Data protection

Table of contents

- Introduction and overview
- scope of application
- Legal basis
- Contact details of the person responsible
- Storage period
- right loud General Data Protection Regulation
- Data transfer to third countries
- Security of data processing
- communication
- Order processing agreement (AVV)
- Cookies
- Web hosting introduction
- Web Analytics Introduction
- Messenger & Communication Introduction
- Social media introduction
- Online marketing introduction
- Web design Introduction
- Miscellaneous Introduction
- Explanation used Terms
- Final word

Introduction and overview

We have written this data protection declaration (version 03/21/2024-112750514) in order to explain to you, in accordance with the requirements of the General Data Protection Regulation (EU) 2016/679 and applicable national laws, which personal data (data for short) we as the controller - and that of 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 understood as gender-neutral.
In short: We inform you comprehensively about the data we process about you.

Privacy policies usually sound very technical and use legal terms. This data protection declaration, however, is intended to describe the most important things to you as simply and transparently as possible. To the extent that it promotes transparency, technical **terms are explained in a reader-friendly manner** , links to further information are provided and **graphics** are used.

We thereby inform you in clear and simple language that we only process personal data as part of our business activities if there is a corresponding legal basis. This is certainly not possible if you make as brief, unclear and legal-technical statements as possible, as are often standard on the Internet when it comes to data protection. I hope you find the following explanations interesting and informative and perhaps there is one or two pieces of information that you didn't know before.
If you still have questions, we would like to ask you to contact the responsible body named below or in the legal notice, follow the existing links and look at further information on third-party sites. You can of course also find our contact details in the legal notice.

scope of application

This data protection declaration applies to all personal data processed by us in the company and to all personal data that companies commissioned by us (contract processors) process. By personal data we mean information within the meaning of Article 4 No. 1 GDPR such as a person's name, email address and postal address. The processing of personal data ensures that we can offer and bill our services and products, whether online or offline. The scope this Data protection includes :

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

In short: The data protection declaration applies to all areas in which personal data is processed in a structured manner within the company via the channels mentioned. If we enter into legal relationships with you outside of these channels, we will inform you separately if necessary.

Legal basis

In the following data protection declaration we provide you with transparent information about the legal principles and regulations, i.e. the legal bases of the General Data Protection Regulation, which enable us to process personal data.
As far as EU law is concerned, we refer to REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 27, 2016.
You can of course access this EU General Data Protection Regulation online

on EUR-Lex, the access to the EU -Law, read at https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32016R0679 .

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

1. **Consent** (Article 6 paragraph 1 lit. a GDPR): You have given us your consent to process data for a specific purpose. An example would be saving the data you entered on a contact form.
2. **Contract** (Article 6 paragraph 1 lit. b GDPR): In order to fulfill a contract or pre-contractual obligations with you, we process your data. For example, if we conclude a purchase contract with you, we need personal information in advance.
3. **Legal obligation** (Article 6 paragraph 1 lit. c GDPR): If we are subject to a legal obligation, we process your data. For example, we are legally obliged to keep invoices for accounting purposes. This usually contain personal information Data .
4. **Legitimate interests** (Article 6 paragraph 1 lit. f GDPR): In the case of legitimate interests that do not restrict your fundamental rights, we reserve the right to process personal data. For example, we need to process certain data in order to operate our website securely and economically efficiently. This processing is thus a legitimate interest .

Other conditions such as the perception of recordings in the public interest and the exercise of public authority as well as the protection of vital interests generally do not apply to us. If such a legal basis is relevant, it will be shown in the appropriate place.

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

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

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

Contact details of the person responsible

If you have any questions about data protection or the processing of personal data, you will find the contact details of the responsible person or body below:
Elektro JoDa GmbHJohannes StockingerPanoramaweg 11 9112 Griffen, AustriaAuthorized representative: Daniel MühlakEmail: office@joda.gmbh Telephone: +4369917454602

Storage period

Our general criterion is that we only store personal data for as long as is absolutely necessary to provide our services and products. This means that we delete personal data as soon as the reason for data processing no longer exists. In some cases, we are legally obliged to store certain data even after the original purpose has ceased, for example for accounting purposes.

If you wish to have your data deleted or revoke your consent to data processing, the data will be deleted as quickly as possible and unless there is an obligation to store it.

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

Rights under the General Data Protection Regulation

In accordance with Articles 13, 14 GDPR, we inform you of the following rights to which you are entitled so that data is processed fairly and transparently:

- According to Article 15 GDPR, you have a right to information as to whether we are processing your data. 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 carry out the processing;
    - the categories, i.e. the types of data, that are processed;
    - who receives this data and, if the data is transferred to third countries, how security can be guaranteed;
    - how long the data is stored;
    - the existence of the right to rectification, deletion or restriction of processing and the right to object to processing;

    - that you can complain to a supervisory authority (links to these authorities can be found below);
    - the origin of the data if we did not collect it from you;
    - whether profiling is carried out, i.e. whether data is automatically evaluated in order to create a personal profile for you.
- According to Article 16 GDPR, you have the right to rectification of data, which means that we must correct data if you find errors.
- According to Article 17 GDPR, you have the right to deletion ("right to be forgotten"), which specifically means that you can request the deletion of your data.
- According to Article 18 GDPR, you have the right to restrict processing, which means that we are only allowed to store the data but not use it any further.
- According to Article 20 GDPR, you have the right to data portability, which means that upon request we will provide you with your data in a common format.
- According to Article 21 GDPR, you have a right to object, which, once enforced, will result in a change to the processing.
    - If the processing of your data is based on Article 6 Paragraph 1 Letter e (public interest, exercise of official authority) or Article 6 Paragraph 1 Letter f (legitimate interest), you can object to the processing. We will then check as quickly as possible whether we can legally comply with this objection.
    - If data is used to conduct direct advertising, you can object to this type of data processing at any time. We may then no longer use your data for direct marketing.
    - If data is used to carry out profiling, you can object to this type of data processing at any time. We are then no longer allowed to use your data for profiling.
- According to Article 22 GDPR, you may have the right not to be subject to a decision based solely on automated processing (e.g. profiling).
- According to Article 77 GDPR, you have the right to lodge a complaint. This means that you can complain to the data protection authority at any time if you believe that the processing of personal data violates the GDPR.

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

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 you can find at https://www.dsb.gv.at/ . In Germany there is a data protection officer for each federal state. For more information, you can contact the Federal Commissioner for Data Protection and Freedom of Information (BfDI) . The following local data protection authority is responsible for our company:

Austria data protection authority

Head: Mag. Dr. Andrea Jelinek
Address: Barichgasse 40-42, 1030 Vienna
Telephone number: +43 1 52 152-0
Email address: dsb@dsb.gv.at
Website: https://www.dsb.gv.at/

Data transfer to third countries

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

We expressly point out that, in the opinion of the European Court of Justice, there is currently only an adequate level of protection for data transfer to the USA if a US company that processes personal data of EU citizens in the USA is an active participant in the EU-US Data Privacy Frameworks is. You can find more information about this at: https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en

Data processing by US services that are not active participants in the EU-US Data Privacy Framework may result in data not being processed and stored anonymously. Furthermore, US government authorities may have access to individual data. It can also happen that collected data is linked to data from

other services from the same provider, provided you have a corresponding user account. If possible, we try to use server locations within the EU, if this is offered.
We will inform you in more detail about data transfer to third countries in the appropriate places in this data protection declaration, if this applies.

Security of data processing

To protect personal data, we have implemented both technical and organizational measures. Where possible, we encrypt or pseudonymize personal data. In doing so, we make it as difficult as possible for third parties to infer personal information from our data.

Art. 25 GDPR speaks here of “data protection through technology design and through data protection-friendly default settings” and means that one always thinks about security and the corresponding security when it comes to both software (e.g. forms) and hardware (e.g. access to the server room). takes measures. Below we will go into specific measures if necessary.

communication

Communication summary
Those affected: Everyone who communicates with us by phone, email or online form
Processed data: e.g. E.g. telephone number, name, email address, entered form data. You can find more details about the type of contact used
Purpose: Handling communication with customers, business partners, etc.
Storage period: Duration of the business transaction and the legal regulations
⚖ Legal basis: Art. 6 Para. 1 lit. a GDPR (consent), Art. 6 Para. 1 lit. b GDPR (contract), Art. 6 Para. 1 lit. f GDPR (legitimate interests)

If you contact us and communicate by telephone, email or online form, personal data may be processed.

The data will be processed to process and process your question and the related business transaction. The data is stored for as long as the law requires.

Affected people

The above-mentioned processes affect everyone who tries to contact us via the communication channels we provide.

phone

If you call us, the call data will be stored pseudonymously on the respective device and by the telecommunications provider used. In addition, data such as name and telephone number can then be sent by email and saved to answer your query. The data will be deleted as soon as the business transaction has ended and legal requirements allow it.

e-mail

If you communicate with us via email, data may be stored on the respective device (computer, laptop, smartphone, etc.) and data may be stored on the email server. The data will be deleted as soon as the business transaction has ended and legal requirements allow it.

Online forms

If you communicate with us using an online form, data will be stored on our web server and, if necessary, forwarded to one of our email addresses. The data will be deleted as soon as the business transaction has ended and legal requirements allow it.

Legal basis

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

- Art. 6 Para. 1 lit. a GDPR (consent): You give us your consent to store your data and to continue using it for purposes relevant to the business transaction;
- Art. 6 Paragraph 1 Letter b GDPR (contract): There is a need to fulfill a contract with you or a processor such as. B. the telephone provider or we need to use the data for pre-contractual activities, such as: B. the preparation of an offer;

- Art. 6 Para. 1 lit. f GDPR (legitimate interests): We want to conduct customer inquiries and business communication in a professional framework. For this purpose, certain technical facilities such as: B. E-mail programs, exchange servers and mobile phone operators are necessary in order to be able to operate communication efficiently.

Order processing agreement (AVV)

In this section we would like to explain to you what a data processing agreement is and why it is needed. Because the word “order processing agreement” is quite a tongue twister, we will often only use the acronym AVV here in the text. Like most companies, we do not work alone, but also use the services of other companies or individuals. Due to the involvement of various companies or service providers, we may pass on personal data for processing. These partners then act as processors with whom we conclude a contract, the so-called data processing agreement (AVV). The most important thing for you to know is that the processing of your personal data takes place exclusively according to our instructions and must be regulated by the AVV.

Who are processors?

As a company and website owner, we are responsible for all data that we process from you. In addition to those responsible, there can also be so-called processors. This includes every company or person who processes personal data on our behalf. More specifically and according to the GDPR definition: any natural or legal person, authority, institution or other body that processes personal data on our behalf is considered a processor. Processors can therefore be service providers such as hosting or cloud providers, payment or newsletter providers or large companies such as Google or Microsoft.

To make the terminology easier to understand, here is an overview of the three roles in the GDPR:

Data subject (you as a customer or interested party) → **Responsible party** (we as a company and client) → **Processor** (service provider such as web host or cloud provider)

Content of an order processing contract

As already mentioned above, we have concluded an AVV with our partners who act as processors. Above all, this states that the processor processes the data to be processed exclusively in accordance with the GDPR. The contract must be concluded in writing, although in this context the electronic contract conclusion is also considered “written”. The processing of personal data only takes place on the basis of the contract. In the Contract must have the following be included :

- Commitment to us as responsible persons
- Obligations and rights of the person responsible
- Categories more affected persons
- Type of personal Data
- Type and purpose of data processing
- Subject and duration of data processing
- Place of data processing

The contract also contains all of the processor’s obligations. The most important Duties are :

- Measures to Data security to guarantee
- to take possible technical and organizational measures to protect the rights of the data subject
- a Data processing directory to lead
- to cooperate with the data protection supervisory authority upon request
- carry out a risk analysis in relation to the personal data received
- Sub-processors may only be commissioned with the written consent of the person responsible

You can see what such an AVV looks like in concrete terms at https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag-vertragsprocessing.html . Here becomes a Sample contract presented .

Cookies

Cookies summary
Those affected: visitors to the website
Purpose: depending on the respective cookie. You can find more details about this below or from the manufacturer of the software that

sets the cookie.
Data processed: Depending on the cookie used. You can find more details about this below or from the manufacturer of the software that sets the cookie.
Storage period: depends on the respective cookie, can vary from hours
to years ⚖ Legal basis: Art. 6 Para. 1 lit. a GDPR (consent), Art. 6 Para. 1 lit. f GDPR (legitimate interests)

What are cookies?

Our website uses HTTP cookies to store user-specific data.
Below we explain what cookies are and why they are used so that you can better understand the following privacy policy.

Whenever you surf the Internet, you use a browser. Well-known browsers include Chrome, Safari, Firefox, Internet Explorer and Microsoft Edge. Most websites store small text files in your browser. These files are called cookies.

One thing cannot be denied: Cookies are really useful little helpers. Almost all websites use cookies. To be more precise, they are HTTP cookies, as there are also other cookies for other areas of application. HTTP cookies are small files that our website stores on your computer. These cookie files are automatically stored in the cookie folder, the “brain” of your browser. A cookie consists of a name and a value. When defining a cookie, one or more attributes must also be specified.

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

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

There are both first-party cookies and third-party cookies. First-party cookies are created directly by our site, third-party cookies are created by partner websites (e.g. Google Analytics). Each cookie must be evaluated individually because 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 “malicious” things. Cookies also cannot access information on your PC.

For example, cookie data might look like this:

Name: _ga
Value: GA1.2.1326744211.152112750514-9
Purpose: Differentiation of website visitors
Expiry date: after 2 years

A browser should be able to support these minimum sizes:

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

What types of cookies are there?

The question of which cookies we use in particular depends on the services used and is clarified in the following sections of the data protection declaration. At this point we would like to briefly discuss the different types of HTTP cookies.

There are 4 types of cookies:

Essential cookies
These cookies are necessary to ensure basic functions of the website. For example, these cookies are needed when a user puts a product in the shopping cart, then continues surfing on other pages and only later checks out. These cookies do not delete the shopping cart, even if the user closes their browser window.

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

Target-oriented cookies
These cookies ensure better user experience. For example, entered locations, font sizes or form data are saved.

Advertising cookies
These cookies are also called targeting cookies. They serve to provide the user with individually tailored advertising. This can be very practical, but also very annoying.

Typically, when you first visit a website, you will be asked which of these types of cookies you would like to allow. And of course this decision is also saved in a cookie.

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

Purpose of processing via cookies

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

Which data is processed?

Cookies are little helpers for many different tasks. Unfortunately, it is not possible to generalize which data is stored in cookies, but we will inform you about the data processed or stored in the following data protection declaration.

Storage period of cookies

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

You also have an influence on the storage period. You can delete all cookies manually at any time via your browser (see also “Right to object” below). Furthermore, cookies that are based on consent will be deleted at the latest after you revoke your consent, although the legality of storage remains unaffected until then.

Right to object – how can I delete cookies?

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

If you would like to find out which cookies have been stored in your browser, if you want to change or delete cookie settings, you can do this in your browser settings:

Chrome: Delete, enable and manage cookies in Chrome

Safari: Manage cookies and site data with Safari

Firefox: Delete cookies to remove data that websites have placed on your computer

Internet Explorer: Deleting and managing cookies

Microsoft Edge: Deleting and managing cookies

If you generally do not want cookies, you can set your browser so that it always informs you when a cookie is to be set. This means you can decide for each individual cookie whether you allow the cookie or not. The procedure varies depending on the browser. The best thing to do is to search for the instructions in Google using the search term “delete cookies Chrome” or “deactivate cookies Chrome” in the case of a Chrome browser.

Legal basis

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

For absolutely necessary cookies, even if consent is not given, there are **legitimate interests** (Article 6 Para. 1 lit. f GDPR), which in most cases are

of an economic nature. We want to provide website visitors with a pleasant user experience and certain cookies are often absolutely necessary for this.

If non-essential cookies are used, this will only happen with your consent. The legal basis in this respect is Article 6 Paragraph 1 Letter a GDPR.

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

Web hosting introduction

Web hosting summary
Those affected: Visitors to the website
Purpose: professional hosting of the website and securing operations
Processed data: IP address, time of website visit, browser used and other data. You can find more details about this below or with the web hosting provider you use.
Storage period: depends on the respective provider, but usually 2 weeks
⚖ Legal basis: Art. 6 Para. 1 lit.f GDPR (legitimate interests)

What is web hosting?

When you visit websites these days, certain information - including personal data - is created and stored automatically, including on this website. This data should be processed as sparingly as possible and only with justification. By the way, by website we mean the entirety of all websites on a domain, i.e. everything from the start page (homepage) to the very last subpage (like this one). By domain we mean, for example, example.de or musterexample.com.

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

To display the website, the browser must connect to another computer where the website's code is stored: the web server. Operating a web server

is a complicated and time-consuming task, which is why it is usually carried out by professional providers. These offer web hosting and thus ensure reliable and error-free storage of website data. A lot of technical terms, but please stay tuned, it gets better!

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

A picture is worth a thousand words, so the following graphic shows the interaction between the browser, the Internet and the hosting provider.

Why do we process personal data?

The purposes of data processing are:

1. Professional website hosting and operational security
2. to maintain operational and IT security
3. Anonymous evaluation of access behavior to improve our offering and, if necessary, to prosecute or pursue claims

Which data is processed?

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

- the complete internet address (URL) of the website accessed
- Browser and browser version (e.g. Chrome 87)
- the operating system used (e.g. Windows 10)
- the address (URL) of the previously visited page (referrer URL) (e.g. https://www.beispielquellsite.de/vondabinichkommen/)
- the host name and IP address of the device from which access is made (e.g. COMPUTERNAME and 194.23.43.121)
- Date and Time
- in files called web server log files

How long is data stored?

As a rule, the above-mentioned data is stored for two weeks and then automatically deleted. We do not pass on this data, but we cannot rule out that this data will be viewed by authorities if illegal behavior occurs.

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

Legal basis

The legality of the processing of personal data in the context of web hosting results from Article 6 Paragraph 1 Letter f of the GDPR (protection of legitimate interests), because the use of professional hosting from a provider is necessary to keep the company safe and user-friendly on the

Internet to be able to present and, if necessary, pursue attacks and claims resulting from this.

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

Web Analytics Introduction

Web Analytics Data Protection Declaration Summary
Affected: Visitors to the website
Purpose: Evaluation of visitor information to optimize the web offering.
Data processed: Access statistics, which include data such as access locations, device data, access duration and time, navigation behavior, click behavior and IP addresses. You can find more details about this in the web analytics tool used.
Storage period: depends on the web analytics tool used
⚖ Legal basis: Art. 6 Para. 1 lit. a GDPR (consent), Art. 6 Para. 1 lit. f GDPR (legitimate interests)

What is Web Analytics?

We use software on our website to evaluate the behavior of website visitors, known as web analytics for short. Data is collected, which the respective analytical tool provider (also called tracking tool) stores, manages and processes. The data is used to create analyzes of user behavior on our website and make them available to us as the website operator. In addition, most tools offer various testing options. For example, we can test which offers or content are best received by our visitors. We will show you two different offers for a limited period of time. After the test (so-called A/B test), we know which product or content our website visitors find more interesting. For such test procedures, as well as for other analytics procedures, user profiles can also be created and the data can be stored in cookies.

Why do we do web analytics?

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

Which data is processed?

Of course, exactly which data is stored depends on the analysis tools used. However, it is usually stored, for example, what content you view on our website, what buttons or links you click on, when you access a page, what browser you use, what device (PC, tablet, smartphone, etc.) you use website you visit or what computer system you use. If you agreed that location data may also be collected, this can also be processed by the web analysis tool provider.

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

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

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

Duration of data processing

We will inform you below about the duration of data processing if we have further information. In general, we only process personal data for as long as it is absolutely necessary to provide our services and products. If required by law, for example in the case of accounting, this storage period can also be exceeded.

Right to object

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

Legal basis

The use of web analytics requires your consent, which we obtained with our cookie popup. According to **Article 6 Paragraph 1 Letter a of the GDPR (consent), this consent** represents the legal basis for the processing of personal data, as may occur when it is collected by web analytics tools.

In addition to consent, we have a legitimate interest in analyzing the behavior of website visitors and thus improving our offering technically and economically. With the help of web analytics, we detect website errors, identify attacks and improve profitability. The legal basis for this is **Article 6 Paragraph 1 Letter f GDPR (legitimate interests)** . However, we only use the tools if you have given your consent.

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

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

Google Analytics privacy policy

Google Analytics Data Protection Declaration Summary

Affected: Visitors to the website

Purpose: Evaluation of visitor information to optimize the website.

Data processed: Access statistics, which include data such as access locations, device data, access duration and time, navigation behavior and click behavior. You can find more details about this further down in this data protection declaration.

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

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

What is Google Analytics?

On our website we use the analysis tracking tool Google Analytics in version Google Analytics 4 (GA4) from the American company Google Inc. For the European area, the company Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is for everyone Google services responsible. Google Analytics collects data about your actions on our website. Through the combination of different technologies such as cookies, device IDs and login information, you as a user can be identified across different devices. This means your actions can also be analyzed across platforms.

For example, if you click on a link, this event is stored in a cookie and sent to Google Analytics. The reports we receive from Google Analytics allow us to better tailor our website and service to your needs. Below we will go into more detail about the tracking tool and, above all, inform you about what data is processed and how you can prevent this.

Google Analytics is a tracking tool that is used to analyze traffic on our website. The basis of these measurements and analyzes is a pseudonymous user identification number. This number does not contain any personal data such as name or address, but is used to assign events to a device. GA4 uses an event-based model that captures detailed information about user interactions such as page views, clicks, scrolling, conversion events. In addition, various machine learning functions have been built into GA4 to better understand user behavior and certain trends.

GA4 relies on modeling with the help of machine learning functions. This means that based on the data collected, missing data can also be extrapolated in order to optimize the analysis and also to be able to make forecasts.

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

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

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

- Target group reports: Through target group reports we get to know our users better and know more precisely who is interested in our service.
- Display Reports: Display reports make it easier for us to analyze and improve our online advertising.
- Acquisition reports: Acquisition reports give us helpful information about how we can attract more people to our service.
- Behavioral reports: This is where we learn how you interact with our website. We can track the route you take on our site and which links you click on.
- Conversion reports: Conversion is the process in which you take a desired action based on a marketing message. For example, when you go from being just a website visitor to a buyer or newsletter subscriber. These reports help us learn more about how our marketing efforts are being received by you. So want we our Conversion rate increase .
- Real-time reports: Here we always find out immediately what is happening on our website. For example, we can see how many users are currently reading this text.

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

- Event-based data model: This model captures very specific events that may occur on our website. For example, playing a video, purchasing a product or signing up for our newsletter.
- Advanced analytics features: These features allow us to better understand your behavior on our website or certain general trends. For example, we can segment user groups, carry out comparative analyzes of target groups or track your path on our website.
- Predictive modeling: Based on collected data, machine learning can extrapolate missing data that predicts future events and trends. That can us help better Marketing strategies to develop .
- Cross-platform analysis: Data collection and analysis is possible from both websites and apps. This gives us the opportunity to analyze user behavior across platforms, provided you have of course consented to data processing.

Why do we use Google Analytics on our website?

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

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

What data does Google Analytics store?

Google Analytics creates a random, unique ID associated with your browser cookie using a tracking code. This is how Google Analytics recognizes you as a new user and you are assigned a user ID. The next time you visit our site, you will be recognized as a “returning” user. All collected data is stored

together with this user ID. This makes it possible to evaluate pseudonymous user profiles.

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

Using identifiers such as cookies, app instance IDs, user IDs or custom event parameters, your interactions are measured across platforms, provided you have consented. Interactions are all types of actions that you take on our website. If you also use other Google systems (such as a Google account), data generated via Google Analytics may be linked to third-party cookies. Google does not pass on Google Analytics data unless we as website operators authorize this. Exceptions may occur if required by law.

According to Google, Google Analytics 4 does not log or store IP addresses. However, Google uses the IP address data to derive location data and deletes it immediately afterwards. All IP addresses collected from users in the EU are deleted before the data is stored in a data center or on a server.

Because Google Analytics 4 focuses on event-based data, the tool uses significantly fewer cookies compared to previous versions (like Google Universal Analytics). However, there are some specific cookies used by GA4. These include, for example:

Name: _ga
Value: 2.1326744211.152112750514-5
Purpose: By default, analytics.js uses the _ga cookie to store the user ID. Basically, it is used to distinguish website visitors.
Expiry date: after 2 years

Name: _gid
Value: 2.1687193234.152112750514-1
Purpose: The cookie is also used to distinguish website visitors.
Expiry date: after 24 hours

Name: _gat_gtag_UA_<property-id>
Value: 1

Purpose: Used to reduce the request rate. If Google Analytics is provided via Google Tag Manager, this cookie is named _dc_gtm_ <property-id>.
Expiry date: after 1 minute

Note: This list cannot claim to be complete, as Google continually changes its choice of cookies. GA4 also aims to improve data protection. Therefore, the tool offers some options for controlling data collection. For example, we can set the storage period ourselves and also control data collection.

Here we show you an overview of the main types of data collected with Google Analytics:

Heatmaps: Google creates so-called heatmaps. Heatmaps show exactly the areas you click on. This gives us information about where you are on our site.

duration: Google refers to the time that you spend on our site without leaving the site. If you have been inactive for 20 minutes, the session ends automatically.

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

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

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

Technical information: Technical information may include, but is not limited to, your browser type, your Internet service provider or your screen resolution.

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

Other data includes contact details, any reviews, playing media (e.g. when you play a video via our site), sharing content via social media or adding it to your favorites. The list does not claim to be complete and only serves as a general guide to data storage by Google Analytics.

How long and where is the data stored?

Google has their servers spread all over the world. You can read exactly where the Google data centers are located here: https://www.google.com/about/datacenters/locations/?hl=de

Your data is distributed on different physical storage media. This has the advantage that the data can be accessed more quickly and is better protected against manipulation. Every Google data center has appropriate emergency programs for your data. For example, if Google's hardware fails or natural disasters paralyze servers, the risk of service disruption at Google remains low.

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

- 2 months: this is the shortest storage period.
- 14 months: By default, data is stored at GA4 for 14 months.
- 26 months: you can also save the data for 26 months.
- Data will not be deleted until we delete it manually

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

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

How can I delete my data or prevent data storage?

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

browser add-on at https://tools.google.com/dlpage/gaoptout?hl=de . Please note that this add-on only deactivates data collection by Google Analytics.

If you generally want to deactivate, delete or manage cookies, you will find the relevant links to the relevant instructions for the most popular browsers under the “Cookies” section.

Legal basis

The use of Google Analytics requires your consent, which we obtained with our cookie popup. According to **Article 6 Paragraph 1 Letter a of the GDPR (consent), this consent** represents the legal basis for the processing of personal data, as may occur when it is collected by web analytics tools.

In addition to consent, we have a legitimate interest in analyzing the behavior of website visitors and thus improving our offering technically and economically. With the help of Google Analytics, we detect errors on the website, identify attacks and improve profitability. The legal basis for this is **Article 6 Paragraph 1 Letter f GDPR (legitimate interests)** . However, we only use Google Analytics if you have given your consent.

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

Google also uses so-called standard contractual clauses (= Art. 46 Paragraphs 2 and 3 GDPR). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Google undertakes to comply with the European level of data protection when processing your relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the corresponding standard contractual clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

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

We hope we were able to provide you with the most important information about data processing by Google Analytics. If you want to find out more about the tracking service, we recommend these two links: https://marketingplatform.google.com/about/analytics/terms/de/ and https://support.google.com/analytics/answer/ 6004245?hl=de .

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

Google Optimize privacy policy

We use Google Optimize, a website optimization tool, on our website. The service provider is the American company Google Inc. For Europe, the company Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services.

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

Google also uses so-called standard contractual clauses (= Art. 46 Paragraphs 2 and 3 GDPR). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Google undertakes to comply with the European level of data protection when processing your relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the corresponding standard contractual clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

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

You can find out more about the data processed through the use of Google Optimize in the Privacy Policy at https://policies.google.com/privacy?hl=de .

Messenger & Communication Introduction

Messenger & Communication Data Protection Declaration Summary
Those affected: Visitors to the website
Purpose: Contact requests and general communication between us and you
Processed data: Data such as name, address, email address, telephone number, general content data, IP address if applicable
More details on this can be found under the tools used.
Storage period: depends on the messenger & communication functions used
⚖ Legal basis: Art. 6 Para. 1 lit. a GDPR (consent), Art. 6 Para. 1 lit. f GDPR (legitimate interests), Art. 6 Para. 1 p. 1 lit. b. GDPR (contractual or pre-contractual obligations)

What are messenger & communication functions?

We offer various options on our website (such as messenger and chat functions, online or contact forms, email, telephone) to communicate with us. Your data will also be processed and stored to the extent necessary to answer your query and our subsequent measures.

In addition to classic means of communication such as email, contact forms or telephone, we also use chats and messengers. The most commonly used messenger function currently is WhatsApp, but there are of course many different providers that offer messenger functions specifically for websites. If content is encrypted end to end, this will be indicated in the individual data protection texts or in the data protection declaration of the respective provider. End-to-end encryption means nothing other than that the contents of a message are not visible to the provider. However, information about your device, location settings and other technical data may still be processed and stored.

Why do we use messenger & communication functions?

Opportunities to communicate with you are very important to us. Ultimately, we want to talk to you and answer any questions you may have about our service in the best possible way. Well-functioning communication is an important part of our service. With the practical messenger & communication functions, you can choose the ones you like most at any time. In exceptional cases, however, it may also happen that we do not answer certain questions via chat or messenger. This is the case when it comes to internal contractual matters. Here we recommend other communication options such as email or telephone.

We generally assume that we remain responsible under data protection law, even if we use the services of a social media platform. However, the European Court of Justice has decided that in certain cases the operator of the social media platform can be jointly responsible with us within the meaning of Article 26 GDPR. If this is the case, we will point this out separately and work on the basis of a relevant agreement. The essence of the agreement is set out below for the affected platform.

Please note that when using our built-in elements, your data may also be processed outside the European Union, as many providers, such as Facebook Messenger or WhatsApp, are American companies. This may mean that you may no longer be able to easily request or enforce your rights in relation to your personal data.

Which data is processed?

Exactly which data is stored and processed depends on the respective provider of the messenger and communication functions. Basically, this is data such as name, address, telephone number, email address and content data such as all the information that you enter into a contact form. In most cases, information about your device and the IP address are also stored. Data collected via a messenger & communication function is also stored on the providers' servers.

If you want to know exactly what data is stored and processed by the respective providers and how you can object to data processing, you should carefully read the company's respective data protection declaration.

How long is data stored?

How long the data is processed and stored depends primarily on the tools we use. You can find out more about the data processing of the individual tools below. The data protection declarations of the providers usually state exactly which data is stored and processed for how long. In principle, personal data is only processed for as long as is necessary to provide our services. When data is stored in cookies, the storage period varies greatly. The data can be deleted immediately after you leave a website, but it can also remain stored for several years. Therefore, you should look at each individual cookie in detail if you want to know more about data storage. You will usually also find informative information about the individual cookies in the data protection declarations of the individual providers.

Right to object

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

Since cookies can be used in messenger and communication functions, we also recommend our general data protection declaration about cookies. To find out exactly which of your data is stored and processed, you should read the data protection declarations of the respective tools.

Legal basis

If you have agreed that your data can be processed and stored through integrated messenger and communication functions, this consent is considered the legal basis for data processing **(Art. 6 Para. 1 lit. a GDPR)** . We process your request and manage your data within the framework of contractual or pre-contractual relationships in order to fulfill our pre-contractual and contractual obligations or to answer inquiries. The basis for this is **Article 6 Paragraph 1 Sentence 1 Letter b. GDPR** . In principle, if you have given your consent, your data will also be stored and processed on the basis of our legitimate interest **(Art. 6 Para. 1 lit. f GDPR)** in quick and good communication with you or other customers and business partners.

Facebook Messenger Privacy Policy

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

What is Facebook Messenger?

Facebook Messenger is a chat messaging feature developed by Facebook that allows you to send and receive text messages, voice and video calls, photos and other media files to other Facebook users.
If you use Facebook Messenger, your personal data will also be processed on the Facebook servers. In addition to your telephone number and chat messages, this also includes sent photos, videos, profile data, your address or your location.

Why do we use Facebook Messenger?

We want to stay in touch with you and the best way to do this is via messaging services such as Facebook Messenger. On the one hand, because the service works perfectly, and on the other hand, because Facebook is still one of the best-known social media platforms. The service is practical and enables easy and quick communication with you.

How secure is data transfer on Facebook Messenger?

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

Facebook also uses so-called standard contractual clauses (= Art. 46 Paragraphs 2 and 3 GDPR). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Facebook undertakes to comply with the European level of data protection when processing your relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing

decision of the EU Commission. You can find the resolution and the corresponding standard contractual clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

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

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

Signal Messenger Privacy Policy

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

What is Signal Messenger?

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

Why do we use Signal Messenger?

Of course we want to stay in communication with you. When we had to choose a messenger, we quickly chose Signal Messenger. Since the security of data is very important to us, we greatly appreciate the option of encrypted communication that the tool offers us. There are also other security settings such as automatic data deletion or two-factor authentication.

How secure is data transfer with Signal Messenger?

Signal also processes data in the USA, among others. We would like to point out that, according to the European Court of Justice, there is currently no adequate level of protection for data transfer to the USA. This can pose various risks to the lawfulness and security of data processing.

As a basis for data processing for recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, in particular in the USA) or for data transfer there, Signal uses standard contractual clauses approved by the EU Commission (= Article 46, Paragraph 2 and 3 GDPR). These clauses oblige Signal to comply with the EU data protection level when processing relevant data even outside the EU. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the clauses here:
https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

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

Telegram privacy policy

We also use the instant messaging service Telegram. The service provider is the international company Telegram Messenger LLP, which operates at a London address (71-75 Shelton Street, Covent Garden, London, Great Britain) and was developed in Russia.

What is Telegram?

Telegram was founded in 2013 by Nikolai and Pawel Durow. Since the Telegram team sees themselves as so-called digital nomads, you never know exactly where the team works. There is also no imprint on the Telegram website.
Similar to other messaging services such as WhatsApp, you can send messages, photos and videos and other files and also make phone calls via Telegram. This messaging service has become increasingly popular in recent years. In 2022 there were already over 700 million users. If you use Telegram, personal data is also processed and stored on the Telegram servers. In addition to chat messages, this also includes sent photos, videos and profile data, IP addresses and synchronized contacts. Although Telegram encrypts data between the server and your device, it can only offer end-to-end encryption for secret chats. Data stored in the cloud can be viewed by the company and also by third parties.

Why do we use Telegram?

Many people now use Telegram as an alternative to other messaging services such as WhatsApp. We want to stay in touch with you and the best

way to do this is via an instant messaging service, which many of our customers also use. The service works perfectly, is practical and enables easy communication with you.

You can find out more about the data processed through the use of Telegram in the Privacy Policy at https://telegram.org/privacy .

WhatsApp privacy policy

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

What is WhatsApp?

We probably don't need to introduce WhatsApp to you in more detail. The likelihood that you yourself use this well-known messaging service on your smartphone is relatively high. For many years there have been voices that have criticized WhatsApp and its parent company Meta Platforms regarding the handling of personal data. The main criticism in recent years has been related to the merging of WhatsApp user data with Facebook. Facebook then reacted in 2021 and adjusted the terms of use. Facebook announced that currently (as of 2021) no personal data from WhatsApp users is shared with Facebook.
Nevertheless, a lot of your personal data will of course be processed by WhatsApp, provided you use WhatsApp and have agreed to the data processing. In addition to your telephone number and chat messages, this also includes sent photos, videos and profile data. However, photos and videos should only be temporarily stored and all messages and phone calls are provided with end-to-end encryption. So they shouldn't be visible from Meta itself. In addition, information from your address book and other metadata are also stored on WhatsApp.

Why do we use WhatsApp?

We want to stay in touch with you and that works best via WhatsApp. On the one hand, because the service works perfectly, and on the other hand, because WhatsApp is still the most used instant messaging tool worldwide.

The service is practical and enables easy and quick communication with you.

How secure is data transfer with WhatsApp?

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

WhatsApp also uses so-called standard contractual clauses (= Art. 46 Paragraphs 2 and 3 GDPR). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, WhatsApp undertakes to comply with European data protection levels when processing your relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the corresponding standard contractual clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de .

Information on data transfer to WhatsApp, which corresponds to the standard contractual clauses, can be found at https://www.whatsapp.com/legal/business-data-transfer-addendum-20210927

We hope we have given you the most important information about the use and data processing by WhatsApp. You can find out more about the data processed through the use of WhatsApp in the Privacy Policy at https://www.whatsapp.com/privacy .

Social media introduction

Social Media Data Protection Declaration Summary
Those affected: Visitors to the website
Purpose: Presentation and optimization of our services, contact with visitors, interested parties, etc., advertising

Processed data: Data such as telephone numbers, email addresses, contact details, data on user behavior, information about Your device and your IP address.
You can find more details about this in the respective social media tool used.

Storage period: depends on the social media platforms used

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

What is Social Media?

In addition to our website, we are also active on various social media platforms. User data can be processed so that we can specifically address users who are interested in us via social networks. In addition, elements of a social media platform may also be embedded directly into our website. This is the case, for example, if you click on a so-called social button on our website and are redirected directly to our social media presence. So-called social media or social media are websites and apps through which registered members can produce content, exchange content openly or in specific groups and network with other members.

Why do we use social media?

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

The data that is stored and processed through your use of a social media channel has the primary purpose of being able to carry out web analyses. The aim of these analyzes is to be able to develop more precise and personal marketing and advertising strategies. Depending on your behavior on a social media platform, appropriate conclusions can be drawn about your interests using the evaluated data and so-called user profiles can be created. This also makes it possible for the platforms to present you with tailored advertisements. Cookies are usually set in your browser for this purpose and store data about your usage behavior.

We generally assume that we remain responsible under data protection law, even if we use the services of a social media platform. However, the European Court of Justice has decided that in certain cases the operator of the social media platform can be jointly responsible with us within the meaning of Article 26 GDPR. If this is the case, we will point this out separately and work on the basis of a relevant agreement. The essence of the agreement is then reproduced below for the affected platform.

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

Which data is processed?

Exactly which data is 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 that you enter in a contact form, user data such as which buttons you click, who you like or follow, when you visited which pages, information about Your device and your IP address. Most of this data is stored in cookies. Especially if you have a profile on the social media channel you are visiting and are logged in, data can be linked to your profile.

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

If you want to know exactly what data is stored and processed by social media providers and how you can object to data processing, you should read the company's respective data protection declaration carefully. If you have any questions about data storage and data processing or want to assert the relevant rights, we recommend that you contact the provider directly.

Duration of data processing

We will inform you below about the duration of data processing if we have further information. For example, the social media platform Facebook stores data until it is no longer needed for its own purpose. However,

customer data that is compared with your own user data will be deleted within two days. In general, we only process personal data for as long as it is absolutely necessary to provide our services and products. If required by law, for example in the case of accounting, this storage period can also be exceeded.

Right to object

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

Since cookies can be used with social media tools, we also recommend our general data protection declaration about cookies. To find out exactly which of your data is stored and processed, you should read the data protection declarations of the respective tools.

Legal basis

If you have agreed that your data can be processed and stored through integrated social media elements, this consent is considered the legal basis for data processing **(Art. 6 Para. 1 lit. a GDPR)** . In principle, if you have given your consent, your data will also be stored and processed on the basis of our legitimate interest **(Art. 6 Para. 1 lit. f GDPR)** in quick and good communication with you or other customers and business partners. However, we only use the tools if you have given your consent. Most social media platforms also set cookies on your browser to store data. We therefore recommend that you read our data protection text about cookies carefully and view the data protection declaration or the cookie guidelines of the respective service provider.

You can find information about specific social media platforms - if available - in the following sections.

AddThis Data protection

AddThis Privacy Policy Summary

□□□□ subjects: Visitors to the website
Purpose: Optimization of our service
Processed data: Data such as data on user behavior, information about your device and your IP address.
You can find more details about this in the data protection declaration below.
Storage period: the collected data is stored for 13 months from data collection
⚖ Legal basis: Art. 6 Para. 1 lit. a GDPR (consent), Art. 6 Para. 1 lit. f GDPR (legitimate interests)

What is AddThis?

On our website we use plugins from AddThis from Oracle America, Inc. (500 Oracle Parkway, Redwood Shores, CA 94065, USA). With these plug-ins you can share content from our website quickly and easily with other people. If you visit a website with an AddThis function, your data can be transferred to the company AddThis, stored and processed. With this data protection declaration you will find out why we use AddThis, what data is processed and how you can prevent this data transfer.

Among other things, AddThis develops software tools that are integrated into websites to enable users to distribute content on various social media channels or via email. In addition, AddThis also offers functions that are used for website analysis. The collected data is also used to offer interest-based advertising to Internet users. The service is used by more than 15 million website operators worldwide.

Why do we use AddThis on our website?

By using the AddThis buttons, you can share interesting content from our website on various social media channels such as Facebook, Twitter, Instagram or Pinterest. If you like our content, we would of course be happy if you share it with your social community. And the easiest way to do this is to use the AddThis buttons.

What data does AddThis store?

If you share content with AddThis and you are logged in with the respective social media account, data such as your visit to our website and the sharing

of content can be assigned to the user account of the corresponding social media channel. AddThis uses cookies, pixels, HTTP headers and browser identifiers to collect data about your visitor behavior. In addition, some of this data is shared with third parties after pseudonymization.
Here one exemplary List of possible processed Data :

- Unique ID of a cookie placed in the web browser
- Address of the visited website
- Time of website visit
- Search queries that led a visitor to the AddThis page
- Duration of stay on one website
- The IP address of the computer or mobile device
- Mobile Advertising IDs (Apple IDFA or Google AAID)
- Information contained in HTTP headers or other transmission protocols used
- Which program was used on the computer (browser) or which operating system was used (iOS)

AddThis uses cookies, which we list below as examples and in extracts. You can find out more about AddThis cookies at https://www.oracle.com/legal/privacy/addthis-privacy-policy.html .

Name: bt2
Value: 8961a7f179d87qq69V69112750514-3
Purpose: This cookie is used to record parts of the website visited in order to recommend other parts of the website.
Expiry date: after 255 days

Name: bku
Value: ra/99nTmYN+fZWX7112750514-4
Purpose: This cookie registers anonymized user data such as your IP address, geographical location, websites visited and which ads you clicked on.
Expiry date: after 179 days

Note: Please remember that this is an exemplary list and we cannot claim to be complete.

AddThis also shares collected information with other companies. Further details can be found at https://www.oracle.com/legal/privacy/addthis-privacy-policy.html . AddThis also uses the data received to create target groups and

interest profiles and to offer interest-based advertising to users in the same advertising network.

How long and where is the data stored?

AddThis stores the collected data for 13 months from the time the data was collected. 1% of the data is kept as a “sample data set” for a maximum of 24 months so that the business relationship is preserved. However, in this “sample data set” the direct and indirect identification (such as your IP address and cookie ID) is hashed. This means that the personal data can no longer be associated with you without additional information. Since the AddThis company is headquartered in the USA, the data collected is also stored on American servers.

How can I delete my data or prevent data storage?

You have the right to access and delete your personal data at any time. If you no longer wish to see advertising based on data collected by AddThis, you can use the opt-out button at https://datacloudoptout.oracle.com/?tid=112750514 . An opt-out cookie is set, which you are not allowed to delete in order to keep this setting.

You can also set your preferences for usage-based online advertising via https://www.youronlinechoices.com/at/ in preference management.

Your browser offers one option to prevent data processing or to manage it according to your wishes. Depending on the browser, data processing works slightly differently. Under the “Cookies” section you will find the corresponding links to the relevant instructions for the most popular browsers.

Legal basis

If you have agreed that your data can be processed and stored through integrated social media elements, this consent is considered the legal basis for data processing **(Art. 6 Para. 1 lit. a GDPR)** . In principle, your data will also be stored and processed on the basis of our legitimate interest **(Art. 6 Para. 1 lit. f GDPR)** in quick and good communication with you or other customers and business partners. However, we only use the integrated social media elements if you have given your consent. Most social media platforms also set cookies on your browser to store data. We therefore

recommend that you read our data protection text about cookies carefully and view the data protection declaration or the cookie guidelines of the respective service provider.

AddThis also processes data in the USA, among others. We would like to point out that, according to the European Court of Justice, there is currently no adequate level of protection for data transfer to the USA. This can pose various risks to the lawfulness and security of data processing.

As the basis for data processing for recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, in particular in the USA) or for data transfer there, AddThis uses standard contractual clauses approved by the EU Commission (= Art. 46 Para. 2 and 3 GDPR). These clauses oblige AddThis to comply with the EU data protection level when processing relevant data even outside the EU. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

If you would like to know more about how AddThis processes your data, you can find more information at https://www.oracle.com/legal/privacy/addthis-privacy-policy.html .

Facebook privacy policy

Facebook data protection declaration Summary
Those affected: Visitors to the website
Purpose: Optimization of our service
Processed data: Data such as customer data, data on user behavior, information about your device and your IP address.
You can find more details about this in the data protection declaration below.
Storage period: until the data is no longer useful for Facebook's purposes
⚖ Legal basis: Art. 6 Para. 1 lit. a GDPR (consent), Art. 6 Para. 1 lit. f GDPR (legitimate interests)

What are Facebook tools?

We use selected tools from Facebook on our website. Facebook is a social media network of the company Meta Platforms Inc. or for the European area of the company Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland. These tools enable us to offer you and people who are interested in our products and services the best possible offer.

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

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

In addition to many other products, Facebook also offers the so-called “Facebook Business Tools”. This is the official name of Facebook. Since the term is hardly known, we have decided to just call them Facebook tools. Below find itself under other things :

- Facebook pixel
- social plug-ins (such as the “Like” or “Share” button)
- Facebook login
- Account kit
- APIs (programming interface)
- SDKs (collection of programming tools)
- Platform integrations
- Plugins
- Codes
- Specifications

- Documentations
- Technologies and services

Through these tools, Facebook expands services and has the opportunity to obtain information about 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 really interested in them. With the help of advertisements (Facebook Ads) we can reach exactly these people. However, in order to show users appropriate advertising, Facebook needs information about people's wishes and needs. The company is provided with information about user behavior (and contact details) on our website. This means that Facebook collects better user data and can show interested people the appropriate advertising about our products or services. The tools thus enable tailor-made advertising campaigns on Facebook.

Facebook calls data about your behavior on our website “event data”. These are also used for measurement and analysis services. This allows Facebook to create “campaign reports” on our behalf about the impact of our advertising campaigns. We also use analyzes to gain a better insight into how you use our services, website or products. This allows us to use some of these tools to optimize your user experience on our website. For example, you can use the social plug-ins to share content on our site directly on Facebook.

What data are stored by Facebook tools?

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

Facebook uses this information to compare the data with the data it has about you (if you are a Facebook member). Before customer data is transmitted to Facebook, so-called “hashing” takes place. This means that a data set of any size is transformed into a character string. This also serves to encrypt data.

In addition to the contact details, “event data” is also transmitted. “Event data” means the information that we receive about you on our website. For

example, which subpages you visit or which products you buy from us. Facebook does not share the information it receives with third parties (such as advertisers) unless the company has explicit permission or is legally required to do so. “Event data” can also be linked to contact details. This allows Facebook to offer better personalized advertising. After the matching process already mentioned, Facebook deletes the contact data again.

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

How long and where is the data stored?

Basically, Facebook stores data until it is no longer needed for its own services and Facebook products. Facebook has servers around the world where its data is stored. However, customer data will be deleted within 48 hours after it has been compared with your own user data.

How can I delete my data or prevent data storage?

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

The data will only be completely deleted if you completely delete your Facebook account. Here's how deleting your Facebook account works:

1) On the right side of Facebook, click Settings.

2) Then click on “Your Facebook information” in the left column.

3) Now click “Deactivation and deletion”.

4) Now select “Delete Account” and then click “Next and Delete Account”

5) Now enter your password, click “Continue” and then click “Delete Account”

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

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

Legal basis

If you have agreed that your data can be processed and stored by integrated Facebook tools, this consent is considered the legal basis for data processing **(Art. 6 Para. 1 lit. a GDPR)** . In principle, your data will also be stored and processed on the basis of our legitimate interest **(Art. 6 Para. 1 lit. f GDPR)** in quick and good communication with you or other customers and business partners. However, we only use the tools if you have given your consent. Most social media platforms also set cookies on your browser to store data. We therefore recommend that you read our data protection text about cookies carefully and view Facebook's data protection declaration or cookie guidelines.

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

Facebook also uses so-called standard contractual clauses (= Art. 46 Paragraphs 2 and 3 GDPR). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Facebook undertakes to comply with the European level of data protection

when processing your relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the corresponding standard contractual clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

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

We hope we have given you the most important information about the use and data processing of Facebook tools. If you want to find out more about how Facebook uses your data, we recommend reading the data policy at https://www.facebook.com/privacy/policy/ .

Facebook login privacy policy

We have integrated the practical Facebook login on our site. This means you can easily log in to us with your Facebook account without having to create another user account. If you decide to register via the Facebook login, you will be redirected to the social media network Facebook. You can register there using your Facebook user data. Through this login process, data about you and your user behavior is stored and transmitted to Facebook.

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

Name: fr
Value: 0jieyh4c2GnlufEJ9..Bde09j…1.0.Bde09j
Purpose: This cookie is used to ensure that the social plugin on our website works as well as possible.
Expiry date: after 3 months

Name: datr
Value: 4Jh7XUA2112750514SEmPsSfzCOO4JFFl
Purpose: Facebook sets the “datr” cookie when a web browser accesses facebook.com, and the cookie helps identify login activity 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 listed are only a small selection of the cookies available to Facebook. Other cookies include _ fbp, sb or wd. A complete list is not possible because Facebook has a large number of cookies and uses them variably.

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

- Your Facebook name
- Her Profile picture
- one stored email address
- Friends lists
- Button information (e.g. “Like” button)
- Birthday date
- Language
- Place of residence

In return, we provide Facebook with information about your activities on our website. This includes, among other things, information about the device you use, which subpages you visit or which products you have purchased from us.

By using Facebook Login, you consent to data processing. You may revoke this agreement at any time. If you would like to find out more information about data processing by Facebook, we recommend the Facebook data protection declaration at https://www.facebook.com/privacy/policy/ .

If you are logged in to Facebook, you can change your advertising settings yourself at https://www.facebook.com/adpreferences/advertisers/?entry_product=ad_settings_screen .

Facebook Social Plugins Privacy Policy

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

The following social plug-ins are offered by Facebook:

- “ Save ” button
- Like button, share, send and quote
- Page plugin
- Comments
- Messenger plugin
- Embedded Posts and video players
- Groups plugin

You can find more information about how the individual plug-ins are used at https://developers.facebook.com/docs/plugins . 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 they allow Facebook to optimize our advertisements.

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

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

In order to prevent Facebook from collecting a lot of data during your visit to our website and combining it with Facebook data, you must log out of Facebook while visiting 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. However, data such as your IP address or which website you visit can be transferred to Facebook. We would like to expressly point out that we do not know exactly the exact contents of the data. However,

based on our current state of knowledge, we try to inform you as much as possible about data processing. You can also read how Facebook uses the data in the company's data policy at https://www.facebook.com/about/privacy/update .

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

Name: dpr
Value: not specified
Purpose: This cookie is used to enable the social plug-ins to work on our website.
Expiry date: after the end of the session

Name: fr
Value: 0jieyh4112750514c2GnlufEJ9..Bde09j...1.0.Bde09j
Purpose: The cookie is also necessary for the plug-ins to function properly.
Expiry date: after 3 months

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

If you are logged in to Facebook, you can change your advertising settings yourself at https://www.facebook.com/adpreferences/advertisers/ . If you are not a Facebook user, you can generally manage your usage-based online advertising at https://www.youronlinechoices.com/de/praferenzmanagement/?tid=112750514 . There you have the option to deactivate or activate providers.

If you would like to learn more about Facebook's data protection, we recommend that you consult the company's own data policies at https://www.facebook.com/privacy/policy/ .

Flickr privacy policy

We also use the online community and photo platform Flickr. The service provider is the American company Flickr Inc., 67 E Evelyn Ave #200, Mountain View, CA 94041, USA.

Flickr also processes data in the USA, among others. We would like to point out that, according to the European Court of Justice, there is currently no

adequate level of protection for data transfer to the USA. This can pose various risks to the lawfulness and security of data processing.

As a basis for data processing for recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, i.e. in particular in the USA) or for data transfer there, Flickr uses standard contractual clauses approved by the EU Commission (= Article 46, Paragraph 2 and 3 GDPR). These clauses oblige Flickr to comply with the EU data protection level when processing relevant data even outside the EU. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

You can find out more about the data processed through the use of Flickr in the Privacy Policy at https://www.flickr.com/help/privacy .

Gravatar Data protection

Gravatar data protection declaration summary
Those affected: Visitors to the website
Purpose: Optimization of our service
Processed data: including your encrypted email address, IP address and URL of our server
. You can find more details about this in the data protection declaration below.
Storage period: the data is generally deleted when it is no longer useful for the provider's services.
⚖ Legal basis: 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 plug-in from Automattic Inc. (60 29th Street #343, San Francisco, CA 94110, USA) on our website. Among other things, Gravatar is automatically activated on all WordPress websites. The function makes it possible to display user images (avatars) in published posts or comments, provided the corresponding email address is registered with www.gravatar.com .

Through this function, data is sent to Gravatar or Automattic Inc., stored and processed there. In this data protection declaration we want to inform you what data is involved, how the network uses this data and how you can manage or prevent data storage.

Gravatar basically stands for “Globally Recognized Avatar” and this means a globally available avatar (a user image) that is linked to the email address. Gravatar is the world's leading provider of this service. As soon as a user enters the email address on a website that is also registered with Gravatar at www.gravatar.com , a previously stored image is automatically displayed together with a published post or comment.

Why do we use Gravatar on our website?

People often talk about anonymity on the internet. Through an avatar, users get a face to the people commenting. In addition, it is generally easier to be recognized online and can therefore build up a certain level of popularity. Many users enjoy the advantages of such a user image and also want to appear personally and authentically online. Of course, we want to offer you the opportunity to display your Gravatar on our website. We also like to see the faces of our commenting users. With the Gravatar function activated, we are also expanding our service on our website. Ultimately, we want you to feel comfortable on our website and to receive a comprehensive and interesting offer.

What data does Gravatar store?

For example, as soon as you post a comment on a blog post that requires an email address, WordPress checks whether the email address is associated with an avatar on Gravatar. For this request, your email address will be sent in encrypted or hashed form, including your IP address and our URL, to the Gravatar or Automattic servers. This will verify that this email address is registered with Gravatar.

If this is the case, the image stored there (Gravatar) will be displayed together with the published comment. If you have registered an email address with Gravatar and comment on our website, further data will be transferred to Gravatar, stored and processed. In addition to the IP address and data on user behavior, this includes, for example, browser type, unique device identifier, preferred language, date and time of page entry, operating system and information about the mobile network. Gravatar uses this

information to improve its services and offers and to obtain better insights into the use of its own service.

The following cookies are set by Automattic when a user uses an email address registered with Gravatar to leave a comment:

Name: gravatar
Value: 16b3191024acc05a238209d51ffcb92bdd710bd19112750514-7
Purpose: We were unable to find out any precise information about the cookie.
Expiry date: after 50 years

Name: is-logged-in
Value: 1112750514-1
Purpose: This cookie stores the information that the user is logged in using the registered email address.
Expiry date: after 50 years

How long and where is the data stored?

Automattic deletes the collected data when it is no longer used for its own services and the company is not legally obliged to retain the data. Web server logs such as IP address, browser type and operating system are deleted after approximately 30 days. As long as Automattic uses the data to analyze the traffic on its own websites (e.g. all WordPress sites) and to fix possible problems. The data is also stored on Automattic's American servers.

How can I delete my data or prevent data storage?

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 at any time.

Since an image is only displayed and data is transferred to Gravatar when using an email address registered with Gravatar, you can also prevent the transfer of your data to Gravatar by using an email address that is not registered with Gravatar comment on our website or write posts.

You can manage, deactivate or delete possible cookies that are set while commenting in your browser. Please just note that any comment functions

will then no longer be fully available. Depending on which browser you use, cookie management works a little differently. Under the “Cookies” section you will find the corresponding links to the relevant instructions for the most popular browsers.

Legal basis

If you have agreed that your data can be processed and stored through integrated social media elements, this consent is considered the legal basis for data processing **(Art. 6 Para. 1 lit. a GDPR)** . In principle, your data will also be stored and processed on the basis of our legitimate interest **(Art. 6 Para. 1 lit. f GDPR)** in quick and good communication with you or other customers and business partners. However, we only use the integrated social media elements if you have given your consent. Most social media platforms also set cookies on your browser to store data. We therefore recommend that you read our data protection text about cookies carefully and view the data protection declaration or the cookie guidelines of the respective service provider.

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

Automattic also uses so-called standard contractual clauses (= Art. 46 Paragraphs 2 and 3 GDPR). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Automattic undertakes to comply with European data protection levels when processing your relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the corresponding standard contractual clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de .

You can find out more about the standard contractual clauses and data processed through the use of Gravatar in the data protection declaration at

https://automattic.com/privacy/ , general information about Gravatar at http://de.gravatar.com/ .

Instagram privacy policy

Instagram data protection declaration summary
Those affected: Visitors to the website
Purpose: Optimization of our service
Processed data: Data such as data on user behavior, information about your device and your IP address.
You can find more details about this in the data protection declaration 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 installed Instagram functions on our website. Instagram is a social media platform owned by Instagram LLC, 1601 Willow Rd, Menlo Park CA 94025, USA. Instagram has been a subsidiary of Meta Platforms Inc. since 2012 and is one of the Facebook products. Embedding Instagram content on our website is called embedding. This allows us to show you content such as buttons, photos or videos from Instagram directly on our website. If you access websites on our website that have an Instagram function integrated, data will be transmitted to Instagram, stored and processed. Instagram uses the same systems and technologies as Facebook. Your data will therefore be processed across all Facebook companies.

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

Instagram is one of the most famous social media networks worldwide. Instagram combines the advantages of a blog with the advantages of audiovisual platforms such as YouTube or Vimeo. You can upload photos

and short videos to “Insta” (as many users casually call the platform), edit them with various filters and also distribute them on other social networks. And if you don't want to be active yourself, you can just follow other interesting users.

Why do we use Instagram on our website?

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

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

What data does Instagram store?

If you come across one of our pages that has built-in Instagram functions (such as Instagram images or plug-ins), your browser will automatically contact Instagram's servers. Data is sent to Instagram, stored and processed. Regardless of whether you have an Instagram account or not. This includes information about our website, about your computer, about purchases you make, about advertisements you see and how you use our services. The date and time of your interaction with Instagram are also stored. If you have an Instagram account or are logged in, Instagram stores significantly more data about you.

Facebook differentiates between customer data and event data. We assume that this is exactly the case with Instagram. Customer data includes, for example, name, address, telephone number and IP address. This customer data will only be transmitted to Instagram once it has been “hashed”. Hashing means turning a data set into a string. This allows you to encrypt the contact details. In addition, the above-mentioned “event data” is also transmitted. By “event data” Facebook – and consequently also

Instagram – means data about your user behavior. It can also happen that contact data is combined with event data. The contact details collected will be compared with the data Instagram already has about you.

The collected data is transmitted to Facebook via small text files (cookies), which are usually set in your browser. Depending on the Instagram functions used and whether you have an Instagram account, different amounts of data are stored.

We assume that data processing on Instagram works in the same way as on Facebook. This means: if you have an Instagram account or have visited www.instagram.com , Instagram has set at least one cookie. If this is the case, your browser will send information to Instagram via the cookie as soon as you come into contact with an Instagram function. This data will be deleted or anonymized after 90 days at the latest (after comparison). Although we have looked intensively into Instagram's data processing, we cannot say exactly what data Instagram collects and stores.

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

These cookies were used in our test:

Name: csrftoken
Value: “”
Purpose: This cookie is most likely set for security reasons to prevent forged requests. However, we were unable to find out more precisely.
Expiry date: after one year

Name: mid
Value: “”
Purpose: Instagram sets this cookie to optimize its own services and offers on and outside of Instagram. The cookie sets a unique user ID.
Expiry date: after the end of the session

Name: fbsr_112750514124024
Value: no information
Purpose: This cookie stores the log-in request for users of the Instagram

app.
Expiry date: after the end of the session

Name: rur
Value: ATN
Purpose: This is an Instagram cookie that ensures functionality on Instagram.
Expiry date: after the end of the session

Name: urlgen
Value: "{"194.96.75.33": 1901}:1iEtYv:Y833k2_UjKvXgYe112750514"
Purpose: This cookie is used for Instagram's marketing purposes.
Expiry date: after the end of the session

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

How long and where is the data stored?

Instagram shares the information it receives between Facebook companies, with external partners and with people you connect with around the world. Data processing takes place in compliance with our own data guidelines. Your data is distributed on Facebook servers around the world, among other things for security reasons. Most of these servers are located in the USA.

How can I delete my data or prevent data storage?

Thanks to the General Data Protection Regulation, you have the right to information, portability, correction and deletion of your data. You can manage your data in Instagram settings. If you want to completely delete your data on Instagram, you will need to permanently delete your Instagram account.

And this is how deleting your Instagram account works:

First open the Instagram app. On your profile page, go down and click on "Help Section." Now you come to the company's website. On the website, click "Manage Account" and then click "Delete Your Account."

If you delete your account entirely, Instagram will delete posts such as your photos and status updates. Information that other people have shared about you is not part of your account and will therefore not be deleted.

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

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

Legal basis

If you have agreed that your data can be processed and stored through integrated social media elements, this consent is considered the legal basis for data processing **(Art. 6 Para. 1 lit. a GDPR)** . In principle, your data will also be stored and processed on the basis of our legitimate interest **(Art. 6 Para. 1 lit. f GDPR)** in quick and good communication with you or other customers and business partners. However, we only use the integrated social media elements if you have given your consent. Most social media platforms also set cookies on your browser to store data. We therefore recommend that you read our data protection text about cookies carefully and view the data protection declaration or the cookie guidelines of the respective service provider.

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

Instagram also uses so-called standard contractual clauses (= Art. 46 Paragraphs 2 and 3 GDPR). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through the EU-US Data Privacy Framework and the Standard Contractual Clauses,

Instagram undertakes to comply with European data protection levels when processing your relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the corresponding standard contractual clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

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

Pinterest Privacy Policy

Pinterest Privacy Policy Summary
Those affected: Visitors to the website
Purpose: Optimization of our service
Processed data: Data such as data on user behavior, information about your device, your IP address and search terms.
You can find more details about this in the data protection declaration below.
Storage period: until Pinterest 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 Pinterest?

On our site we use buttons and widgets from the social media network Pinterest, the company Pinterest Inc., 808 Brannan Street, San Francisco, CA 94103, USA. The Irish company Pinterest Europe Ltd. is responsible for the European region. (Palmerston House, 2nd Floor, Fenian Street, Dublin 2, Ireland) is responsible for all data protection-related aspects.

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

Why do we use Pinterest?

Pinterest has been around for several years now and this social media platform 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's why we're also represented on Pinterest and want to present our content accordingly outside of our website. The data collected can also be used for advertising purposes so that we can show advertising messages to exactly those people who are interested in our services or products.

What data does Pinterest process?

So-called log data can be saved. This includes information about your browser, IP address, the address of our website and the activities carried out on it (for example when you click the bookmark or pin button), search history, date and time of the request and 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, preset language settings and clickstream data are stored in cookies. Pinterest understands clickstream data to be information about your website behavior.

If you have a Pinterest account and are logged in, the data collected through our site may be added 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. Here you can see an example selection of cookies that are then set in your browser.

Name: _auth
Value: 0
Purpose: The cookie is used for authentication. For example, a value such as your “username” can be stored there.
Expiry date: after one year

Name: _pinterest_referrer
Value: 1
Purpose: The cookie stores that you came to Pinterest via our website. So the URL of our website is saved.
Expiry date: after the end of the session

Name: _pinterest_sess
Value: …9HRHZvVE0rQlUxdG89
Purpose: The cookie is used to log in to Pinterest and contains user IDs, authentication tokens and timestamps.
Expiry date: after one year

Name: _routing_id
Value: “8d850ddd-4fb8-499c-961c-77efae9d4065112750514-8”
Purpose: The 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 a user ID and the timestamp.
Expiry date: after one year

Name: csrftoken
Value: 9e49145c82a93d34fd933b0fd8446165112750514-1
Purpose: This cookie is most likely set for security reasons to prevent forged requests. However, we were unable to find out more precisely.
Expiry date: after one year

Name: sessionFunnelEventLogged
Value: 1
Purpose: We have not yet been able to find out any further information about this cookie.
Expiry date: after one day

How long and where is the data stored?

Pinterest generally stores the data collected until it is no longer needed for the company's purposes. As soon as data retention is no longer necessary, for example to comply with legal regulations, the data will either be deleted or anonymized so that you can no longer be identified as a person. The data can also be stored on American servers.

Right to object

You also have the right and option to revoke your consent to the use of cookies or third-party providers such as Pinterest at any time. This works

either via our cookie management tool or via other opt-out functions. For example, you can also prevent data collection through cookies by managing, deactivating or deleting cookies in your browser.

Since cookies can be used for embedded Pinterest elements, we also recommend our general data protection declaration about cookies. To find out exactly which of your data is stored and processed, you should read the data protection declarations of the respective tools.

Legal basis

If you have agreed that your data can be processed and stored through integrated social media elements, this consent is considered the legal basis for data processing **(Art. 6 Para. 1 lit. a GDPR)** . In principle, your data will also be stored and processed on the basis of our legitimate interest **(Art. 6 Para. 1 lit. f GDPR)** in quick and good communication with you or other customers and business partners. However, we only use the tool if you have given your consent. Most social media platforms also set cookies on your browser to store data. We therefore recommend that you read our data protection text about cookies carefully and view the data protection declaration or the cookie guidelines of the respective service provider.

Pinterest also processes your data in the USA, among other places. We would like to point out that, according to the European Court of Justice, there is currently no adequate level of protection for data transfer to the USA. This can pose various risks to the lawfulness and security of data processing.

As the basis for data processing for recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, i.e. in particular in the USA) or for data transfer there, Pinterest uses so-called standard contractual clauses (= Article 46, Paragraphs 2 and 3 of the GDPR). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through these clauses, Pinterest undertakes to comply with European data protection standards when processing your relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the

corresponding standard contractual clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de.

You can find more information about Pinterest's standard contractual clauses at https://policy.pinterest.com/de/privacy-policy#section-residents-of-the-eea .

We have tried to provide you with the most important information about data processing by Pinterest. You can find out more about Pinterest's data policies at https://policy.pinterest.com/de/privacy-policy .

ShareThis Data protection

ShareThis Privacy Policy Summary

subjects: Visitors to the website

Purpose: Optimization of our service

Processed data: Data such as data on user behavior, information about your device and your IP address.
You can find more details about this in the data protection declaration below.

Storage period: the collected data is stored for up to 14 months

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

What is ShareThis?

On our website we have integrated functions from ShareThis from ShareThis Inc. (4005 Miranda Ave, Suite 100, Palo Alto, 94304 California, USA). These are, for example, “sharing” plug-ins for various social media channels. These functions allow you to share content from our website on social media channels. If you access a website with a ShareThis function, your data may be transferred to the company, stored and processed. With this data protection declaration you will find out why we use ShareThis, what data is processed and how you can prevent this data transfer.

ShareThis is a technology company that offers website owners tools to improve website quality. By using ShareThis's social plugins, you can share content from our website on various social media channels such as Facebook, Twitter, Instagram and Co. The company offers content sharing

to over 40 different channels and is used by over 3 million website owners worldwide. The data collected by ShareThis is also used for individual advertisements.

Why do we use ShareThis on our website?

We want to convince people with our content and of course we are happy if our content is recommended to others. Then we know we are on the right path. The easiest way to do this is to use the “Share buttons” directly on our website. Thanks to the variety of different social media channels, our content can also be presented to a wide audience. This helps us to become better known and more successful on the Internet. The plug-ins also serve you because you can share interesting content with your social media community with just one click.

What data does ShareThis store?

If you share content with ShareThis and you are logged in with the respective social media account, data such as your visit to our website and the sharing of content can be assigned to the user account of the corresponding social media channel. ShareThis uses cookies, pixels, HTTP headers and browser identifiers to collect data about your visitor behavior. In addition, some of this data is shared with third parties after pseudonymization.

Here is a list of the data that may be processed:

- Unique ID of a cookie placed in the web browser
- General Click behavior
- Addresses of those visited Web pages
- Search queries that led a visitor to the ShareThis page
- Navigation from website to website if this is done via ShareThis services
- Duration of stay on one website
- Which items were clicked or highlighted
- The IP address of the computer or mobile device
- Mobile Advertising IDs (Apple IDFA or Google AAID)
- Information contained in HTTP headers or other transmission protocols used
- Which program was used on the computer (browser) or which operating system was used (iOS)

ShareThis uses cookies, which we list as examples below. You can find out more about ShareThis cookies at https://sharethis.com/de/privacy/ .

Name: __unam
Value: 8961a7f179d1d017ac27lw87qq69V69112750514-5
Purpose: This cookie counts the “clicks” and “shares” on a website.
Expiry date: after 9 months

Name: __stid
Value: aGCDwF4hjVEI+oIsABW7112750514Ag==
Purpose: This cookie stores user behavior, such as the websites accessed, navigation from page to page and the time spent on the website.
Expiry date: after 2 years

Name: __sharethis_cookie_test__
Value: 0
Purpose: This cookie monitors “clickstream” activity. This means it monitors where you clicked on the website.
Expiry date: after the end of the session

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

How long and where is the data stored?

ShareThis retains collected data for a period of up to 14 months from the date of data collection. ShareThis cookies expire 13 months after the last update. Since ShareThis is an American company, data is transferred and stored on American ShareThis servers.

How can I delete my data or prevent data storage?

If you no longer wish to see advertising based on data collected by ShareThis, you can use the opt-out button at https://sharethis.com/de/privacy/ . An opt-out cookie is set, which you are not allowed to delete in order to keep this setting.

You can also set your preferences for usage-based online advertising via https://www.youronlinechoices.com/at/ in preference management.

You also have the option of managing, deactivating or deleting data stored via cookies in your browser. How the administration works exactly depends

on your browser. Under the “Cookies” section you will find the corresponding links to the relevant instructions for the most popular browsers.

You can also set your browser so that you are always informed when a cookie is about to be set.

Legal basis

If you have agreed that your data can be processed and stored through integrated social media elements, this consent is considered the legal basis for data processing **(Art. 6 Para. 1 lit. a GDPR)** . In principle, your data will also be stored and processed on the basis of our legitimate interest **(Art. 6 Para. 1 lit. f GDPR)** in quick and good communication with you or other customers and business partners. However, we only use the integrated social media elements if you have given your consent. Most social media platforms also set cookies on your browser to store data. We therefore recommend that you read our data protection text about cookies carefully and view the data protection declaration or the cookie guidelines of the respective service provider.

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

ShareThis also uses so-called standard contractual clauses (= Art. 46 Paragraphs 2 and 3 GDPR). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, ShareThis undertakes to comply with European data protection levels when processing your relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the corresponding standard contractual clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de .

You can find out more about the standard contractual clauses and data processed through the use of ShareThis in the data protection declaration at https://sharethis.com/de/privacy/ .

Snapchat privacy policy

Snapchat data protection declaration summary
Affected parties: Visitors to the website
Purpose: Optimization of our service
Processed data: Data such as data on user behavior, information about your device and your IP address.
You can find more details about this in the data protection declaration below.
Storage period: depends on the type of data
⚖ Legal basis: Art. 6 Para. 1 lit. a GDPR (consent), Art. 6 Para. 1 lit. f GDPR (legitimate interests)

What is Snapchat?

We also use integrations with the messaging and social media service Snapchat for our website. The service provider is the American company Snap Inc., 2772 Donald Douglas Loop N, Santa Monica (HQ), CA, USA.

With Snapchat, users can create so-called “snaps”, i.e. short images or videos, and share them with friends or followers. Snapchat is a popular communication tool, especially among younger people. Unlike other social media tools, these “snaps” are deleted after a limited time. Depending on the user's preferences, this time can be set between a few seconds and up to 24 hours. Snapchat also offers functions such as group chats, video calls and a Discover section for media companies.

Why do we use Snapchat on our website?

We have provided Snapchat features on our website so that we can also point out Snapchat content and you can also follow us on Snapchat. This means we can stay in touch with you beyond our website presence. By integrating Snapchat content, we also offer all of our visitors who are not on Snapchat the opportunity to get an insight into the Snapchat world. So we see the integration as part of our overall offering on our website.

What data does Snapchat process?

When you view or interact with Snapchat content through our website, Snapchat may collect information about your usage behavior and device. This may include information such as your IP address, browser type, operating system, location, language preferences and other technical information. Snapchat may also use cookies and similar technologies to collect information and personalize your experience.

If you have or create a Snapchat account yourself, further information can also be collected and processed. In this case, you voluntarily provide information such as your name, username, email address, telephone number and date of birth. If you purchase something within the app , you will also need to provide payment details. All of this information is processed by Snapchat if you provide this data. If you actively use the service with your account, all information sent via Snapchat will also be processed. This information includes chats, conversations, images and videos.

How long and where is the data stored?

Snapchat stores different data for different lengths of time and Snapchat servers are distributed in different regions around the world. This means that your data can also be processed in the USA, for example. As already mentioned above, the storage duration of the “snaps” can be partially selected in the settings. Most messages sent in the tool are automatically deleted by the servers once they have been received or have expired. But there is also data that is stored for significantly longer. This includes account information such as name, mobile phone number or email address. The length of time location data is retained depends on how accurate it is and which Snapchat service is being used.

At https://help.snapchat.com/hc/de/articles/7012334940948 you will find a very good overview of the storage period of various Snapchat data.

How can I delete my data or prevent data storage?

If you have a Snapchat account, you can manage your privacy settings directly on Snapchat and determine how long various content is stored. For example, you can use the settings of your Snapchat account to specify whether “Snaps” are deleted after a few seconds or after 24 hours. You can

also ask those directly responsible at Snapchat to delete your personal data. However, Snapchat's data protection declaration points out that although most data is deleted, it may arise for legal reasons that the data deletion has to be suspended or that some data remains stored.

Additionally, you can manage and disable cookies that Snapchat may set in your web browser to limit data collection. This is also possible without a Snapchat account. However, please note that this may affect the functionality of our website.

Legal basis

If you have agreed that your data can be processed and stored by Snapchat, this consent is considered the legal basis for data processing **(Art. 6 Para. 1 lit. a GDPR)** . In principle, your data will also be stored and processed on the basis of our legitimate interest **(Art. 6 Para. 1 lit. f GDPR)** in quick and good communication with you or other customers and business partners. However, we only use the integrated Snapchat elements if you have given your consent. Snapchat may also set cookies on your browser to store data. We therefore recommend that you read our data protection text about cookies carefully and view the data protection declaration or the cookie guidelines of the respective service provider.

Snap also processes your data in the USA, among other places. We would like to point out that, according to the European Court of Justice, there is currently no adequate level of protection for data transfer to the USA. This can pose various risks to the lawfulness and security of data processing.

As the basis for data processing for recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, i.e. in particular in the USA) or for data transfer there, Snap uses so-called standard contractual clauses (= Article 46, Paragraphs 2 and 3 of the GDPR). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through these clauses, Snap undertakes to comply with European data protection standards when processing your relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the corresponding

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

For more information about Snap's standard contractual clauses, please visit https://snap.com/en-US/terms/standard-contractual-clauses .

You can find out more about the data processed through the use of Snapchat in the Privacy Policy at https://snap.com/de-DE/privacy/privacy-policy .

TikTok Data protection

TikTok data protection declaration summary
Those affected: Visitors to the website
Purpose: Optimization of our service
Data processed: your IP address, browser data, date and time of your page access can be stored
. You can find more details about this in the data protection declaration below.
Storage period: varies depending on settings
⚖ Legal basis: Art. 6 Para. 1 lit. a GDPR (consent), Art. 6 Para. 1 lit. f GDPR (legitimate interests)

What is TikTok?

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

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

Why do we use TikTok on our website?

We have integrated TikTok into our website so that you can watch TikTok videos if you wish and, if necessary, interact with the videos. TikTok is

particularly known for funny and creative content and of course we don't want to withhold such content from you. After all, we also like to watch one or two creative TikTok videos ourselves.

What data does TikTok process?

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

If you have a TikTok account yourself, further information can also be collected and processed. This includes user information (such as name, date of birth or your email address) and data about your communications with other TikTok users.

How long and where is the data stored?

The storage period and locations of the data collected by TikTok can vary widely and are subject to TikTok's privacy policy. TikTok may also store data on servers in the United States and other countries. The storage period usually depends on the respective legal requirements and internal guidelines. However, we have not yet been able to find out exactly how long data is stored. As soon as we have more information, we will of course let you know.

How can I delete my data or prevent data storage?

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

Legal basis

If you have consented to your data being processed and stored by TikTok, this consent is considered the legal basis for data processing **(Art. 6 Para. 1 lit. a GDPR)** . In principle, your data will also be stored and processed on

the basis of our legitimate interest **(Art. 6 Para. 1 lit. f GDPR)** in quick and good communication with you or other customers and business partners. However, we only use the integrated social media elements if you have given your consent. TikTok may also set cookies on your browser to store data. We therefore recommend that you read our data protection text about cookies carefully and view the data protection declaration or the cookie guidelines of the respective service provider.

TikTok also processes your data in the USA, among other places. We would like to point out that, according to the European Court of Justice, there is currently no adequate level of protection for data transfer to the USA. This can pose various risks to the lawfulness and security of data processing.

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

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

X (formerly : Twitter) Privacy Policy

X (Former: Twitter) Data protection declaration Summary
Visitors to the website
Purpose: Optimization of our service
Processed data: Data such as data on user behavior, information on

your device and your IP address.
You can find more details about this in the data protection declaration below.

Storage period: X deletes data collected from other websites after 30 days at the latest

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

What is X?

We have integrated functions from X on our website. These include, for example, embedded tweets, timelines, buttons or hashtags. X is a short messaging service and social media platform from the American company X Corp., 1355 Market Street, Suite 900 San Francisco, CA 94103, USA. For Europe, the company Twitter International Unlimited Company (One Cumberland Place, Fenian Street, Dublin 2, D02 AX07, Ireland) is responsible for processing personal data.

To our knowledge, in the European Economic Area and Switzerland, no personal data or data about your web activities are transferred to X simply by integrating X functions. Only when you interact with the X functions, such as clicking on a button, can data be sent to X, stored and processed there. We have no influence on this data processing and bear no responsibility. As part of this data protection declaration, 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 against data transfer.

For some, X is a news service, for others it is a social media platform, and for others it is a microblogging service. All of these terms have their place and mean more or less the same thing.

Both private individuals and companies use X to communicate with interested people via short messages. X only allows 280 characters per message. These messages are called “tweets”. Unlike Facebook, for example, the service does not focus on expanding a network for “friends”, but rather wants to be seen as a global and open news platform. At X you can also have an anonymous account and tweets can be deleted by the company on the one hand and by the users themselves on the other.

Why do we use X on our website?

Like many other websites and companies, we try to offer our services and communicate with our customers through various channels. X in particular (better known to many as Twitter) has grown close to our hearts as a useful “small” news service. We constantly tweet or retweet exciting, funny or interesting content. We understand that you cannot follow every channel separately. After all, you also have something else to do. That's why we have also integrated X functions on our website. You can experience our X activity “on site” or come to our X page via a direct link. Through the integration we want to strengthen our service and user-friendliness on our website.

What data does X store?

On some of our subpages you will find the built-in X functions. When you interact with the X Content, such as clicking a button, X may collect and store data. Even if you don't have an X account yourself. X calls this data “log data”. This includes demographic data, browser cookie IDs, your smartphone ID, hashed email addresses, and information about which pages you have visited on X and what actions you have taken. Of course, X stores more data if you have an X account and are logged in. Until now, this storage was 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 set when you are not logged in to X but visit a website with built-in X functions. Please consider this list as an example. We cannot guarantee completeness under any circumstances, as the choice of cookies is always changing and depends on your individual actions with the X content.

These cookies were used in our test:

Name: personalization_id
Value: “v1_cSJIsogU51SeE112750514”
Purpose: This cookie stores information about how you use the website and which advertisements may have brought you to X.
Expiry date: after 2 years

Name: long
Value: de

Purpose: This cookie stores your default or preferred language.
Expiry date: after the end of the session

Name: guest_id
Value: 112750514v1%3A157132626
Purpose: This cookie is set to identify you as a guest.
Expiry date: after 2 years

Name: fm
Value: 0
Purpose: Unfortunately, we were unable to find out the purpose of this cookie.
Expiry date: after the end of the session

Name: external_referer
Value: 1127505142beTA0sf5lkMrlGt
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 various advertising purposes by X.
Expiry date: After one year

Name: ct0
Value: c1179f07163a365d2ed7aad84c99d966
Purpose: Unfortunately, we did not find any information about this cookie.
Expiry date: after 6 hours

Name: _twitter_sess
Value: 53D%253D–dd0248112750514-
Purpose: This cookie allows you to use functions within the X website.
Expiry date: after the end of the session

Note: X also works with third parties. That's why we also recognized the three Google Analytics cookies _ga, _gat, _gid in our test.

On the one hand, X uses the data collected to better understand user behavior and thus improve its own services and advertising offers, and on the other hand, the data also serves internal security measures.

How long and where is the data stored?

If X collects data from other websites, it will be deleted, summarized or otherwise hidden after a maximum of 30 days. The X servers are located in various server centers throughout the United States. It can therefore be assumed that the data collected is collected and stored in America. After our research, we could not clearly determine whether X also has its own servers in Europe. In principle, X can store the data collected until it is no longer useful to the company, you delete the data or there is a statutory deletion period.

How can I delete my data or prevent data storage?

In its data protection guidelines, X repeatedly emphasizes that it does not store data from external website visits if you or your browser are located in the European Economic Area or Switzerland. However, if you interact with X directly, X will of course also store your data.

If you have an X account, you can manage your information by clicking “More” under the “Profile” button. Then click on “Settings and data protection”. Here you can manage data processing individually.

If you don't have an X account, you can go to twitter.com and then click "Customization." You can manage your collected data under “Individualization and data”.

As mentioned above, most data is stored via cookies and you can manage, deactivate or delete them in your browser. Please note that you can only “edit” the cookies in the browser you have chosen. This means: if you use a different browser in the future, you will have to manage your cookies again according to your wishes. Under the “Cookies” section you will find the corresponding links to the relevant instructions for the most popular browsers.

You can also manage your browser so that you are informed about each individual cookie. Then you can always decide individually whether you allow a cookie or not.

X also uses the data for personalized advertising inside and outside of X. You can switch off personalized advertising in the settings under “Individualization and data”. If you use X on a browser, you can deactivate personalized advertising at https://optout.aboutads.info/?c=2&lang=EN .

Legal basis

If you have agreed that your data can be processed and stored through integrated social media elements, this consent is considered the legal basis for data processing **(Art. 6 Para. 1 lit. a GDPR)** . In principle, your data will also be stored and processed on the basis of our legitimate interest **(Art. 6 Para. 1 lit. f GDPR)** in quick and good communication with you or other customers and business partners. However, we only use the integrated social media elements if you have given your consent. Most social media platforms also set cookies on your browser to store data. We therefore recommend that you read our data protection text about cookies carefully and view the data protection declaration or the cookie guidelines of the respective service provider.

X also processes your data in the USA, among other places. We would like to point out that, according to the European Court of Justice, there is currently no adequate level of protection for data transfer to the USA. This can pose various risks to the lawfulness and security of data processing.

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

More information about the standard contractual clauses at X can be found at https://gdpr.twitter.com/en/controller-to-controller-transfers.html .

We hope we have given you a basic overview of data processing by X. 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 the X data protection declaration at https://twitter.com/de/privacy .

XING privacy policy

Xing data protection declaration Summary

Those affected: Visitors to the website

Purpose: Optimization of our service

Processed data: Your IP address, browser data, date and time of your page access can be stored
. You can find more details about this in the data protection declaration below.

Storage period: Xing user data is stored until deletion is requested

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

What is Xing?

On our website we use social plugins from the social media network Xing, the company Xing SE, Dammtorstraße 30, 20354 Hamburg, Germany. These functions allow you, for example, to share content on Xing directly via our website, log in via Xing or follow interesting content. You can recognize the plug-ins by the company name or the Xing logo. If you access a website that uses a Xing plug-in, data can be transmitted to the “Xing servers”, stored and evaluated. In this data protection declaration we want to inform you about what data is involved and how you can manage or prevent this data storage.

Xing is a social network with headquarters in Hamburg. The company specializes in managing professional contacts. This means that, unlike other networks, Xing is primarily about professional networking. The platform is often used for job hunting or to find employees for your own company. Xing also offers interesting content on various professional topics. The global counterpart to this is the American company LinkedIn.

Why do we use Xing on our website?

There is now a flood of social media channels and we are well aware that your time is very valuable. Not every company's social media channel can be scrutinized closely. That's why we want to make your life as easy as possible so that you can share or follow interesting content directly via our website on Xing. With such “social plug-ins” we expand our service on our website. In addition, the data collected by Xing helps us to carry out targeted advertising measures on the platform. This means that our service is only shown to people who are really interested in it.

What data does Xing store?

Xing offers the share button, the follow button and the log-in button as plug-ins for websites. As soon as you open a page where a Xing social plug-in is installed, your browser connects to servers in a data center used by Xing. In the case of the share button - according to Xing - no data should be stored that could be directly related to a person. In particular, Xing does not store your IP address. Furthermore, no cookies are set in connection with the share button. This means that no evaluation of your user behavior takes place. Further information can be found at https://dev.xing.com/plugins/share_button/privacy_policy

With the other Xing plug-ins, cookies are only set in your browser when you interact with the plug-in or click on it. Personal data such as your IP address, browser data, date and time of your page access on Xing can be stored here. If you have a XING account and are logged in, collected data will be assigned to your personal account and the data stored therein.

The following cookies are set in your browser when you click on the follow or log-in button and are not yet logged in to Xing. Please keep in mind that this is an exemplary list and we cannot claim to be complete:

Name: AMCVS_0894FF2554F733210A4C98C6%40AdobeOrg
Value: 1
Purpose: This cookie is used to create and store identifications of website visitors.
Expiry date: after the end of the session

Name: c_
Value: 157c609dc9fe7d7ff56064c6de87b019112750514-8
Purpose: We were unable to find out
any further information about this cookie . **Expiry date:** after one day

Name: prevPage
Value: wbm%2FWelcome%2Flogin
Purpose: This cookie stores the URL of the previous website you visited.
Expiry date: after 30 minutes

Name: s_cc
Value: true
Purpose: This Adobe Site Catalyst cookie determines whether cookies are generally activated in the browser.
Expiry date: after the end of the session

Name: s_fid
Value: 6897CDCD1013221C-39DDACC982217CD1112750514-2
Purpose: This cookie is used to identify a unique visitor.
Expiry date: after 5 years

Name: visitor_id
Value: fe59fbe5-e9c6-4fca-8776-30d0c1a89c32
Purpose: The visitor cookie contains a unique visitor ID and the unique identifier for your account.
Expiry date: after 2 years

Name: _session_id
Value: 533a0a6641df82b46383da06ea0e84e7112750514-2
Purpose: This cookie creates a temporary session ID that is used as an in-session user ID. The cookie is absolutely necessary to provide the functions of Xing.
Expiry date: after the end of the session

As soon as you are logged in to Xing or are a member, further personal data will definitely be collected, processed and stored. Xing also passes on personal data to third parties if this is necessary to fulfill its own business purposes, if you have given your consent or if there is a legal obligation.

How long and where is the data stored?

Xing stores the data on various servers in various data centers. The company stores this data until you delete the data or until you delete a user account. Of course, this only affects users who are already Xing members.

How can I delete my data or prevent data storage?

You have the right to access and delete your personal data at any time. Even if you are not a Xing member, you can prevent possible data processing via your browser or manage it according to your wishes. Most data is stored via cookies. Depending on which browser you have, management works slightly differently. Under the “Cookies” section you will find the corresponding links to the relevant instructions for the most popular browsers.

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

Legal basis

If you have agreed that your data can be processed and stored through integrated social media elements, this consent is considered the legal basis for data processing **(Art. 6 Para. 1 lit. a GDPR)** . In principle, your data will also be stored and processed on the basis of our legitimate interest **(Art. 6 Para. 1 lit. f GDPR)** in quick and good communication with you or other customers and business partners. However, we only use the integrated social media elements if you have given your consent. Most social media platforms also set cookies on your browser to store data. We therefore recommend that you read our data protection text about cookies carefully and view the data protection declaration or the cookie guidelines of the respective service provider.

We have tried to provide you with the most important information about data processing by Xing. You can find out more about data processing by the social media network Xing at https://privacy.xing.com/de/datenschutzerklaerung .

Online marketing introduction

Online marketing data protection declaration Summary

Those affected: Visitors to the website

Purpose: Evaluation of visitor information to optimize the website.

Data processed: Access statistics, which include data such as access locations, device data, access duration and time, navigation behavior, click behavior and IP addresses. Personal data such as name

or email address can also be processed. You can find more details about the online marketing tool used.

Storage period: depends on the online marketing tools used

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

What is online marketing?

Online marketing refers to all measures that are carried out online to achieve marketing goals such as increasing brand awareness or closing a deal. Furthermore, our online marketing measures aim to draw people's attention to our website. In order to be able to show our offer to many interested people, we do online marketing. Most of the time this involves online advertising, content marketing or search engine optimization. So that we can use online marketing efficiently and in a targeted manner, personal data is also stored and processed. On the one hand, the data helps us to only show our content to those people who are interested in it and, on the other hand, we can measure the advertising success of our online marketing measures.

Why do we use online marketing tools?

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

Which data is processed?

So that our online marketing works and the success of the measures can be measured, user profiles are created and data is stored, for example, in cookies (these are small text files). With the help of this data, we can not only place advertising in the classic way, but also display our content directly on our website in the way you prefer. There are various third-party tools that offer these functions and also collect and store your data. The named cookies store, for example, which web pages you have visited on our website, how long you have viewed these pages, which links or buttons you

clicked or from which website you came to us. Technical information can also be stored. For example, your IP address, which browser you use, which device you use to visit our website or the time when you accessed our website and when you left it again. If you have consented to us also determining your location, we can also store and process this.

Your IP address is stored in a pseudonymized form (i.e. shortened). Unique data that directly identifies you as a person, such as name, address or email address, is only stored in pseudonymized form as part of advertising and online marketing processes. We cannot therefore identify you as a person, but we have only stored the pseudonymized, stored information in the user profiles.

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

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

For all advertising tools we use that store your data on their servers, we only receive aggregated information and never data that identifies you as an individual. The data only shows how well implemented advertising measures worked. For example, we see what actions prompted you or other users to come to our website and purchase a service or product there. Based on the analyses, we can improve our advertising offering in the future and adapt it even more precisely to the needs and wishes of interested people.

Duration of data processing

We will inform you below about the duration of data processing if we have further information. In general, we only process personal data for as long as it is absolutely necessary to provide our services and products. Data stored in cookies is stored for different lengths of time. Some cookies are deleted after you leave the website, others can be stored in your browser for several years. You can usually find detailed information about the individual

cookies that the provider uses in the respective data protection declarations of the individual providers.

Right to object

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

Since cookies can usually be used in online marketing tools, we also recommend our general data protection declaration about cookies. To find out exactly which of your data is stored and processed, you should read the data protection declarations of the respective tools.

Legal basis

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

We also have a legitimate interest in measuring online marketing measures in an anonymous form in order to use the data obtained to optimize our offering and our measures. The corresponding legal basis for this is **Article 6 Paragraph 1 Letter f GDPR (legitimate interests)** . However, we only use the tools if you have given your consent.

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

Web design Introduction

Web design data protection declaration Summary
Those affected: Visitors to the website
Purpose: To improve the user experience
Processed data: Which data is processed depends largely on the

services used. This usually involves the IP address, technical data, language settings, browser version, screen resolution and name of the browser. You can find more details about the web design tools used.
Storage period: depends on the tools used
⚖ Legal basis: Art. 6 Para. 1 lit. a GDPR (consent), Art. 6 Para. 1 lit. f GDPR (legitimate interests)

What is web design?

We use various tools on our website that serve our web design. Web design is not, as is often assumed, just about making our website look pretty, but also about functionality and performance. But of course the right look of a website is also one of the major goals of professional web design. Web design is a sub-area of media design and deals with the visual as well as the structural and functional design of a website. The aim is to use web design to improve your experience on our website. In web design jargon, this is referred to as user experience (UX) and usability. User experience refers to all the impressions and experiences that website visitors experience on a website. A sub-point of the user experience is usability. This is about the user-friendliness of a website. The main emphasis here is on ensuring that content, subpages or products are clearly structured and that you can find what you are looking for easily and quickly. In order to offer you the best possible experience on our website, we also use so-called third-party web design tools. In this data protection declaration, the “web design” category includes all services that improve the design of our website. These can be, for example, fonts, various plugins or other integrated web design functions.

Why do we use web design tools?

How you absorb information on a website depends very much on the structure, functionality and visual perception of the website. Therefore, good and professional web design became more and more important for us. We are constantly working on improving our website and see this as an extended service for you as a website visitor. Furthermore, a beautiful and functioning website also has economic advantages for us. After all, you will only visit us and take advantage of our offers if you feel completely comfortable.

What data are stored by web design tools?

When you visit our website, web design elements may be integrated into our pages, which can also process data. Of course, exactly what data is involved depends heavily on the tools used. Below you can see exactly which tools we use for our website. We recommend that you read the respective data protection declaration of the tools used for more information about data processing. You will usually find out what data is being processed, whether cookies are being used and how long the data is being kept. Fonts such as Google Fonts also automatically transmit information such as language settings, IP address, browser version, browser screen resolution and browser name to the Google servers.

Duration of data processing

How long data is processed is very individual and depends on the web design elements used. For example, if cookies are used, the retention period can last as little as a minute or as long as a few years. Please be smart about this. On the one hand, we recommend our general text section on cookies and the data protection declarations of the tools used. There you can usually find out exactly which cookies are used and what information is stored in them. For example, Google Font files are stored for one year. This is intended to improve the loading time of a website. In principle, data is only retained for as long as is necessary to provide the service. If required by law, data can also be stored for longer.

Right to object

You also have the right and the opportunity 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. You can also prevent data collection through cookies by managing, deactivating or deleting cookies in your browser. However, there is also data among web design elements (mostly fonts) that cannot be deleted so easily. This is the case when data is automatically collected directly when a page is accessed and transmitted to a third-party provider (such as Google). Then please contact the support of the relevant 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, the legal basis for the corresponding data processing is this consent. According to Article 6 Para. 1 lit to improve our website. After all, only then can we provide you with a beautiful and professional website. The corresponding legal basis for this is Article 6 Paragraph 1 Letter f GDPR (legitimate interests). However, we only use web design tools if you have given your consent. We definitely want to emphasize this again here.

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

Adobe Fonts Privacy Policy

We use Adobe Fonts, a web font hosting service, on our website. The service provider is the American company Adobe Inc. The Irish company Adobe Systems Software Ireland Companies, 4-6 Riverwalk, Citywest Business Campus, Dublin 24, Ireland, is responsible for the European area.

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

Adobe also uses so-called standard contractual clauses (= Art. 46 Paragraphs 2 and 3 GDPR). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Adobe undertakes to comply with European data protection standards when processing your relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the corresponding standard contractual clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

You can find more information about Adobe's standard contractual clauses at https://www.adobe.com/at/privacy/eudatatransfers.html .

You can find out more about the data processed through the use of Adobe Fonts in the Privacy Policy at https://www.adobe.com/at/privacy.html .

Font Awesome Privacy Policy

Font Awesome Data Protection Declaration Summary

Those affected: Visitors to the website

Purpose: Optimization of our service

Processed data: such as IP address and which icon files are loaded

You can find more details further down in this data protection declaration.

Storage period: Files in identifiable form are stored for a few weeks

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

What is Font Awesome?

We use Font Awesome from the American company Fonticons (307 S. Main St., Suite 202, Bentonville, AR 72712, USA) on our website. When you visit one of our websites, the Font Awesome web font (specifically icons) is loaded via the Font Awesome content delivery network (CDN). This means that the texts, fonts and icons are displayed appropriately on every device. In this data protection declaration we go into more detail about data storage and data processing by this service.

Icons are playing an increasingly important role for websites. Font Awesome is a web font designed specifically for web designers and web developers. With Font Awesome, icons can be scaled and colored as desired using the CSS style sheet language. They replace old image icons. Font Awesome CDN is the easiest way to load the icons or fonts on your website. All we had to do was integrate a small line of code into our website.

Why do we use Font Awesome on our website?

Font Awesome allows content on our website to be better prepared. This allows you to orientate yourself better on our website and understand the content more easily. With the icons you can sometimes even replace entire words and save space. This is particularly practical when we optimize

content specifically for smartphones. These icons are inserted as HMTL code instead of as an image. This allows us to edit the icons with CSS exactly how we want. At the same time, with Font Awesome we also improve our loading speed because they are only HTML elements and not icon images. All of these advantages help us to make the website even clearer, fresher and faster for you.

What data does Font Awesome store?

The Font Awesome Content Delivery Network (CDN) is used to load icons and symbols. CDNs are networks of servers distributed worldwide that make it possible to quickly load files from nearby locations. As soon as you access one of our pages, the corresponding icons are provided by Font Awesome.

In order for the web fonts to be loaded, your browser must establish a connection to the Fonticons, Inc. servers. Your IP address will be recognized. Font Awesome also collects data about which icon files are downloaded and when. Technical data such as your browser version, screen resolution or the time of the page accessed are also transmitted.

This data is collected and stored for the following reasons:

- to optimize content delivery networks
- to identify and correct technical errors
- to protect CDNs from misuse and attacks
- to be able to charge fees to Font Awesome Pro customers
- to know the popularity of icons
- to know what computer and software you are using

If your browser does not allow web fonts, a standard font on your PC will automatically be used. Based on our current knowledge, no cookies are set. We are in contact with Font Awesome's data protection department and will let you know as soon as we find out more.

How long and where is the data stored?

Font Awesome stores data about the use of the Content Delivery Network on servers also in the United States of America. However, the CDN servers are located worldwide and store user data wherever you are. The data is usually only stored in an identifiable form for a few weeks. Aggregated

statistics about the usage of the CDNs may also be stored for longer. Personal data is not included here.

How can I delete my data or prevent data storage?

As far as we know, Font Awesome does not currently store any personal data via the content delivery networks. If you do not want data about the icons used to be stored, you unfortunately cannot visit our website. If your browser does not allow web fonts, no data will be transmitted or stored. In this case, your computer's default font will simply be used.

Legal basis

If you have consented to Font Awesome being used, the legal basis for the corresponding data processing is this consent. According to **Art. 6 Para. 1 lit. a GDPR (consent), this consent** represents the legal basis for the processing of personal data, as may occur when it is collected by Font Awesome.

We also have a legitimate interest in using Font Awesome to optimize our online service. The corresponding legal basis for this is **Article 6 Paragraph 1 Letter f GDPR (legitimate interests)** . However, we only use Font Awesome if you have given your consent.

We would like to point out that, according to the European Court of Justice, there is currently no adequate level of protection for data transfer to the USA. The data processing is essentially done by Font Awesome. This can lead to data not being processed and stored anonymously. Furthermore, US government authorities may have access to individual data. It may also happen that this data is linked to data from other Font Awesome services where you have a user account.

If you want to find out more about Font Awesome and how it handles data, we recommend the privacy policy at https://fontawesome.com/privacy and the help page at https://fontawesome.com/support .

Getty Images Privacy Policy

We use the image portal Getty Images for our website. The service provider is the American company Getty Images Inc., 605 5th Avenue South Suite 400 Seattle, WA 98104, USA.

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

In addition, Getty Images uses so-called standard contractual clauses (= Art. 46 Paragraphs 2 and 3 GDPR). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Getty Images is committed to complying with European data protection standards when processing your relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the corresponding standard contractual clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de .

You can find out more about the data and standard contractual clauses processed through the use of Getty Images in the data protection declaration at https://www.gettyimages.at/company/privacy-policy .

Google Fonts privacy policy

Google Fonts Data Protection Declaration Summary
Those affected: Visitors to the website
Purpose: Optimization of our service
Processed data: Data such as IP address and CSS and font requests

You can find more details further down in this data protection declaration.
Storage period: Font files are stored by Google for one year
⚖ Legal basis: Art. 6 Para. 1 lit. a GDPR (consent), Art. 6 Para. 1 lit. f GDPR (legitimate interests)

What are Google Fonts?

We use Google Fonts on our website. These are the “Google Fonts” from Google Inc. For the European region, Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services.

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

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

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

Why do we use Google Fonts on our website?

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

What data does Google store?

When you visit our website, the fonts are downloaded via a Google server. Through this external call, data is transmitted to the Google servers. This is how Google also recognizes that you or your IP address visits our website. The Google Fonts API is designed to reduce the use, storage, and collection of end-user data to what is necessary for proper font delivery. By the way, API stands for “Application Programming Interface” and serves, among other things, as a data transmitter in the software sector.

Google Fonts stores CSS and font requests securely on Google and is therefore protected. By collecting usage figures, Google can determine how well the individual fonts are received. Google publishes the results on internal analysis sites, such as Google Analytics. Google also uses data from its own web crawler to determine which websites use Google fonts. This data is published in the Google Fonts BigQuery database. Entrepreneurs and developers use the Google web service BigQuery to examine and move large amounts of data.

However, it should also be remembered that with every Google Font request, information such as language settings, IP address, browser version, browser screen resolution and browser name are automatically transmitted to the Google servers. Whether this data is also stored cannot be clearly determined or is not clearly communicated by Google.

How long and where is the data stored?

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

The font files are stored by Google for one year. Google's goal is to fundamentally improve the loading time of websites. When millions of websites reference the same fonts, they are cached after the first visit and immediately appear on all other websites visited later. Sometimes Google updates font files to reduce file size, increase language coverage, and improve design.

How can I delete my data or prevent data storage?

The data that Google stores for a day or a year cannot simply be deleted. The data is automatically transmitted to Google when the page is accessed.

In order to delete this data early, you must contact Google Support at https://support.google.com/?hl=de&tid=112750514 . In this case, you can only prevent data storage if you do not visit our site.

Unlike other web fonts, Google allows us unlimited access to all fonts. So we have unlimited access to a sea of fonts and get the best for our website. You can find out more about Google Fonts and other questions at https://developers.google.com/fonts/faq?tid=112750514 . Although Google addresses data protection-related matters there, it does not contain any really detailed information about data storage. It is relatively difficult to get really precise information about stored data from Google.

Legal basis

If you have consented to Google Fonts being used, the legal basis for the corresponding data processing is this consent. According to **Art. 6 Para. 1 lit. a GDPR (consent), this consent** represents the legal basis for the processing of personal data, as may occur when it is collected by Google Fonts.

We also have a legitimate interest in using Google Font to optimize our online service. The corresponding legal basis for this is **Article 6 Paragraph 1 Letter f GDPR (legitimate interests)** . However, we only use Google Font if you have given your consent.

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

Google also uses so-called standard contractual clauses (= Art. 46 Paragraphs 2 and 3 GDPR). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Google undertakes to comply with the European level of data protection when processing your relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing

decision of the EU Commission. You can find the resolution and the corresponding standard contractual clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

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

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

Google Fonts Local Privacy Policy

On our website we use Google Fonts from Google Inc. The company Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for Europe. We have integrated the Google fonts locally, i.e. on our web server - not on Google's servers. This means there is no connection to Google servers and therefore no data transfer or storage.

What are Google Fonts?

Google Fonts used to be called Google Web Fonts. This is an interactive directory with over 800 fonts that Google provides for free. With Google Fonts you could use fonts without uploading them to your own server. However, in order to prevent any information transfer to Google servers, we have downloaded the fonts to our server. In this way, we act in accordance with data protection regulations and do not send any data to Google Fonts.

Miscellaneous Introduction

Miscellaneous Data protection declaration Summary
Data subjects: Visitors to the website
Purpose: To improve the user experience
Processed data: Which data is processed depends largely on the services used. This is usually an IP address and/or technical data. You can find more details about the tools used in each case.
Storage period: depends on the tools used
⚖ Legal basis: Art. 6 Para. 1 lit. a GDPR (consent), Art. 6 Para. 1 lit. f GDPR (legitimate interests)

What falls under “other”?

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

Why do we use other third parties?

With our website we want to offer you the best web offering in our industry. A website has long been more than just a business card for a company. Rather, it is a place designed to help you find what you are looking for. 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, stored and processed there. This is necessary because otherwise the content will not be sent to your browser and therefore will not be displayed accordingly. It may also happen that service providers also use pixel tags or web beacons. These are small graphics on websites that record a log file and can also create analyzes of this file. With the information received, providers can improve their own marketing efforts. In addition to pixel tags, such information (such as which button you click or when you access which page) can also be stored in cookies. In addition to analysis data about your web behavior, technical information such as your browser type or operating system can also be stored there. Some providers can also link the data obtained with other internal services or with third-party providers. Each provider handles your data differently. We therefore recommend that you carefully read the data protection declarations of the respective services. We generally strive to only use services that handle the issue of data protection very carefully.

Duration of data processing

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

Legal basis

If we ask you for your consent and you also agree that we may use the service, this is considered the legal basis for processing your data (Art. 6 Para. 1 lit. a GDPR). In addition to consent, we have a legitimate interest in analyzing the behavior of website visitors and thus improving our offering technically and economically. The legal basis for this is Article 6 Paragraph 1 Letter f GDPR (legitimate interests). However, we only use the tools if you have given your consent.

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

Explanation used Terms

We always strive to make our data protection declaration as clear and understandable as possible. However, this is not always easy, especially when it comes to technical and legal issues. It often makes sense to use legal terms (such as personal data) or certain technical terms (such as cookies, IP address). But we don't want to use them without explanation. Below you will find an alphabetical list of important terms used that we may not have addressed sufficiently in the previous data protection declaration. If these terms were taken from the GDPR and they are definitions, we will also cite the GDPR texts here and add our own explanations if necessary.

Processor

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

Explanation: As a company and website owner, we are responsible for all data that we process from you. In addition to those responsible, there can also be so-called processors. This includes every company or person who processes personal data on our behalf. In addition to service providers such as tax consultants, processors can also include 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 voluntary, informed and unambiguous expression of the wishes of the data subject in the specific case, in the form of a statement or other unequivocal affirmative action, by which the data subject indicates that he or she consents to the processing of personal data concerning him or her agrees;*

Explanation: As a rule, such consent is given on websites via a cookie consent tool. You probably know that. Whenever you visit a website for the first time, you will usually be asked via a banner whether you agree to data processing. You can usually also make individual settings and decide for yourself which data processing you allow and which not. If you do not consent, no personal data about you may be processed. In principle, consent can of course also be given in writing, i.e. not via a tool.

Personal Data

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

*“**personal data**” means any information relating to an identified or identifiable natural person (hereinafter “data subject”); A natural person is considered to be identifiable if he or she 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 special characteristics that express the physical, physiological, genetic, psychological, 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 How approximately :

- Surname
- address
- E-mail address
- Postal address
- Telephone number

- birth date
- Identification numbers such as social security number, tax identification number, ID card number or matriculation number
- Bank details such as account number, credit information, account balances and much more.

According to the European Court of Justice (ECJ), your **IP address is also considered personal data** . Using your IP address, IT experts can at least determine the approximate location of your device and subsequently you as the connection owner. Therefore, storing an IP address also requires a legal basis within the meaning of the GDPR. There are also so-called **"special categories"** of personal data that are particularly worthy of protection. In addition to count :

- racial and ethnic Origin
- political Opinions
- religious or . ideological Beliefs
- union membership
- genetic data such as data collected from blood or saliva samples
- biometric data (this is information about psychological, physical or behavioral characteristics that can identify a person).
  Health data
- Data on sexual orientation or sex life

Profiling

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

*" **Profiling** " any type of automated processing of personal data, which consists in using that personal data to evaluate certain personal aspects relating to a natural person, in particular aspects relating to work performance, economic situation, health, personal Analyze or predict that natural person's preferences, interests, reliability, behavior, location or movements;*

Explanation: Profiling involves collecting various information about a person in order to learn more about that person. In the web sector , profiling is often used for advertising purposes or for credit checks. Web or advertising analysis programs, for example, collect data about your

behavior and interests on a website. This results in a special user profile that can be used to target advertising to a specific target group.

Responsible person

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

Explanation: In our case, we are responsible for the processing of your personal data and therefore the “controller”. If we pass on collected data to other service providers for processing, these are “ processors ”. To do this, an “order processing agreement (AVV)” must be signed.

processing

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

*“**Processing” means** any operation or series of operations carried out with or without the aid of automated procedures in connection with personal data, such as the collection, recording, organization, structuring, storage, adaptation or modification, reading, querying, use , disclosure by transmission, distribution or other form of making available, alignment or combination, restriction, deletion or destruction;*

Note: When we talk about processing in our privacy policy, we mean any type of data processing. As mentioned above in the original GDPR declaration, this includes not only collecting but also storing and processing data.

Final word

Congratulations! If you are reading these lines, you have actually “fought” your way through our entire privacy policy or at least scrolled this far. As you can see from the scope of our privacy policy, we do not take the protection of your personal data lightly.
It is important to us to inform you to the best of our knowledge and belief about the processing of personal data. We not only want to tell you which data is processed, but also explain the reasons for using various software programs. As a rule, data protection declarations sound very technical and legal. Since most of you are not web developers or lawyers, we wanted to take a different linguistic approach and explain the matter in simple and clear language. Of course, this is not always possible due to the subject matter. The most important terms are therefore explained in more detail at the end of the data protection declaration.
If you have any questions about data protection on our website, please do not hesitate to contact us or the responsible body. We wish you a wonderful time and hope to welcome you back to our website soon.

All texts are copyrighted.

Source: Created with AdSimple ’s Privacy Generator