

Privacy Policy

We have written this privacy policy (version 20.02.2024) 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.

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.

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 (not yet established)) 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:

Ischia Consulting

Alessandro Ischia

Keinergasse 4, TOP 23+24, 1030 Vienna

e-Mail: office@ischiacon.com

Mobile. +43 699 11116559

Legal Notice: <https://ischia.consulting/legal-notice>

Storage Period

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

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

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

Rights in accordance with the General Data Protection Regulation

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

- According to Article 15 DSGVO, you have the right to information about whether we are processing data about you. If this is the case, you have the right to receive a copy of the data and to know the following information:
 - for what purpose we are processing;
 - the categories, i.e. the types of data that are processed;
 - who receives this data and if the data is transferred to third countries, how security can be guaranteed;
 - how long the data will be stored;
 - the existence of the right to rectification, erasure or restriction of processing and the right to object to processing;

- that you can lodge a complaint with a supervisory authority (links to these authorities can be found below);
 - the origin of the data if we have not collected it from you;
 - Whether profiling is carried out, i.e. whether data is automatically evaluated to arrive at a personal profile of you.
- You have a right to rectification of data according to Article 16 GDPR, which means that we must correct data if you find errors.
- You have the right to erasure (“right to be forgotten”) according to Article 17 GDPR, which specifically means that you may request the deletion of your data.
- According to Article 18 of the GDPR, you have the right to restriction of processing, which means that we may only store the data but not use it further.
- According to Article 20 of the GDPR, you have the right to data portability, which means that we will provide you with your data in a standard format upon request.
- According to Article 21 DSGVO, you have the right to object, which entails a change in processing after enforcement.
 - If the processing of your data is based on Article 6(1)(e) (public interest, exercise of official authority) or Article 6(1)(f) (legitimate interest), you may object to the processing. We will then check as soon as possible whether we can legally comply with this objection.
 - If data is used to conduct direct advertising, you may object to this type of data processing at any time. We may then no longer use your data for direct marketing.
 - If data is used to conduct profiling, you may object to this type of data processing at any time. We may no longer use your data for profiling thereafter.
- According to Article 22 of the GDPR, you may have the right not to be subject to a decision based solely on automated processing (for example, profiling).
- You have the right to lodge a complaint under Article 77 of the GDPR. This means that you can complain to the data protection authority at any time if you believe that the data processing of personal data violates the GDPR.

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

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

Austria Data protection authority

Manager: Mag. Dr. Andrea Jelinek

Address: Barichgasse 40-42, 1030 Wien

Phone number.: +43 1 52 152-0

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

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

Data transfer to third countries

We only transfer or process data to countries outside the EU (third countries) if you consent to this processing, if this is required by law or if it is contractually necessary. In any case, we generally only do so to the permitted extent. In most cases, your consent is the most important reason for data being processed in third countries. When personal data is being processed in third countries such as the USA, where many software manufacturers offer their services and have their servers located, your personal data may be processed and stored in unexpected ways.

We want to expressly point out, that according to the European Court of Justice, there is currently no adequate level of protection for data transfer to the USA. Data processing by US services (such as Google Analytics) may result in data processing and retention without the data having undergone anonymisation processes. Furthermore, US government authorities may be able to access individual data. The collected data may also get linked to data from other services of the same provider, should you have a user account with the respective provider. We try to use server locations within the EU, whenever this is offered and possible.

We will provide you with more details about data transfer to third countries in the appropriate sections of this privacy policy, whenever applicable.

Security of data processing operations

In order to protect personal data, we have implemented both technical and organisational measures. We encrypt or pseudonymise personal data wherever this

is possible. Thus, we make it as difficult as we can for third parties to extract personal information from our data.


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

TLS encryption with https

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.

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.

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: GA1.2.1326744211.152122504394-9

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=122504394>)
- 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.

Webhosting Other

Contact data for our Webhosting:

Godaddy

You can learn more about the data processing at this provider in their <https://www.godaddy.com/en-ie/legal/agreements/privacy-policy>.

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.

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, click behaviour and IP addresses. You can find more details on this in the privacy policy below.

Storage period: depending on the properties used

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

What is Google Analytics?

We use the tracking and analysis tool Google Analytics (GA) of the US-American company Google LLC (1600 Amphitheatre Parkway Mountain View, CA 94043, USA). Google Analytics collects data on your actions on our website. Whenever you click a link for example, this action is saved in a cookie and transferred to Google Analytics. With the help of reports which we receive from Google Analytics, we can adapt our website and our services better to your wishes. In the following, we will explain the tracking tool in more detail, and most of all, we will inform you what data is saved and how you can prevent this.

Google Analytics is a tracking tool with the purpose of conducting data traffic analysis of our website. For Google Analytics to work, there is a tracking code integrated to our website. Upon your visit to our website, this code records various actions you perform on your website. As soon as you leave our website, this data is sent to the Google Analytics server, where it is stored.

Google processes this data and we then receive reports on your user behaviour. These reports can be one of the following:

- Target audience reports: With the help of target audience reports we can get to know our users better and can therefore better understand who is interested in our service.
- Advertising reports: Through advertising reports we can analyse our online advertising better and hence improve it.
- Acquisition reports: Acquisition reports provide us helpful information on how we can get more people enthusiastic about our service.
- Behaviour reports: With these reports, we can find out how you interact with our website. By the means of behaviour reports, we can understand what path you go on our website and what links you click.
- Conversion reports: A conversion is the process of leading you to carry out a desired action due to a marketing message. An example of this would be transforming you from a mere website visitor into a buyer or a newsletter subscriber. Hence, with the help of these reports we can see in more detail, if our marketing measures are successful with you. Our aim is to increase our conversion rate.
- Real time reports: With the help of these reports we can see in real time, what happens on our website. It makes us for example see, we can see how many users are reading this text right now.

Why do we use Google Analytics on our website?

The objective of our website is clear: We want to offer you the best possible service. Google Analytics' statistics and data help us with reaching this goal.

Statistically evaluated data give us a clear picture of the strengths and weaknesses of our website. On the one hand, we can optimise our page in a way, that makes it easier to be found by interested people on Google. On the other hand, the data helps us to get a better understanding of you as our visitor. Therefore, we can very accurately find out what we must improve on our website, in order to offer you the best possible service. The analysis of that data also enables us to carry out our advertising and marketing measures in a more individual and more cost-effective way. After all, it only makes sense to show our products and services exclusively to people who are interested in them.

What data is stored by Google Analytics?

With the aid of a tracking code, Google Analytics creates a random, unique ID which is connected to your browser cookie. That way, Google Analytics recognises you as a new user. The next time you visit our site, you will be recognised as a “recurring” user. All data that is collected gets saved together with this very user ID. Only this is how it is made possible for us to evaluate and analyse pseudonymous user profiles.

To analyse our website with Google Analytics, a property ID must be inserted into the tracking code. The data is then stored in the corresponding property. Google Analytics 4-property is standard for every newly created property. An alternative however, is the Universal Analytics Property. Depending on the property that is being used, data are stored for different periods of time.

Your interactions on our website are measured by tags such as cookies and app instance IDs. Interactions are all kinds of actions that you perform on our website. If you are also using other Google systems (such as a Google Account), data generated by Google Analytics can be linked with third-party cookies. Google does not pass on any Google Analytics data, unless we as the website owners authorise it. In case it is required by law, exceptions can occur.

The following cookies are used by Google Analytics:

Name: _ga

Value: 2.1326744211.152122504394-5

Purpose: By default, analytics.js uses the cookie _ga, to save the user ID. It generally serves the purpose of differentiating between website visitors.

Expiration date: After 2 years

Name: _gid

Value: 2.1687193234.152122504394-1

Purpose: This cookie also serves the purpose of differentiating between website users

Expiration date: After 24 hours

Name: _gat_gtag_UA_<property-id>

Value: 1

Verwendungszweck: It is used for decreasing the demand rate. If Google Analytics is provided via Google Tag Manager, this cookie gets the name _dc_gtm_ <property-id>.

Expiration date: After 1 minute

Name: AMP_TOKEN

Value: No information

Purpose: This cookie has a token which is used to retrieve the user ID by the AMP Client ID Service. Other possible values suggest a logoff, a request or an error.

Expiration date: After 30 seconds up to one year

Name: __utma

Value: 1564498958.1564498958.1564498958.1

Purpose: With this cookie your behaviour on the website can be tracked and the site performance can be measured. The cookie is updated every time the information is sent to Google Analytics.

Expiration date: After 2 years

Name: __utmt

Value: 1

Purpose: Just like _gat_gtag_UA_<property-id> this cookie is used for keeping the requirement rate in check.

Expiration date: After 10 minutes

Name: __utmb

Value: 3.10.1564498958

Purpose: This cookie is used to determine new sessions. It is updated every time new data or information gets sent to Google Analytics.

Expiration date: After 30 minutes

Name: __utmc

Value: 167421564

Purpose: This cookie is used to determine new sessions for recurring visitors. It is therefore a session cookie, and only stays stored until you close the browser again.

Expiration date: After closing the browser

Name: __utmz

Value: m|utmcn=(referral)|utmcmd=referral|utmcct=

Purpose: This cookie is used to identify the source of the number of visitors to our website. This means, that the cookie stored information on where you came to our website from. This could be another site or an advertisement.

Expiration date: After 6 months

Name: __utmv

Value: No information

Purpose: The cookie is used to store custom user data. It gets updated whenever information is sent to Google Analytics.

Expiration date: After 2 years

Note: This list is by no means exhaustive, since Google are repeatedly changing the use of their cookies.

Below we will give you an overview of the most important data that can be evaluated by Google Analytics:

Heatmaps: Google creates so-called Heatmaps on. These Heatmaps make it possible to see the exact areas you click on, so we can get information on what routes you make on our website.

Session duration: Google calls the time you spend on our website without leaving it session duration. Whenever you are inactive for 20 minutes, the session ends automatically.

Bounce rate If you only look at one page of our website and then leave our website again, it is called a bounce.

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

IP-Address: The IP address is only shown in a shortened form, to make it impossible to clearly allocate it.

Location: Your approximate location and the country you are in can be defined by the IP address. This process is called IP location determination.

Technical information: Information about your browser type, your internet provider and your screen resolution are called technical information.

Source: Both, Google Analytics as well as ourselves, are interested what website or what advertisement led you to our site.

Further possibly stored data include contact data, potential reviews, playing media (e.g. when you play a video on our site), sharing of contents via social media or adding our site to your favourites. This list is not exhaustive and only serves as general guidance on Google Analytics' data retention.

How long and where is the data stored?

Google has servers across the globe. Most of them are in America and therefore your data is mainly saved on American servers. Here you can read detailed information on where Google's data centres are located: <https://www.google.com/about/datacenters/locations/?hl=en>

Your data is allocated to various physical data mediums. This has the advantage of allowing to retrieve the data faster, and of protecting it better from manipulation. Every Google data centre has respective emergency programs for your data. Hence, in case of a hardware failure at Google or a server error due to natural disasters, the risk for a service interruption stays relatively low.

The data retention period depends on the properties used. When using the newer Google Analytics 4-properties, the retention period of your user data is set to 14 months. For so-called event data, we have the option of choosing a retention period of either 2 months or 14 months.

Google Analytics has a 26 months standardised period of retaining your user data. After this time, your user data is deleted. However, we have the possibility to choose the retention period of user data ourselves. There are the following five options:

- Deletion after 14 months
- Deletion after 26 months

- Deletion after 38 months
- Deletion after 50 months
- No automatical deletion

Additionally, there is the option for data to be deleted only if you no longer visit our website within a period determined by us. In this case, the retention period will be reset every time you revisit our website within the specified period.

As soon as the chosen period is expired, the data is deleted once a month. This retention period applies to any of your data which is linked to cookies, user identification and advertisement IDs (e.g. cookies of the DoubleClick domain). Any report results are based on aggregated information and are stored independently of any user data. Aggregated information is a merge of individual data into a single and bigger unit.

How can I delete my data or prevent data retention?

Under the provisions of the European Union's data protection law, you have the right to obtain information on your data and to update, delete or restrict it. With the help of a browser add on that can deactivate Google Analytics' JavaScript (ga.js, analytics.js, dc.js), you can prevent Google Analytics from using your data. You can download this add on at <https://tools.google.com/dlpage/gaoptout?hl=en-GB>. Please consider that this add on can only deactivate any data collection by Google Analytics.

If you generally want to deactivate, delete or manage all cookies (independently of Google Analytics), you can use one of the guides that are available for any 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

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

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

Google 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 Google Analytics if you have given your consent.

Google 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.

Google 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 Google 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

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

We hope we could provide you with the most important information about data processing by Google Analytics. If you want to find out more on the tracking service, we recommend these two

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

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&%3Butm_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 progress 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.

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.

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 X, 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 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.

Facebook 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 Facebook 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 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 Login Privacy Policy

We integrated the convenient Facebook Login to our website. With it, you can easily log into our site with your Facebook account, without having to create a new user account. If you decide to register via the Facebook Login, you will be redirected to the social media network Facebook. There, you can log in with your Facebook user data. By using this method to log in, data on you and your user behaviour is stored and transmitted to Facebook.

To save the data, Facebook uses various cookies. In the following we will show you the most significant cookies that are placed in your browser or that already exist when you log into our site via the Facebook Login:

Name: fr

Value: 0jieyh4c2GnlufEJ9..Bde09j...1.0.Bde09j

Purpose: This cookie is used to make the social plugin function optimally on our website.

Expiry date: after 3 months

Name: datr

Value: 4Jh7XUA2122504394SEmPsSfzCOO4JFFI

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

Expiry date: after 2 years

Name: _js_datr

Value: deleted

Purpose: Facebook sets this session cookie for tracking purposes, even if you do not have a Facebook account or are logged out.

Expiry date: after the end of the session

Note: The cookies we stated are only a small range of the cookies which are available to Facebook. Other cookies include for example _fbp, sb or wd. It is not possible to disclose an exhaustive list, since Facebook have a multitude of cookies at their disposal which they use in variation.

On the one hand, Facebook Login enables a fast and easy registration process. On the other hand, it gives us the opportunity to share data with Facebook. In turn, we can customise our offer and advertising campaigns better to your needs and interests. The data we receive from Facebook by this means, is public data such as

- your Facebook name
- your profile picture
- your stored email address
- friends lists

- button clicks (e.g. “Like” button)
- date of birth
- language
- place of residence

In return, we provide Facebook with information about your activities on our website. These include information on the terminal device you used, which of our subpages you visit, or what products you have bought from us.

By using Facebook Login, you agree to the data processing. You can terminate this agreement anytime. If you want to learn more about Facebook’s data processing, we recommend you to read Facebook’s Data Policy at <https://www.facebook.com/policy.php>.

If you are registered with Facebook, you can change your advertisement settings anytime at https://www.facebook.com/ads/preferences/?entry_product=ad_settings_screen.

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: 0jieyh4122504394c2GnlufEJ9..Bde09j...1.0.Bde09j

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

Expiry date: after 3 months

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

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

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

If you are not a Facebook user, you can go

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

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

Gravatar Privacy Policy

Gravatar Privacy Policy Overview

? Affected parties: website visitors

? Purpose: optimising our service

? Processed data: includes your encrypted e-mail address, IP address and our server URL

More details can be found in the privacy policy below.

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

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

What is Gravatar?

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

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

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

Why do we use Gravatar on our website?

Anonymity on the internet is a popular topic. An avatar gives people that make posts or comments a face. Moreover, it makes it easier to be recognised on the web and to make oneself known. Many users enjoy the advantages of user pictures as they want

to appear on the web in a personal and authentic manner. Of course, we want to offer you the possibility to display your Gravatar also on our website. Furthermore, we also like to see faces of our commenting users. With the activated Gravatar function, we are expanding the service on our website. After all, we want you to feel comfortable on our website and enable you to receive an extensive and interesting offer.

What data is stored by Gravatar?

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

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

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

Name: gravatar

Value: 16b3191024acc05a238209d51ffcb92bdd710bd19122504394-7

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

Expiry date: after 50 years

Name: is-logged-in

Value: 1122504394-1

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

Expiry date: after 50 years

How long and where is the data retained?

Automattic deletes the collected data either if they are no longer used for their services, or if the company is not legally obliged to keep the data. Web server logs such as IP addresses, browser types and operating systems will be deleted after

about 30 days. Until deletion, Automattic use the data to analyse traffic on their own websites (for example all WordPress sites) and to fix potential problems. The data is also stored on Automattic's American servers.

How can I delete my data or prevent data retention?

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

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

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

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

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

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

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

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

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

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

You can find more details on the privacy policy and what data is collected by Gravatar at <https://automattic.com/privacy/> . Moreover, at <https://en.gravatar.com/> you can find general information on Gravatar.

Legal basis

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

communication with you or other customers and business partners. We only use the integrated social media elements if you have given your consent. Most social media platforms also place cookies in your browser to store data. We therefore recommend you to read our privacy policy about cookies and to carefully take a look at the privacy policy or the cookie policy of the respective service provider.

Gravatar processes data 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 the data processing.

Gravatar 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 transfers there (= Art. 46, paragraph 2 and 3 of the GDPR). These clauses oblige Gravatar to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses

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

You can find more details on the privacy policy as well as on what data is recorded by Gravatar and in what way at <https://automattic.com/privacy/>. Moreover, you can find general information about Gravatar at <http://de.gravatar.com/>.

Instagram Privacy Policy

Instagram Privacy Policy Overview

? Affected parties: website visitors

? Purpose: optimising our service

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

More details can be found in the privacy policy below.

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

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

What is Instagram?

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

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

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

Why do we use Instagram on our website?

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

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

What data is stored by Instagram?

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

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

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

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

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

The following cookies were used in our test:

Name: csrftoken

Value: ""

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

Expiry date: after one year

Name: mid

Value: ""

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

Expiry date: after end of session

Name: fbsr_122504394124024

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_UjKvXgYe122504394"

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 and Facebook also process 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 transfer to the USA. This can be associated with various risks to the legality and security of data processing.

As a basis for data processing by recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway and especially in the USA) or data transfers there, Facebook uses standard contractual clauses approved by the EU Commission (= Art. 46, paragraphs 2 and 3 of the GDPR). These clauses oblige Facebook 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 give you the most important information about data processing by Instagram. On <https://help.instagram.com/519522125107875> you can take a closer look at Instagram's data guidelines.

LinkedIn Privacy Policy

LinkedIn Privacy Policy Overview

? Affected parties: website visitors

? Purpose: optimisation of our service

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

More details can be found in the privacy policy below.

? Storage period: the data is generally deleted within 30 days

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

What is LinkedIn?

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

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

LinkedIn is the largest social network for business contacts. In contrast to e.g. Facebook, LinkedIn focuses exclusively on establishing business connections. Therefore, companies can present services and products on the platform and

establish business relationships. Many people also use LinkedIn to find a job or to find suitable employees for their own company. In Germany alone, the network has over 11 million members. In Austria there are about 1.3 million.

Why do we use LinkedIn on our website?

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

What data are stored by LinkedIn?

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

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

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

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

Name: bcookie

Value: =2&34aab2aa-2ae1-4d2a-8baf-c2e2d7235c16122504394-

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=AQF6KNnJ0G122504394...

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:1225043942900777718326218137

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.

Pinterest Privacy Policy

Pinterest Privacy Policy Overview

? Affected parties: website visitors

? Purpose: service optimisation

? Processed data: data such as data on user behaviour, device information, IP address and search terms.

You can find more details in the Privacy Policy below.

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

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

What is Pinterest?

On our website we use buttons and widgets by the social media network Pinterest, of the company Pinterest Inc., 808 Brannan Street, San Francisco, CA 94103, USA. For the European area, the entity responsible for all aspects of privacy is the Irish company Pinterest Europe Ltd. (Palmerston House, 2nd Floor, Fenian Street, Dublin 2, Ireland).

Pinterest is a social network that specialises in graphic representations and photographs. Its name is made up of the two words “pin” and “interest”. Users can exchange ideas about various hobbies and interests via Pinterest and view profiles with pictures openly or in defined groups.

Why do we use Pinterest?

The social media platform Pinterest has been around for a few years now and is still one of the most visited and valued platforms. Pinterest is particularly suitable for our industry because the platform is primarily known for beautiful and interesting images. That is why we are of course also represented on Pinterest and want to put our content in the limelight in places other than our website. The collected data may also be used for advertising purposes, so we can show advertising messages to precisely those people who are interested in our services or products.

Which data are processed by Pinterest?

Pinterest may store so-called log data. This includes information about your browser, IP address, our website address and the your activities on it (e.g. when you click the save or pin button), along with your search history, the date and time of the request as well as cookie and device data. If you interact with an embedded Pinterest function, cookies that store various data may also be set in your browser. Most of the above-mentioned log data, as well as preset language settings and clickstream data are stored in cookies. Pinterest considers clickstream data as information about your website behaviour.

If you have a Pinterest account yourself and are logged in, the data collected via our site may be linked to your account and used for advertising purposes. If you interact with our integrated Pinterest functions, you will usually be redirected to the Pinterest page. Below you will see an exemplary selection of cookies that can then be placed in your browser.

Name: _auth

Value: 0

Purpose: The cookie is used for authentication. A value such as your “username” can

be stored in it, for example.

Expiry date: after one year

Name: _pinterest_referrer

Value: 1

Purpose: This cookie stores the information that you came to Pinterest via our website. Thus, the URL of our website is retained.

Expiry date: after the session ends

Name: _pinterest_sess

Value: ... 9HRHZvVE0rQIUxdG89

Purpose: This cookie is used to log into Pinterest and it contains user IDs, authentication tokens and time stamps.

Expiry date: after one year

Name: _routing_id

Value: "8d850ddd-4fb8-499c-961c-77efae9d4065 122504394 -8"

Purpose: This cookie contains an assigned value that is used to identify a specific routing destination.

Expiry date: after one day

Name: cm_sub

Value: denied

Purpose: This cookie stores user IDs and time stamps.

Expiry date: after one year

Name: csrftoken

Value: 9e49145c82a93d34fd933b0fd8446165 122504394-1

Purpose: This cookie is most certainly placed for security reasons in order to prevent falsified inquiries. However, we could not find more precise information.

Expiry date: after one year

Name: sessionFunnelEventLogged

Value: 1

Purpose: We have not yet been able to find out more information about this cookie.

Expiry date: after one day

How long and where are the data retained?

Pinterest basically stores the collected data until it is no longer needed for the company's purposes. As soon as the storage of this data is no longer necessary, e.g. for the compliance with legal regulations, the data is either erased or anonymised so you can no longer be identified as a person. The data may also be stored on American servers.

Right to object

You also have the right and the option to revoke your consent to the use of cookies or third-party providers such as Pinterest 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 retention by cookies by managing, deactivating or erasing cookies in your browser.

Since cookies can be used with embedded Pinterest elements, we also recommend you to read our general privacy policy on cookies. To find out which of your data are stored and processed, you should 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 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**) in maintaining fast and good communication with you or other customers and business partners. Nevertheless, we only use the tool if you have given your consent to it. Most social media platforms also place 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.

Pinterest 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.

Pinterest 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 Pinterest 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 hope we could provide you with the most important information about data processing by Pinterest. You can find out more about Pinterest's privacy guidelines at <https://policy.pinterest.com/en-gb/privacy-policy>.

TikTok Privacy Policy

We also use TikTok, which is a social media and video channel. The provider of this service is the Chinese company Beijing Bytedance Technology Ltd. The responsible entity for the European area is the Irish company TikTok Technology Limited, 10 Earlsfort Terrace, Dublin, D02 T380, Ireland.

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

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

You can find out more about the data processed by TikTok in the Privacy Policy at <https://www.tiktok.com/legal/privacy-policy?lang=en#privacy-eea>.

X Privacy Policy

X 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: X deletes collected data of other websites after 30 days at most

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

What is X?

We have incorporated X functions on our website. These are, for example, embedded tweets, timelines, buttons or hashtags. X is a short message service and social media platform from the firm X Inc., One Cumberland Place, Fenian Street, Dublin 2 D02 AX07, Ireland.

To our knowledge, in the European Economic Area and Switzerland, a mere integration of the X function does not transfer any personal data or data about your web activities to X. Only when you interact with the X functions, such as by clicking a button, data could be sent to X and get saved as well as processed there. We have no influence on this processing of data and do not bear any responsibility for it. Within this privacy statement, we want to give you an overview of what data X stores, what X does with this data and how you can largely protect yourself from data transmission.

For some, X is a news service, for others, a social media platform, and for others still it is a microblogging service. All these terms are justified and mean pretty much the same.

Both individuals as well as companies use X for communicating with interested people via short messages. X only allows 280 characters per message. These messages are called “tweets”. In contrast to Facebook, for example, the service does not focus on the expansion of a network of “friends”, but strives to be regarded as an open, worldwide news platform. On X you can also have an anonymous account and tweets can be deleted by both, either the company or the users themselves.

Why do we use X on our website?

Like many other websites and companies, we try to use different channels for offering our services and communicating with our customers. X is a truly useful “small” news service, which is why it has grown dear to us. We regularly tweet or retweet exciting, funny or interesting content. We understand that you do not have the time to follow every channel after channel, as you surely have enough other things to do. That is why we also have integrated X functions to our website. That way, you can experience our X activities “on site” or come to our X page via a direct link. With the integration, we want to strengthen the service and user-friendliness on our website.

What data is stored by X?

You will find integrated X functions on some of our subpages. If you interact with X content, such as by clicking a button, X may collect and save data. This can happen even if you don’t have a X account yourself. X calls this data “log data”. It includes demographic data, browser cookie IDs, your smartphone’s ID, hashed email addresses, and information on which pages you have visited on X and what actions you have taken there. Of course, X stores more data if you have a X account and are logged in. This retention is usually done via cookies. Cookies are small text files that are usually set in your browser and transmit various information to X.

We will now show you which cookies are placed if you are not logged in to X but visit a website with built-in X functions. Please consider this list as an example. We do not

claim for this list to be extensive, since the array of cookies always changes and depends on your individual actions with X content.

The following cookies have been used in our test:

Name: personalization_id

Value: "v1_cSJIsogU51SeE122504394"

Purpose: This cookie stores information on how you use the website and what ad may have led you to X.

Expiry date: after 2 years

Name: lang

Value: en

Purpose: This cookie stores your default or preferred language.

Expiry date: after end of session

Name: guest_id

Value: 122504394v1%3A157132626

Purpose: This cookie is set to identify you as a guest.

Expiry date: after 2 years

Name: fm

Value: 0

Purpose: Unfortunately, we could not find out the purpose of this cookie.

Expiry date: after end of session

Name: external_referer

Value: 1225043942beTA0sf5lkMrlGt

Purpose: This cookie collects anonymous data, such as how often you visit X and how long you visit X.

Expiry date: after 6 days

Name: eu_cn

Value: 1

Purpose: This cookie stores user activity and is used for X's various advertising purposes.

Expiry date: after one year

Name: ct0

Value: c1179f07163a365d2ed7aad84c99d966

Purpose: Unfortunately we could not find any information on this cookie.

Expiry date: after 6 hours

Name: _X_sess

Value: 53D%253D-dd0248122504394-

Purpose: With this cookie you can use functions within X's website.

Expiry date: after end of session

Note: X also works with third parties. Therefore, we have recognized the three Google Analytics cookies _ga, _gat, _gid in our test.

On the one hand, X uses the collected data for gaining better understand on user behaviour, and thus to improve their own services and advertising offers. On the other hand, the data are also used for internal security measures.

How long and where are the data stored?

When X collects data from other websites, after a maximum of 30 days, they will be deleted, summarised or otherwise concealed. X's servers are in various server centres in the United States. Accordingly, it can be assumed that the gathered data will be collected and stored in America. In our research we could not clearly determine whether X also owns servers in Europe. Generally, X may keep collected data stored until either the data are no longer useful to the company, until you delete the data or until a potential legal deletion period has been reached.

How can I erase my data or prevent data retention?

In their Privacy Policy, X repeatedly emphasise that they do not save data from external website visits, provided you or your browser are in the European Economic Area or Switzerland. However, if you interact directly with X, the company will of course store your data.

If you have a X account, you can manage your data by clicking on "More" under the "Profile" button. Then click on "Settings and privacy". Here you can manage data processing individually.

If you do not have a X account, you can go to [X.com](https://x.com) and click "Settings". At "Personalisation and data" you can manage data that is collected on you.

As mentioned above, most data are stored via cookies, which you can manage, deactivate or delete in your browser. Please note that when changing cookie settings in your browser, the edits will only affect that very browser. This means that if you use another browser in the future, you will have to manage your cookie settings there again. In the following you will find instructions for managing cookies in the most popular 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

You can also set your browser to notify you about each individual cookie. This lets you decide individually whether you want to allow or deny a cookie.

X also uses the data for personalised advertising in-and outside of X. You can switch off personalised advertising in the settings under "Personalization and data". If you use X on a browser, you can deactivate personalised advertising at <http://optout.aboutads.info/?c=2&lang=EN>.

Legal basis

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

X 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.

X uses standard contractual clauses, which are 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 transfers there (= Art. 46, paragraphs 2 and 3 of the GDPR). These clauses oblige ShareThis 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 hope we could give you a basic overview of X's data processing. We do not receive any data from X and are not responsible for what X does with your data. If you have any further questions on this topic, we recommend you to read X's privacy statement at <https://X.com/en/privacy>.

Blogs and Publication

Media Introduction

Blogs and Publication Media Privacy Policy Overview

? Affected parties: website visitors

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

? Data processed: Data such as contact details, IP address and published content.

More details can be found under the tools used.

? Storage duration: depending on the tools used

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

What are blogs and publishing media?

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

Why do we use blogs and publication media?

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

Which data is processed?

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

Duration of data processing

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

Right to object

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

Since cookies can also be used in publication media, we also recommend you read our general privacy policy on cookies. To find out exactly which of your data is stored and processed, you should read the privacy policies of the respective tools.

Legal Basis

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

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

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

Blog Posts and Comment Functions Privacy Policy

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

WordPress-Emojis Privacy Policy

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

Automattic 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.

Automattic 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, paragraphs 2 and 3 of the GDPR). These clauses oblige Automattic to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses here: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

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

Content Delivery Networks

Content Delivery Networks Privacy Policy Overview

? Affected parties: website visitors

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

? Processed data: data such as your IP address

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

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

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

What is a Content Delivery Network?

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

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

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

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

Which data are processed?

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

Right to object

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

Legal basis

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

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

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

Cloudflare Privacy Policy

Cloudflare Privacy Policy Overview

? Affected parties: website visitors

? Purpose: service performance optimisation (to accelerate website loading times)

? Processed data: data such as IP address, contact and protocol information, security fingerprints and website performance data

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

? Storage duration: most of the data is stored for less than 24 hours

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

What is Cloudflare?

We use Cloudflare by the company Cloudflare, Inc. (101 Townsend St., San Francisco, CA 94107, USA) on our website to enhance its speed and security. For this, Cloudflare uses cookies and processes user data. Cloudflare, Inc. is an American company that offers a content delivery network and various security services. These services take place between the user and our hosting provider. In the following, we will try to explain in detail what all this means.

A content delivery network (CDN), as provided by Cloudflare, is nothing more than a network of servers that are connected to each other. Cloudflare has deployed servers around the world, which ensure websites can appear on your screen faster. Simply put, Cloudflare makes copies of our website and places them on its own servers. Thus, when you visit our website, a load distribution system ensures that the main part of our website is delivered by a server that can display our website to you as

quickly as possible. The CDN significantly shortens the route of the transmitted data to your browser. Thus, Cloudflare does not only deliver our website's content from our hosting server, but from servers from all over the world. Cloudflare is particularly helpful for users from abroad, since pages can be delivered from a nearby server. In addition to the fast delivery of websites, Cloudflare also offers various security services, such as DDoS protection, or the web application firewall.

Why do we use Cloudflare on our website?

Of course, we want our website to offer you the best possible service. Cloudflare helps us make our website faster and more secure. Cloudflare offers us web optimisations as well as security services such as DDoS protection and a web firewall. Moreover, this includes a [Reverse-Proxy](#) and the content distribution network (CDN). Cloudflare blocks threats and limits abusive bots as well as crawlers that waste our bandwidth and server resources. By storing our website in local data centres and blocking spam software, Cloudflare enables us to reduce our bandwidth usage by about 60%. Furthermore, the provision of content through a data centre near you and certain web optimizations carried out there, cut the average loading time of a website in about half. According to Cloudflare, the setting "I'm Under Attack Mode" can be used to mitigate further attacks by displaying a JavaScript calculation task that must be solved before a user can access a website. Overall, this makes our website significantly more powerful and less susceptible to spam or other attacks.

What data is stored by Cloudflare?

Cloudflare generally only transmits data that is controlled by website operators. Therefore, Cloudflare does not determine the content, but the website operator themselves does. Additionally, Cloudflare may collect certain information about the use of our website and may process data we send or data which Cloudflare has received certain instructions for. Mostly, Cloudflare receives data such as IP addresses, contacts and protocol information, security fingerprints and websites' performance data. Log data for example helps Cloudflare identify new threats. That way, Cloudflare can ensure a high level of security for our website. As part of their services, Cloudflare process this data in compliance with the applicable laws. Of course, this also includes the compliance with the General Data Protection Regulation (GDPR).

Furthermore, Cloudflare uses a cookie for security reasons. The cookie (`__cfduid`) is used to identify individual users behind a shared IP address, and to apply security settings for each individual user. The cookie is very useful, if you e.g. use our website from a restaurant where several infected computers are located. However, if your

computer is trustworthy, we can recognise that with the cookie. Hence, you will be able to freely and carelessly surf our website, despite the infected PCs in your area. Another point that is important to know, is that this cookie does not store any personal data. The cookie is essential for Cloudflare's security functions and cannot be deactivated.

Cookies by Cloudflare

Name: __cfduid

Value: d798bf7df9c1ad5b7583eda5cc5e78122504394-3

Purpose: Security settings for each individual visitor

Expiry date: after one year

Cloudflare also works with third party providers. They may however only process personal data after the instruction of Cloudflare and in accordance with the data protection guidelines and other confidentiality and security measures. Without explicit consent from us, Cloudflare will not pass on any personal data.

How long and where is the data stored?

Cloudflare stores your information primarily in the United States and the European Economic Area. Cloudflare can transfer and access the information described above, from all over the world. In general, Cloudflare stores domains' user-level data with the Free, Pro and Business versions for less than 24 hours. For enterprise domains that have activated Cloudflare Logs (previously called Enterprise LogShare or ELS), data can be stored for up to 7 days. However, if IP addresses trigger security warnings in Cloudflare, there may be exceptions to the storage period mentioned above.

How can I erase my data or prevent data retention?

Cloudflare only keeps data logs for as long as necessary and in most cases deletes the data within 24 hours. Cloudflare also does not store any personal data, such as your IP address. However, there is information that Cloudflare store indefinitely as part of their permanent logs. This is done to improve the overall performance of Cloudflare Resolver and to identify potential security risks. You can find out exactly which permanent logs are saved

at <https://developers.cloudflare.com/1.1.1.1/commitment-to-privacy/privacy-policy/privacy-policy/>. All data Cloudflare collects (temporarily or permanently) is cleared of all personal data. Cloudflare also anonymise all permanent logs.

In their privacy policy, Cloudflare state that they are not responsible for the content you receive. For example, if you ask Cloudflare whether you can update or delete content, Cloudflare will always refer to us as the website operator. You can also completely prevent the collection and processing of your data by Cloudflare, when you deactivate the execution of script-code in your browser, or if you integrate a script blocker to your browser.

Legal basis

If you have consented to the use of Cloudflare, your consent is 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 Cloudflare.

We also have a legitimate interest in using Cloudflare 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 Cloudflare if you have given your consent to it.

Cloudflare 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.

Cloudflare 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 Cloudflare to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses here: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

You can find more information about data protection at Cloudflare at <https://www.cloudflare.com/en-gb/privacypolicy/>.

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).

BorlabsCookie Privacy Policy

On our website we use BorlabsCookie, which is one of the tools that store your consent to cookies. The provider of this service is the German company Borlabs – Benjamin A. Bornschein, Rübenkamp 32, 22305 Hamburg, Germany. You can find out more about the data that is processed by the use of BorlabsCookie in their Privacy Policy at <https://borlabs.io/privacy/>.

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.

PayPal Privacy Policy

On our website we use the online payment service PayPal. The provider of this service is the American company PayPal Inc. The responsible entity for the European region is the company PayPal Europe (S.à r.l. et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxembourg).

PayPal 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.

PayPal 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 PayPal to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses

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

You can find out more about the data processed by using PayPal in the Privacy Policy at <https://www.paypal.com/webapps/mpp/ua/privacy-full>.

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-e05f1779e84e040456122504394-5

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-a7419a5b8819875de9122504394-1

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 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.

Stripe 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 Stripe 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 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/at/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-CV6ojl5Y122504394-1

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_INFO01_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: zILlvClZSkqGsSwl/AU1aZl6HY7122504394-

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: AcRwpgUik9Dveht0l

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/AnUdDUlsJ9iJz2vdM

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

Expiry date: after 2 years

Name: SID

Value: oQfNKjAsl122504394-

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.

YouTube 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 the data processing.

YouTube uses standard contractual clauses approved by the EU Commission (= Art. 46, paragraphs 2 and 3 of the GDPR) as basis for data processing by recipients based in third countries (which are outside the European Union, Iceland, Liechtenstein and Norway) or for data transfer there. These clauses oblige YouTube 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

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>.

Video Conferencing & Streaming

Video Conferencing & Streaming Privacy Policy Overview

? Affected parties: users of our video conferencing or streaming tools

? Purpose: communication and presentation of content

? Processed data: Access statistics such as your name, address, contact details, email address, telephone number or IP address. You can find more details on this directly at the video

conference or streaming tool that is being used.

? Storage duration: depending on the video conferencing or streaming tool

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

What are video conferences & streamings?

We use software programs that enable us to hold video conferences, online meetings, webinars and to utilise display sharing and/or streaming. In a video conference or a streaming, information is transmitted simultaneously via sound and moving images. With such video conference or streaming tools, we can communicate quickly and easily with customers, business partners, clients and employees via the Internet. Of course, when selecting the service provider, we consider the given legal framework.

Generally, third-party providers can process data as soon as you interact with the software program. Third-party video conference providers or streaming solutions use your data and metadata for different purposes. The data helps to e.g. make the tool more secure and to improve the service. Most of the time, the data may also be used for the respective third-party provider's own marketing purposes.

Why do we use video conferencing & streaming on our website?

We want to communicate digitally, quickly, easily and securely with you, our customers and our business partners. This works best with video conferencing solutions that are very easy to use. Most tools also work directly in your browser and with just a few clicks you can get right to your video meeting. The tools also offer helpful additional features such as chat and screen sharing functions or the possibility of sharing content between meeting participants.

Which data are processed?

If you join our video conference or streaming, your data will also be processed and stored on the servers of the respective service provider.

The exact data that gets stored depends on the respective software. Each provider stores and processes data differently. Generally, however, most providers store your name, address, contact details such as your email address or telephone number and your IP address. Information about the device you are using may also get stored, along with usage data, such as which websites you visit, when you visit a website or which buttons you click. Data that is shared within the video conference (photos, videos, texts) may also be retained.

Duration of data processing

Below we will inform you about the duration of the data processing of the service that is being used, provided we have further information on this. In general, we only process personal data for as long as is absolutely necessary to provide our services and products. Moreover, it is possible that the provider may store your data according to their own requirements, which we have no influence on.

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 responsible for the respective video conferencing or streaming tool. You can find contact details either in our specific privacy policy or on the website of the relevant provider.

In your browser you can erase, deactivate or manage cookies that providers use for their functions. This works slightly different, depending on which browser you are using. Please note, however, that functions may not keep working as usual after doing so.

Legal basis

If you have consented to the processing and storage of your data by the respective video or streaming solution, this consent is the legal basis for data processing (**Art. 6 para. 1 lit. a GDPR**). We may also offer a video conference as part of our services, if there has been a contractual agreement with you in advance (**Art. 6 para. 1 lit. b 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, provided you have priorly given consent. Most video or streaming solutions 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.

Provided it is available, you can find information on special video conference and streaming solutions in the following sections.

WebinarJam Privacy Policy

We use the web conference provider WebinarJam for our website. The service provider is the American company Genesis Digital LLC, 4730 S. Fort Apache Rd. Suite 300, Las Vegas, NV 89147-7947, USA.

WebinarJam 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.

WebinarJam 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, WebinarJam 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 the Data Processing Addendum which corresponds to the Standard Contractual Clauses at <https://home.webinarjam.com/dpa>.

To learn more about the data processed through the use of WebinarJam, see their privacy policy at <https://home.webinarjam.com/privacypolicy>.

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.

Google Fonts Privacy Policy

Google Fonts Privacy Policy Overview

? Affected parties: website visitors

? Purpose: service optimisation

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

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

? Storage period: Google stores font files for one year

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

What are Google Fonts?

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

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

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

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

Why do we use Google Fonts on our website?

With Google Fonts we can use different fonts on our website and do not have to upload them to our own server. Google Fonts is an important element which helps to keep the quality of our website high. All Google fonts are automatically optimised for the web, which saves data volume and is an advantage especially for the use of mobile terminal devices. When you use our website, the low data size provides fast loading times. Moreover, Google Fonts are secure Web Fonts. Various image synthesis systems (rendering) can lead to errors in different browsers, operating systems and mobile terminal devices. These errors could optically distort parts of texts or entire websites. Due to the fast Content Delivery Network (CDN) there are no cross-platform issues with Google Fonts. All common browsers (Google Chrome, Mozilla Firefox, Apple Safari, Opera) are supported by Google Fonts, and it reliably operates on most modern mobile operating systems, including Android 2.2+ and iOS 4.2+ (iPhone, iPad, iPod). We also use Google Fonts for presenting our entire online service as pleasantly and as uniformly as possible.

Which data is stored by Google?

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

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

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

How long and where is the data stored?

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

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

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

The data Google stores for either a day or a year cannot be deleted easily. Upon opening the page this data is automatically transmitted to Google. In order to clear the data ahead of time, you have to contact Google's support at <https://support.google.com/?hl=en-GB&tid=122504394>. 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=122504394>. 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 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.

Google 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 Google to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses

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

You can find 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>.

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=h26c1Ktha7fCQTx8rXgLyATyITJ122504394-5

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 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.

Google 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 Google 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

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

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

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>.

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: 447c84f810834056ab37cfe5ed27f204122504394-7

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%7C95f8053ce0cea135bbce671043e740122504394-4aa

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.

WooCommerce 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.

WooCommerce 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 WooCommerce to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses here: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

You can find 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/>.

Explanation of the terminology used

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

Processor

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Consent

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Data concerning health

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Personal Data

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

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

According to the European Court of Justice (ECJ), your **IP address is also personal data**. IT experts can use your IP address to determine at least the approximate location of your device and subsequently your location as the connection owner. Therefore, storing an IP address also requires a legal basis within the scope of the

GDPR. There are also so-called “**special categories**” of personal data, which are particularly worthy of protection. These include:

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

Profiling

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Controller

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

*“**controller**” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the*

purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

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

Processing

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

All texts are copyrighted.