yourself. In most cases, your personal data is also collected and stored.

Bookings usually work as follows: You will find a booking system on our website, through which you can book an appointment directly with one click. Then you will enter your data and usually also be able to pay immediately. You may also have the option to enter various information about yourself into a form. Please be aware that any information you enter may be stored and managed in a database.

Why do we use an online booking system?

In a way, we also consider our website a free service for you. We want you to receive helpful information on our site and feel comfortable on there. This also includes an online service that makes it as easy as possible for you to book appointments or services. Gone are the days when you had to wait days for booking confirmations via phone or email. With an online booking system, you can get everything done after just a few clicks and get on with your day. The system also makes it easier for us to manage all bookings and appointments. Therefore, we consider a booking system absolutely sensible for both you and ourselves.

Which data is processed?

In this general introduction about booking systems, we naturally cannot tell you exactly what data is processed for which system. It always depends on the tool used, as well as the functions and possibilities it contains. What is more, in addition to the conventional booking function, many booking systems also offer a range of other features. For example, many systems also have an external online payment system (e.g. Stripe, Klarna or Paypal) and an integrated calendar synchronisation function. Accordingly, different data and different amounts of data can be processed, depending on the included functions. Usually, data such as your IP address, name and contact details, technical device information and the time of your booking are processed. If you also make a payment via the system, your bank details such as your account number, credit card number, passwords, TANs etc. will also be stored and passed on to the respective payment provider. We recommend you carefully read the respective privacy policy of the tool used, so that you know which of your data is processed specifically.

Duration of data processing

Each booking system stores data for different lengths of time. Therefore, we cannot yet give any specific information about the duration of data processing in this instance. In general, however, personal data is only stored for as long as is absolutely necessary to provide the services. Booking systems usually also use cookies, which store information for different lengths of time. While some cookies are erased immediately after leaving the site, others can be stored for a number of years. You can find out more about this in our “Cookies” section. Please also take a look at the respective privacy policies of the providers. There you should find answers on how long your data will be stored specifically.

Right to object

If you have consented to data processing by a booking system, you always retain the option and the right to revoke this consent. So please, always be aware that you have

rights in relation to your personal data and that you can exercise these rights at any time. Thus, if you do not agree to the processing of your personal data, then none of your personal data may be processed. It is that simple. The easiest way to revoke data processing is via a cookie consent tool or via other available opt-out functions. You can, for example, manage data retention by cookies directly in your browser. Until you withdraw your consent, the lawfulness of data processing remains unaffected.

Legal Basis

If you have agreed that booking systems may be used, this consent is the legal basis for the corresponding data processing. According to Article 6 (1) (a) GDPR (consent), your consent represents the legal basis for the processing of personal data, as it may occur through the use of booking systems.

Furthermore, we also have a legitimate interest in using booking systems because we use them to extend our customer service and to optimise our internal booking organisation. The corresponding legal basis for this is Article 6 (1) (f) GDPR (legitimate interests). However, we strongly want to emphasise once more that we only use these tools if you have given your consent.

You can find information on different booking systems – if available – in the following sections.

Calendly Privacy Policy

We use Calendly, a planning and organization tool, for our website. The service provider is the American company Calendly LCC, 271 17th St NW, Ste 1000, Atlanta, Georgia, 30363, USA.

Calendly 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.

Calendly 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, Calendly 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.

You can find out more about the data that is processed through the use of Calendly in their Privacy Policy at <https://calendly.com/privacy>.

Data Processing Agreement (DPA) Calendly

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have entered into a Data Processing Agreement (DPA) with Calendly. What exactly a DPA is and especially what must be included in a DPA, you can read in our general section “Data Processing Agreement (DPA)”.


This contract is required by law because Calendly processes personal data on our behalf. It clarifies that Calendly may only process data they receive from us according to our instructions and must comply with the GDPR. You can find the link to the Data Processing Agreement (DPA) under <https://calendly.com/dpa>.

Miscellaneous Overview


Miscellaneous Privacy Policy Overview

 Affected parties: website visitors

 Purpose: Improvement of user experience

 Processed data: The processed data depends heavily on the services used. Usually, it is an IP address and/or technical data. You can find more details on this in the sections of the respective tools.

 Storage duration: depends on the tools used

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

What is included in “Miscellaneous”?

The “Miscellaneous” category includes any services that do not fit into any of the above categories. Usually, they are various plugins and integrated elements that are meant to improve our website. Generally, these functions are obtained from third parties and integrated into our website. They may e.g. be web search services such as Algolia Place, Giphy, Programmable Search Engine or online services for weather data such as OpenWeather.

Why do we use these third parties?

With our website, we want to provide you with the best web offer in our industry. Websites have long been so much more than just a business card for companies. Instead, they are a place designed to help you find what you’re looking for. And in order to make our website even more interesting and helpful for you, we use various third-party services.

Which data is processed?

Whenever elements are integrated into our website, your IP address will be transmitted to the respective provider, where it will be stored and processed. This is

necessary to send the content to your browser which will then display it for you. Moreover, service providers may also use pixel tags or web beacons. These are small graphics on websites that can record a log file and create analyses of it. Providers can improve their own marketing measures with the information they receive this way. In addition to pixel tags, this information (e.g. which button you click or when you access which page) can also be stored in cookies. In addition to data analyses on your web behaviour, technical information such as your browser type or operating system may also be stored there. Some providers can also link the data they obtain to other internal services or to third-party providers. Each provider handles your data differently. Therefore, we recommend you carefully read the privacy policies of the respective services. We make every effort to only use services that operate very carefully in regards to data protection and privacy.

Duration of data processing

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

Legal Basis

If we ask for your consent and you agree to us using a service, this consent serves as the legal basis for the processing of your data (Article 6 (1) (a) GDPR). In addition to your consent, we have a legitimate interest in analysing the behaviour of our website visitors and thus technically and economically improving our offer. The legal basis for this is Article 6 (1) (f) GDPR (legitimate interests). However, we only use any tools if you have given your consent.


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

WooCommerce Privacy Policy


WooCommerce Privacy Policy Overview

 Affected parties: website visitors

 Purpose: service optimisation

 Processed data: data such as IP address, browser information, preset language settings as well as date and time of web access

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

 Storage period: Server log files, technical data and IP addresses will be erased after about 30 days

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

What is WooCommerce?

We have integrated the open-source shop system WooCommerce to our website as a plugin. This WooCommerce plugin is based on the content management system WordPress, which is a subsidiary company of Automattic Inc. (60 29th Street #343, San Francisco, CA 94110, USA). Through the implemented functions, data are stored and sent to Automattic Inc where they are processed. In this privacy policy we want to inform you on what data this is, how the network uses this data and how you can manage or prevent data retention.

WooCommerce is an online shop system that has been part of the WordPress directory since 2011 and was specially developed for WordPress websites. It is a customisable, open source eCommerce platform that is based on WordPress. It has been integrated into our website as a WordPress plugin.

Why do we use WooCommerce on our website?

We use this practical online shop system, to be able to offer you our physical or digital products or services in the best possible way on our website. The aim is to give you easy and easy access to our offer, so that you can quickly and easily navigate to the products you want. With WooCommerce we have found a good plugin that meets our requirements for an online shop.

What data is stored by WooCommerce?

Information that you actively enter to a text field in our online shop can be collected and stored by WooCommerce or Automattic. Hence, if you register with us or order a product, Automattic may collect, process and save this data. In addition to email address, name or address, this can also be your credit card or billing information. Subsequently, Automattic can also use this information for their own marketing campaigns.

There is also evidence that Automattic automatically collects information on you in so-called server log files:

- IP-address
- Browser information
- Pre-set language settings
- Date and time of the web access

Moreover, WooCommerce sets cookies in your browser and uses technologies such as pixel tags (web beacons), to for example clearly identify you as a user and to be able to offer interest-based advertising. WooCommerce uses several different cookies, which are placed depending on the user action. This means that if you for example add a product to the shopping cart, a cookie is set so that the product remains in the shopping cart when you leave our website and come back later.

Below we want to show you an example list of possible cookies that may be set by WooCommerce:

Name: woocommerce_items_in_cart

Value: 1

Purpose: This cookie helps WooCommerce to determine when the contents of the shopping cart change.

Expiry date: after end of session

Name: woocommerce_cart_hash

Value: 447c84f810834056ab37cfe5ed27f204312427560-7

Purpose: This cookie is also used to recognise and save the changes in your shopping cart.

Expiry date: after end of session

Name: wp_woocommerce_session_d9e29d251cf8a108a6482d9fe2ef34b6

Value:

1146%7C%7C1589034207%7C%7C95f8053ce0cea135bbce671043e740312427560-4aa

Purpose: This cookie contains a unique identifier for you to allow the shopping cart data to be found in the database.

Expiry date: after 2 days

How long and where is the data stored?

Unless there is a legal obligation to keep data for a longer period, WooCommerce will delete your data if it is no longer needed for the purposes it was saved for. Server log files for example, the technical data for your browser and your IP address will be deleted after about 30 days. This is how long Automattic use the data to analyse the traffic on their own websites (for example all WordPress websites) and to fix possible problems. The data is stored on Automattic's American servers.

How can I erase my data and prevent data retention?

You have the right to access your personal data anytime, as well as to object to it being used and processed. You can also lodge a complaint with a state supervisory authority anytime.

You can also manage, delete or deactivate cookies individually in your browser. However, please note that deactivated or deleted cookies may have a negative impact on the functions of our WooCommerce online shop. Depending on the browser you use, managing cookies differs slightly. Below you will find links to the instructions for the most common browsers:

[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](#)

Legal basis

If you have agreed to the use of WooCommerce, then your consent the legal basis for the corresponding data processing. According to **Art. 6 paragraph 1 lit. a (Consent)** your consent is the legal basis for the processing of personal data, as can occur when it is collected by WooCommerce.

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

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 details on WooCommerce's Privacy Policy and on which data is retained as well as how at <https://automattic.com/privacy/> and you can find more general information about WooCommerce at <https://woocommerce.com/>.

Zapier Privacy Policy

We use the automation software Zapier for our website. The service provider is the American company Zapier Inc, 548 Market Street 6241, San Francisco, CA 94104, USA.

Zapier processes data from you, among other things, in the USA. Zapier 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, Zapier 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, Zapier 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.

For more information on Zapier's standard contractual clauses, see <https://zapier.com/help/account/data-management/standard-contractual-clauses-at-zapier>.

You can learn more about the data processed using Zapier in the privacy policy at <https://zapier.com/privacy>.

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.