

Imprint

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

Horse Tensegrity Training GmbH
Ebenedt 27,
4372 St. Georgen am Walde, Austria

Object of the company: Extended services

Registration number: Fn587683

UID number: ATU78556046

Commercial register court: Linz

Company headquarters: Ebenedt

Phone: +43 676 4076116

E-mail: office@horse-tensegrity-training.com

Managing Director

Christian Jantscher

Liability for the content of this website

We are constantly developing the content of this website and endeavor to provide correct and up-to-date information. Unfortunately, we cannot accept any liability for the accuracy of all content on this website, especially for that by third parties. As a service provider, we are not obliged to monitor the information transmitted or stored by you or to investigate circumstances that indicate illegal activity.

Our obligations to remove information or to block the use of information in accordance with the general laws due to judicial or official orders remain unaffected even in the case of our non-responsibility.

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

Liability for links on this website

Our website contains links to other websites for whose content we are not responsible. We are not liable for linked websites, as we had and have no knowledge of illegal activities, we have not noticed any such illegal activities and we would remove links immediately if we became aware of any illegal activities.

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

Copyright notice

All contents of this website (images, photos, texts, videos) are subject to copyright. Please ask us before distributing, reproducing or exploiting the content of this website, for example by republishing it on other websites. If necessary, we will the unauthorized use of parts of the contents of our website.

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

Picture credits

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

image rights are held by:

Horse Tensegrity Training GmbH

All texts are protected by copyright.

Source: Created with the [imprint generator](#) from AdSimple

Privacy policy

Table of contents

- [Introduction and overview](#)
- [Area of application](#)
- [Legal basis](#)
- [Contact details of the person responsible](#)
- [Storage duration](#)
- [Rights under the General Data Protection Regulation](#)
- [Security of data processing](#)
- [Communication](#)
- [Cookies](#)
- [Webhosting introduction](#)
- [Website modular systems Introduction](#)
- [Web Analytics Introduction](#)
- [Email marketing introduction](#)
- [Push messages Introduction](#)
- [Messenger & Communication Introduction](#)
- [Chatbots introduction](#)
- [Social media introduction](#)
- [Blogs and publication media Introduction](#)
- [Online Marketing Introduction](#)
- [Cookie Consent Management Platform Introduction](#)

- [Security & Anti-Spam](#)
- [Payment providers Introduction](#)
- [Audio & Video Introduction](#)
- [Video conferencing & streaming Introduction](#)
- [Survey and interview systems Introduction](#)
- [Evaluation platforms Introduction](#)
- [Online map services Introduction](#)
- [Content search providers Introduction](#)
- [Other Introduction](#)
- [Explanation of terms used](#)

Introduction and overview

We have prepared this privacy policy (version 22.07.2023-121963999) to explain to you, in accordance with the requirements of the [General Data Protection Regulation \(EU\) 2016/679](#) and applicable national laws, which personal data (data for short) we as the controller - and the processors commissioned by us (e.g. providers) - process, will process in the future and what lawful options you have. The terms used are to be understood as gender-neutral.

In short, we provide you with comprehensive information about the data we process about you.

Data protection declarations usually sound very technical and use legal jargon. This privacy policy, on the other hand, is intended to describe the most important things to you as simply and transparently as possible. Where it is conducive to transparency, technical **terms are explained in a reader-friendly way**, links to further information are provided and **graphics are used**. We thus inform you in clear and simple language that we only process personal data as part of our business activities if there is a corresponding legal basis. This is certainly not possible if we provide explanations that are as brief, unclear and legally technical as possible, as is often standard on the Internet when it comes to data protection. I hope you find the following explanations interesting and informative and perhaps there is one or two pieces of information that you did not yet know.

If still have any questions, please contact the responsible body named below or in the legal notice, follow the links provided and view further information on third-party websites. Our contact details can of course also be found in the legal notice.

Area of application

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

- all online presences (websites, online stores) that we operate
- Social media presence and e-mail communication
- Mobile apps for smartphones and other devices

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

Legal basis

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

As far as EU law is concerned, we refer to REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 27, 2016.

You can of course read up on the EU's General Data Protection Regulation online at EUR-Lex, the gateway to EU law, at <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32016R0679>.

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

1. **Consent** (Article 6(1)(a) GDPR): You have given us your consent to process data for a specific purpose. An example would be the storage of the data you entered in a contact form.
2. **Contract** (Article 6(1)(b) GDPR): 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(1)(c) GDPR): If we are subject to a legal obligation, we process your data. For example, we are legally obliged to keep invoices for accounting purposes. These usually contain personal data.
4. **Legitimate interests** (Article 6(1)(f) GDPR): In the case of legitimate interests that do not restrict your fundamental rights, we reserve the right to process personal data. For example, we need to process certain data in order to operate our website securely and efficiently. This processing is therefore a legitimate interest.

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

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

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

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

Contact details of the person responsible

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

Storage duration

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

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

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

Rights under the General Data Protection Regulation

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

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

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

short: You have rights - do not hesitate to contact the responsible office listed above!

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

Austria Data Protection Authority

Head: Dr. Andrea Jelinek

Address: Barichgasse 40-42, 1030 Vienna

Telephone no.: +43 1 52 152-0

E-mail address dsb@dsb.gv.at

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

Security of data processing

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

Art. 25 GDPR speaks here of "data protection by design and by default" and thus means that both software (e.g. forms) and hardware (e.g. access to the server room) should always be designed with security in mind and appropriate measures should be taken. If necessary, we will discuss specific measures below.

TLS encryption with https

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

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

We have thus introduced an additional layer of security and comply with data protection by design ([Article 25\(1\) GDPR](#)). By using TLS (Transport Layer Security), an encryption protocol for secure data transmission on the internet, we can ensure the protection of confidential data.

You can recognize the use of this data transmission protection by the small lock symbol at the top left of the browser, to the left of the Internet address (e.g. examplepage.com) and the use of the https scheme (instead of http) as part of our Internet address.

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

Communication

Communication Summary

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

Processed data: e.g. telephone number, name, email address, form data entered.

You can find more details on this in the respective contact type used

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

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

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

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

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

Affected persons

All those who seek contact with us via the communication channels provided by us are affected by the aforementioned processes.

Telephone

When you call us, the call data is stored pseudonymously on the respective end device and with the telecommunications provider used. In addition, data such as name and telephone number may subsequently be sent by e-mail and stored for the purpose of responding to inquiries. The data will be deleted as soon as the business case has been completed and legal requirements permit.

e-mail

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

Online forms

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

Legal basis

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

- Art. 6 para. 1 lit. a GDPR (consent): You give us your consent to store your data and to use it for purposes relating to the business transaction;
- Art. 6 para. 1 lit. b GDPR (contract): It is necessary for the performance of a contract with you or a processor, such as the telephone provider, or we need to process the data for pre-contractual activities, such as the preparation of an offer;
- Art. 6 para. 1 lit. f GDPR (legitimate interests): We want to handle customer inquiries and business communication in a professional manner. This requires certain technical facilities such as e-mail programs, exchange servers and mobile network operators in order to operate communication efficiently.

Cookies

Cookies summary

Affected parties: Visitors to the website

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

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

Storage period: depending on the cookie, can vary from hours to years
Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit.f GDPR
(legitimate interests)

What are cookies?

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

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

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

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

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

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

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

Cookie data can look like this, for example:

Name: _ga

Wert: GA1.2.1326744211.152121963999-9

Intended use: Differentiation of website visitors

Expiration date: after 2 years

A browser should be able to support these minimum sizes:

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

What types of cookies are there?

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

A distinction can be made between 4 types of cookies:

Essential cookies

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

Purposeful cookies

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

Targeted cookies

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

Advertising cookies

These cookies are also known as targeting cookies. They are used to deliver customized advertising to the user. This can be very practical, but also very annoying.

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

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

Purpose of processing via cookies

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

What data is processed?

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

Storage duration of cookies

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

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

Right to object - how can I delete cookies?

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

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

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

[Safari: Managing cookies and website data with Safari](#)

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

[Internet Explorer: Deleting and managing cookies](#)

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

If you generally do not want to have cookies, you can set up your browser so that it always informs you when a cookie is to be set. You can then decide for each individual cookie whether or not to allow it. The procedure differs depending on the browser. It is best to search for the instructions in Google using the search term "delete cookies Chrome" or "deactivate cookies Chrome" in the case of a Chrome browser.

Legal basis

The so-called "Cookie Guidelines" have been in place since 2009. These state that the storage of cookies requires your **consent** (Article 6(1)(a) GDPR). However, there are still very different reactions to these directives within the EU countries. In Austria, however, this directive has been implemented in Section 96 (3) of the Telecommunications Act (TKG). In Germany, the cookie directives have not been implemented as national law. Instead, this directive was largely implemented in Section 15 (3) of the Telemedia Act (TMG).

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

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

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

Webhosting introduction

Web hosting summary

Affected parties: Visitors to the website

Purpose: professional hosting of the website and securing its operation

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

Storage period: depending on the respective provider, but usually 2 weeks

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

What is web hosting?

When you visit websites these days, certain information - including personal data - is automatically created and stored, including on this website. This data should be processed as sparingly as possible and only with justification. By website, by the way, we mean the entirety of all web pages on a domain, i.e. everything from

from the start page (homepage) to the very last subpage (like this one). By domain we mean, for example, example.de or example.com.

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

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

When the browser on your computer (desktop, laptop, tablet or smartphone) connects and during data transfer to and from the web server, personal data may be processed. On the one hand, your computer stores data; on the other hand, the web server must also store data for a certain period of time in order to ensure proper operation.

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

Why do we process personal data?

The purposes of data processing are:

1. Professional website hosting and operational security
2. to maintain operational and IT security
3. Anonymous evaluation of access behavior to improve our offer and, if necessary, for criminal prosecution or prosecution of claims

What data is processed?

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

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

How long is data stored?

As a rule, the above-mentioned data is stored for two weeks and then automatically deleted. We do not pass this data on, but we cannot rule out the possibility of this data being viewed by the authorities in the event of unlawful conduct.

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

Legal basis

The lawfulness of the processing of personal data in the context of web hosting results from Art. 6 para. 1 lit. f GDPR (protection of legitimate interests), because the use of professional hosting with a provider is necessary in order to present the company securely and user-friendly on the Internet and to be able to pursue attacks and claims from this if necessary.

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

Website modular systems Introduction

Website builder systems Privacy policy summary

Affected parties: Visitors to the website

Purpose: Optimization of our service performance

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

Storage duration: depends on the provider

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

What are website builder systems?

We use a modular website system for our website. Modular systems are special forms of a content management system (CMS). With a modular system, website operators can create a website very easily and without programming knowledge. In many cases, web hosts also offer modular systems. By using a modular system, your personal data can also be collected, stored and processed. In this data protection text, we provide you with general information about data processing by modular systems. You can find more detailed information in the provider's data protection declarations.

Why do we use website builder systems for our website?

The biggest advantage of a modular system is its ease of use. We want to offer you a clear, simple and well-organized website that we can easily operate and maintain ourselves - without external support. A modular system now offers many helpful functions that we can use even without programming knowledge. This allows us to design our web presence according to our wishes and offer you an informative and enjoyable time on our website.

What data is stored by a modular system?

Exactly which data is stored depends, of course, on the website builder system used. Each provider processes and collects different data from the website visitor. As a rule, however, technical usage information such as operating system, browser, screen resolution, language and keyboard settings, hosting provider and the date of your website visit are collected. Tracking data (e.g. browser activity, clickstream activity, session heatmaps, etc.) may also be processed. Personal data may also be collected and stored. This usually involves contact data such as email address, telephone number (if you have provided this), IP address and geographical location data. You can find out exactly which data is stored in the provider's privacy policy.

How long and where is the data stored?

We will inform you about the duration of data processing below in connection with the website building block system used, if we have further information on this. You can find detailed information about this in the provider's privacy policy. In general, we only process personal data for as long as absolutely necessary for the provision of our services and products. The provider may store your data according to its own specifications, over which we have no influence.

Right of objection

You always have the right to information, correction and deletion of your personal data. If you have any questions, you can also contact the person responsible for the website builder system used at any time. Contact details can be found either in our privacy policy or on the website of the relevant provider.

You can delete, deactivate or manage cookies that providers use for their functions in your browser. Depending on which browser you use, this works in different ways. Please note, however, that not all functions may then work as usual.

Legal basis

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

Insofar as the processing of data is not absolutely necessary for the operation of the website, the data will only be processed on the basis of your consent. This applies in particular to tracking activities. The legal basis in this respect is Art. 6 para. 1 lit. a GDPR.

In this privacy policy, we have provided you with the most important general information about data processing. If you would like more detailed information in this regard, you will find further information - if available - in the following section or in the provider's privacy policy.

Web Analytics Introduction

Web Analytics privacy policy summary

Affected parties: Visitors to the website

Purpose: Evaluation of visitor information to optimize the website.

Processed data: Access statistics that contain data such as access locations, device data, access duration and time, navigation behavior, click behavior and IP addresses.

You can find more details on this in the respective web analytics tool used.

Storage duration: depending on the web analytics tool used

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

What is web analytics?

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

Why do we use web analytics?

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

What data is processed?

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

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

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

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

Duration of data processing

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

Right of objection

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

Legal basis

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

In addition to consent, we have a legitimate interest in analyzing the behavior of website visitors in order to improve our offer technically and economically. With the help of web analytics, we can detect errors on the website, identify attacks and improve efficiency. The legal basis for this is **Art. 6 para. 1 lit. f GDPR (legitimate interests)**. Nevertheless, we only use the tools if you have given your consent.

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

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

Facebook Conversions API privacy policy

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

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

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

The Facebook data processing conditions, which correspond 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 Conversions API in the privacy policy at <https://www.facebook.com/about/privacy>

Google Analytics privacy policy

Google Analytics privacy policy summary

Affected parties: Visitors to the website

Purpose: Evaluation of visitor information to optimize the website.

Processed data: Access statistics containing data such as access locations, device data, access duration and time, navigation behavior and click behavior. More details can be found below in this privacy policy.

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

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

What is Google Analytics?

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

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

Google Analytics is a tracking tool that is used to analyze the traffic on our website. These measurements and analyses are based on a pseudonymous user identification number. This number does not contain any personal data such as name or address, but is used to assign events to an end device. GA4 uses an event-based model that records detailed information on user interactions such as page views, clicks, scrolling and conversion events. GA4 also incorporates various machine learning functions to better understand user behavior and certain trends. GA4 relies on modeling with the help of machine learning functions. This means that missing data can also be extrapolated on the basis of the collected data in order to optimize the analysis and also to be able to make forecasts.

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

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

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

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

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

- Event-based data model: This model captures very specific events that can take place on our website. For example, playing a video, purchasing a product or subscribing to our newsletter.
- Extended analysis functions: These functions allow us to better understand your behavior on our website or certain general trends. For example, we can segment user groups, carry out comparative analyses of target groups or track your path on our website.
- Predictive modeling: Based on collected data, missing data can be extrapolated using machine learning to predict future events and trends. This can help us to develop better marketing strategies.
- Cross-platform analysis: Data can be collected and analyzed from both websites and apps. This gives us the opportunity to analyze user behavior across platforms, provided you have of course consented to data processing.

Why do we use Google Analytics on our website?

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

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

What data is stored by Google Analytics?

Google Analytics uses a tracking code to create a random, unique ID that is linked to your browser cookie. This is how Google Analytics recognizes you as a new user and you are assigned a user ID. The next time you visit our site, you will be 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 standard for every newly created property. Depending on the property used, data is stored for different lengths of time.

Through identifiers such as cookies, app instance IDs, user IDs or user-defined event parameters, your interactions are measured across platforms if you have given your consent. Interactions are all types of actions that you perform on our website. If you also use other Google systems (such as a Google account), data generated via Google Analytics may be linked to third-party cookies. Google does not pass on any Google Analytics data unless we as the website operator authorize this. Exceptions may be made if required by law.

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

Since Google Analytics 4 focuses event-based data, the tool uses significantly fewer cookies compared to previous versions (such as Google Universal Analytics). Nevertheless, there are some specific cookies that are used by GA4. These include, for example:

Name: `_ga`

Wert: 2.1326744211.152121963999-5

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

Expiration date: after 2 years

Name: `_gid`

Wert: 2.1687193234.152121963999-1

Purpose: The cookie is also used to distinguish website visitors

Expiration date: after 24 hours

Name: `_gat_gtag_UA_<property-id>`

Value: 1

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

Expiration date: after 1 minute

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

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

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

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

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

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

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

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

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

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

How long and where is the data stored?

Google has distributed its servers all over the world. Here you can read exactly where the Google data centers are located:

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

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

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

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

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

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

How can I delete my data or prevent data storage?

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

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

Legal basis

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

In addition to consent, we have a legitimate interest in analyzing the behavior of website visitors in order to improve our offer technically and economically. With the help of Google Analytics, we recognize errors on the website, can identify attacks and improve efficiency. The legal basis for this is **Art. 6 para. 1 lit. f GDPR (legitimate interests)**. Nevertheless, we only use Google Analytics if you have given your consent.

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

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

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

We hope we have been able to provide you with the most important information about data processing by Google Analytics. If you would like to learn 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 data processing, use the Google privacy policy at <https://policies.google.com/privacy?hl=de>.

Google Analytics reports on demographic characteristics and interests

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

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

Google Analytics IP anonymization

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

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

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

Google uses so-called standard contractual clauses (= Art. 46. para. 2 and 3 GDPR) 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 to these countries. Standard contractual clauses (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 and stored in third countries (such as the USA). Through these clauses, Google undertakes to comply with the European level of data protection when processing your relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the decision and the corresponding standard contractual clauses here, among other places: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=en

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 through the use of Google Optimize in the privacy policy at <https://policies.google.com/privacy?hl=de>.

Google Site Kit Privacy Policy

Google Site Kit Privacy Policy Summary

Data subject: Visitors to the website

Purpose: Evaluation of visitor information to optimize the website.

Processed data: Access statistics containing data such as locations of access, device data, access duration and time, navigation behavior, click behavior and IP addresses. More details can be found below and in the

Privacy policy of Google Analytics.

Storage duration: depending on the properties used

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

What is Google Site Kit?

We have integrated the WordPress plugin Google Site Kit from the American company Google Inc. into our website. For the European area, the company Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services. With Google Site Kit, we can quickly and easily view statistics from various Google products such as Google Analytics directly in our WordPress dashboard. The tool or the tools integrated into Google Site Kit also collect personal data from you, among other things. In this privacy policy, we explain why we use Google Site Kit, how long and where data is stored and which other data protection texts are relevant for you in this context.

Google Site Kit is a plugin for the WordPress content management system. With this plugin, we can view important website analysis statistics directly in our dashboard. These are statistics that are collected by other Google products. First and foremost Google Analytics. In addition to Google Analytics, the

services Google Search Console, Page Speed Insight, Google AdSense, Google Optimize and Google Tag Manager can be linked to Google Site Kit.

Why do we use Google Site Kit on our website?

As a service provider, it is our job to offer you the best possible experience on our website. We want you to feel comfortable on our website and find exactly what you are looking for quickly and easily. Statistical evaluations help us to get to know you better and to adapt our offer to your wishes and interests. We use various Google tools for these evaluations. Site Kit makes our work much easier in this respect because we can view and analyze the statistics of Google products directly in the dashboard. We no longer have to register for the respective tool separately. Site Kit therefore always provides a good overview of the most important analysis data.

What data is stored by Google Site Kit?

If you have actively consented to tracking tools in the cookie notice (also called script or banner), Google products such as Google Analytics will set cookies and send data from you, for example about your user behavior, to Google, where it will be stored and processed. This also includes storing personal data such as your IP address.

For more detailed information on the individual services, we have separate text sections in this privacy policy. For example, take a look at our privacy policy for Google Analytics. Here we go into great detail about the data collected. You can find out how long Google Analytics stores, manages and processes data, which cookies may be used and how you can prevent data storage. We also have separate privacy policies with comprehensive information for other Google services such as Google Tag Manager and Google AdSense.

Below we show you examples of Google Analytics cookies that can be set in your browser if you have consented to data processing by Google. Please note that these cookies are only a selection:

Name: _ga

Wert:2.1326744211.152121963999-2

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

Expiration date: after 2 years

Name: _gid

Wert:2.1687193234.152121963999-7

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

Expiration date: after 24 hours

Name: _gat_gtag_UA_<property-id>

Value: 1

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

Expiration date: after 1 minute

How long and where is the data stored?

Google stores collected data on its own Google servers, which are distributed worldwide. Most of the servers are located in the United States and it is therefore easily possible that your data is also stored there. At <https://www.google.com/about/datacenters/locations/?hl=de> you can see exactly where the company provides servers.

Data collected by Google Analytics is stored for a standardized period of 26 months. Your user data will then be deleted. The retention period applies to all data linked to cookies, user recognition and advertising IDs.

How can I delete my data or prevent data storage?

You always have the right to receive information about your data and to have your data deleted, corrected or restricted. You can also deactivate, delete or manage cookies in your browser at any time.

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

Legal basis

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

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

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

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

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

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

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

Email marketing introduction

Email marketing summary

Affected parties: Newsletter subscribers

Purpose: Direct advertising by e-mail, notification of system-relevant events

Processed data: Data entered during registration, but at least the e-mail address. You can find more details on this in the respective email marketing tool used.

Storage period: Duration of the subscription

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

What is email marketing?

In order to keep you up to date, we also use the option of e-mail marketing. If you have agreed to receive our e-mails or newsletters, your data will also be processed and stored. E-mail marketing is a sub-area of online marketing. It involves sending news or general information about a company, products or services by e-mail to a specific group of people who are interested in them.

If you want to take part in our e-mail marketing (usually by newsletter), you normally just need to register with your e-mail address. To do this, you fill out an online form and send it off. However, we may also ask you to provide your title and name so that we can write to you personally.

Basically, the registration for newsletters works with the help of the so-called "double opt-in procedure". After you have registered for our newsletter on our website, you will receive an e-mail confirming your newsletter registration. This ensures that the e-mail address belongs to you and that no one has registered with a third-party e-mail address. We or a notification tool used by us logs each individual registration. This is necessary so that we can prove that the registration process is legally correct. As a rule, the time of registration, the time of registration confirmation and your IP address are recorded.

saved. In addition, it is also logged when you make changes to your saved data.

Why do we use email marketing?

We naturally want to stay in contact with you and always present you with the most important news about our company. To do this, we use email marketing - often just referred to as "newsletters" - as an essential part of our online marketing. If you agree to this or if it is permitted by law, we will send you newsletters, system e-mails or other notifications by e-mail. When we use the term "newsletter" in the following text, we mainly mean regularly sent e-mails. Of course, we do not want to bother you in any way with our newsletters. That is why we always endeavor to offer only relevant and interesting content. For example, you can find out more about our company, our services or products. As we are constantly offering our offers, you will always find out via our newsletter when there is news or when we are offering special, lucrative promotions. If we commission a service provider who offers a professional mailing tool for our email marketing, we do so in order to be able to offer you fast and secure newsletters. The purpose of our email marketing is basically to inform you about new offers and also to achieve our business goals.

What data is processed?

If you become a subscriber to our newsletter via our website, you confirm your membership of an e-mail list by e-mail. In addition to your IP address and e-mail address, your title, name, address and telephone number may also be stored.

However, only if you agree to this data storage. The data marked as such is necessary so that you can participate in the service offered. Providing this data is voluntary, but failure to provide it will mean that you will not be able to use the service.

In addition, information about your device or your preferred content on our website may also be stored. You can find out more about the storage of data when you visit a website in the section "Automatic data storage". We record your declaration of consent so that we can always prove that it complies with our laws.

Duration of data processing

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

However, if you confirm that you have given us your consent to the newsletter registration, you can submit an individual deletion request at any time. If you permanently revoke your consent, we have the right to store your e-mail address in a blacklist. As long as you have voluntarily subscribed to our newsletter, we will of course retain your e-mail address.

Right of objection

You can cancel your newsletter subscription at any time. All you have to do is withdraw your consent to the newsletter subscription. This usually only takes a few seconds or one or two clicks. You will usually find a link to cancel your newsletter subscription at the end of every email. If really cannot find the link in the newsletter, please contact us by e-mail and we cancel your newsletter subscription immediately.

Legal basis

Our newsletter is sent on the basis of your consent (Article 6(1)(a) GDPR). This means that we may only send you a newsletter if you have actively subscribed to it beforehand. We may also send you advertising messages if you have become our customer and have not objected to the use of your email address for direct advertising.

Information on specific email marketing services and how they process personal data, if available, can be found in the following sections.

Push messages Introduction

Push message summary

Affected: Push message subscribers

Purpose: Notification of system-relevant and interesting events

Processed data: Data entered during registration, usually also location data.

You can find more details on this in the respective push message tool used.

Storage duration: Data is usually stored for as long as is necessary to provide the services.

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

What are push notifications?

We also use so-called push notification services on our website, with which we can keep our users up to date at all times. This means that if you have consented to the use of such push notifications, we can send you short news items with the help of a software tool. Push notifications are a form of text message that appears directly on your smartphone or other devices such as tablets or PCs if you have registered for them. You will also receive these messages if you are not on our website or are not actively using our services. Data about your location and your usage behavior may also be collected and stored.

Why do we use push notifications?

On the one hand, we use push notifications in order to be able to fully provide the services that we have contractually agreed with you. On the other hand, the messages also serve our online marketing. We can use these messages to inform you about our

service or our products. Especially when there news in our company, we can you immediately. We want to get to know the preferences and habits of all our users as well as possible in order to continuously improve our offer.

What data is processed?

In order to receive push messages, you must also confirm that you wish to receive these messages. The data collected during the consent process is also stored, managed and processed. This is necessary so that it can be proven and recognized that a user has agreed to receive the push messages. A so-called device token or push token is stored in your browser for this purpose. The data of your location or the location of the end device you are using is usually also stored.

To ensure that we always send interesting and important push messages, we also statistically evaluate how the messages are handled. This allows us to see, for example, whether and when you open the message. With the help of these findings, we can adapt our communication strategy to your wishes and interests. Although this stored data can be assigned to you, we do not want to check you as an individual. Rather, we are interested in the data collected from all our users so that we make optimizations. You can find out exactly which data is stored in the data protection declarations of the respective service providers.

Duration of data processing

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

Legal basis

It may also be that the push notifications are necessary so that certain obligations contained in a contract can be fulfilled. For example, so that we can inform you of technical or organizational news. Then the legal basis is Art. 6 para. 1 lit. b GDPR.

If this is not the case, the push messages will only be sent on the basis of your consent. In particular, our push messages may have advertising content. The push messages can also be sent depending on your location, which your end device displays. The above-mentioned analytical evaluations are also based on your consent to receive such messages.

The legal basis in this respect is Art. 6 para. 1 lit. a GDPR. You can of course withdraw your consent or change various settings at any time in the settings.

Messenger & Communication Introduction

Messenger & Communication Privacy policy summary

Data subject: Visitors to the website

Purpose: Contact requests and general communication between us and you

Processed data: Data such as name, address, e-mail address, telephone number, general content data, IP address if applicable

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

Storage duration: depending on the messenger & communication functions used

Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests), Art. 6 para. 1 sentence 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 and contact forms, email, telephone) for communicating with us. Your data will also be processed and stored to the extent necessary to answer your request and our subsequent actions.

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

Why do we use messenger & communication functions?

Communication options with you are of great importance to us. After all, we want to talk to you and answer all possible questions 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 prefer at any time. In exceptional cases, however, we may not be able to answer certain questions via chat or messenger. This the case, for example, when it comes to internal contractual matters. In this case, we recommend other communication options such as e-mail or telephone.

As a rule, we that we remain responsible under data protection law, even if we use the services of a social media platform. The European Court of Justice has

However, we have decided that in certain cases the operator of the social media platform may be jointly responsible with us within the meaning of Art. 26 GDPR. If this is the case, we will this out separately and work on the basis of an agreement to this effect. The essence of the agreement is set out below for the platform concerned.

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.

As a result, you may no longer be able to claim or enforce your rights in relation to your personal data as easily.

What data is processed?

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

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 privacy policies of the providers usually state exactly which data is stored and processed and for how long. In principle, personal data is only processed for as long as is necessary for the provision of our services. If data is stored in cookies, the storage period varies greatly. The data can be deleted immediately after leaving a website, but it can also remain stored for several years. You should therefore look at each individual cookie in detail if you want to know more about data storage. In most cases, you will also find informative information about the individual cookies in the data protection declarations of the individual providers.

Right of objection

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

As cookies may be used for messenger & communication functions, we also recommend that you read our general privacy policy on cookies. In order to

to find out exactly which of your data stored and processed, you should read the data protection declarations of the respective tools.

Legal basis

If you have consented to your data being processed and stored by integrated messenger & communication functions, this consent is the legal basis for data processing (**Art. 6 para. 1 lit. a GDPR**). We process your request and manage your data in the context of contractual or pre-contractual relationships in order to fulfill our pre-contractual and contractual obligations or to answer inquiries. The basis for this is **Art. 6 para. 1 sentence 1 lit. b. 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 fast and good communication with you or other customers and business partners if you have given your consent.

Chatbots introduction

Chatbots privacy policy summary

Affected parties: Visitors to the website

Purpose: Contact requests and general communication between us and you

Processed data: Data such as name, address, e-mail address, telephone number, general content data, IP address if applicable

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

Storage duration: depending on the chatbots & chat functions used

Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests), Art. 6 para. 1 sentence 1 lit. b. GDPR (contractual or pre-contractual obligations)

What are chatbots?

You can also communicate with us via chatbots or similar chat functions. A chat offers the opportunity to write or speak to each other with very little delay. A chatbot is a piece of software that attempts to answer your question and informs you of any news. By using these means of communication, your personal data may also be processed and stored.

Why do we use chatbots?

Communication options with you are important to us. After all, we want to talk to you and answer all possible questions about our service in the best possible way. Well-functioning communication is an important part of our service.

Chatbots have the great advantage that we can answer frequently asked questions automatically with the help of this software. This saves us time and you still receive detailed and helpful answers. If the chatbot is unable to help, you can of course contact us in person at any time.

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

What data is processed?

You may also use the chat services on other websites/platforms. In this case, your user ID will also be stored on the servers of this website. We may also be informed about which user has used the chat and when. The content is also stored. Exactly which data is stored depends on the respective service. As a rule, however, it is contact data such as e-mail address or telephone number, IP address and various usage data.

If you have consented to the chat function being used, this consent and any registration will also be saved or logged. We do this that we can prove the registration or consent if this is required by law.

The provider of a chat platform can also find out when you chat and also receives technical information about the device you are using. Exactly what information is stored and processed also depends on your PC settings. In many cases, for example, data on your approximate location can be collected. This is done on the one hand to optimize the chat services and on the other hand to ensure greater security. Furthermore, the information can also be used to set personalized advertising and marketing measures.

If you have agreed that a chatbot can send you messages, you can of course deactivate this activation at any time. The chatbot also serves as an aid here and shows you how to unsubscribe from this function. All your data in this regard will then be deleted from the recipient directory.

We use the above-mentioned data to be able to address you personally via the chat, for example, to answer your questions and inquiries or to send you possible content. It also enables us to fundamentally improve our chat services.

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 privacy policies of the providers usually state exactly which data is stored and processed and for how long. In principle, personal data is only processed for as long as is necessary for the provision of our services. If data is stored in cookies, the storage period varies greatly. The data can be deleted immediately after leaving a website, but it can also remain stored for several years. You should therefore look at each individual cookie in detail if you want to know more about data storage. In most cases, you will also find informative information about the individual cookies in the data protection declarations of the individual providers.

Right of objection

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

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

Legal basis

We use a pop-up window to ask for your permission to process your data as part of the chat services. If you consent, this consent also serves as the legal basis (**Art. 6 para. 1 lit. a GDPR**) for data processing. In addition, we process your inquiries and manage your data in the context of contractual or pre-contractual relationships in order to fulfill our pre-contractual and contractual obligations or to answer inquiries. The basis for this is **Art. 6 para. 1 sentence 1 lit. b. GDPR**. In principle, your data is also stored and processed on the basis of our legitimate interest (**Art. 6 para. 1 lit. f GDPR**) in fast and good communication with you or other customers and business partners. Nevertheless, we only use the tools if you have given your consent.

LiveChat privacy policy

We use the chat software LiveChat for our website. The service provider is the American company LiveChat Inc, 101 Arch Street, 8th Floor, Boston MA 02110, USA.

What is LiveChat?

This tool allows us to communicate with you via a chat interface. LiveChat can be used on both websites and mobile applications and offers you and us a user-friendly platform for marketing measures, customer support and sales. Many other platforms and tools such as project management or CRM systems, can also be integrated. According to the company, great importance is also attached to security and data protection.

Why do we use LiveChat?

We have opted for LiveChat because the protection of personal data is important to us. Via LiveChat you can ask us questions, solve problems or get general information about our services or products very quickly and easily. The user interface is easy to use and the support team is on hand to answer any questions quickly.

How secure is data transfer with LiveChat?

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

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

Further information on the standard contractual clauses at LiveChat can be found at <https://.www.livechat.com/legal/gdpr-faq/>

You can find out more about the data that is processed through the use of LiveChat in the privacy policy at <https://.www.livechat.com/legal/privacy-policy/>

Social media introduction

Social media privacy policy summary

Data subject: Visitors to the website

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

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

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

Storage duration: depending on the social media platforms used

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

What is social media?

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

Why do we use social media?

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

The data that is stored and processed through your use of a social media channel is primarily for the purpose of carrying out web analyses. The aim of these analyses is to be able to develop more precise and personalized marketing and advertising strategies. Depending on your behavior on a social media platform, the evaluated data can be used to draw conclusions about your interests and create user profiles. This also enables the platforms to present you with customized advertisements. Cookies are usually set in your browser for this purpose, which store data on your usage behavior.

As a rule, we remain responsible under data protection law, even if we use the services of a social media platform. However, the European Court of Justice has ruled that in certain cases the operator of the social media platform may be jointly responsible with us within the meaning of Art. 26 GDPR.

If this is the case, we will point this out separately and work on the basis of an agreement to this effect. The essence of the agreement is then set out below for the platform concerned.

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

What data is processed?

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

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

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

Duration of data processing

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

Right of objection

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

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

Legal basis

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

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

Facebook privacy policy

Facebook privacy policy summary

Data subject: Visitors to the website

Purpose: Optimization of our service performance

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

You can find more details below in the privacy policy.

Storage period: until the data is no longer useful for Facebook's purposes

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

What are Facebook tools?

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

If data is collected and forwarded from you via our embedded Facebook elements or via our Facebook page (fan page), both we and Facebook Ireland Ltd. are responsible for this. Facebook is solely responsible for the further processing of this data. Our joint obligations have also been set out in a publicly accessible agreement at https://www.facebook.com/legal/controller_addendum. This, 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 securely integrated into our website in accordance with data protection law. Facebook, on the other hand, is responsible for the data security of Facebook products, for example. If you have any questions about data collection and data processing by Facebook, you can contact the company directly. If you address the question to us, we are obliged to forward it to Facebook.

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

In addition to many other products, Facebook also offers the so-called "Facebook Business Tools". This is the official name of Facebook. However, as the term is hardly known, we have decided to simply call them Facebook tools.

These include, among others:

- Facebook pixel
- social plug-ins (such as the "" or "Share" button)
- Facebook Login
- Account Kit
- APIs (programming interface)
- SDKs (collection of programming tools)
- Platform integrations
- Plugins
- Codes
- Specifications
- Documentations
- Technologies and services

Through these tools, Facebook expands services and has the ability to obtain information about user activity outside of Facebook.

Why do we use Facebook tools on our website?

We only want to show our services and products to people who are really interested in them. With the help of advertisements (Facebook ads), we can reach precisely these people. However, Facebook needs information about people's wishes and needs in order to show users suitable advertising. The company is therefore provided with information about user behavior (and contact details) on our website. As a result, Facebook collects better user data and can show interested people suitable advertising about our products or services. The tools thus enable customized advertising campaigns on Facebook.

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

What data is stored by Facebook tools?

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

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

In addition to the contact data, "event data" is also transmitted. "Event data" refers to the information that we receive about you on our website. For example, which subpages you visit or which products you buy from us. Facebook does not share the information it receives with third parties (such as advertisers) unless the company has explicit permission or is legally obliged to do so. "Event data" can also be linked to contact details. This allows Facebook to offer better personalized advertising. After the aforementioned matching process, Facebook deletes the contact data again.

In order to deliver optimized ads, Facebook only uses the event data if it has been combined with other data (collected by Facebook in other ways). Facebook also uses this event data for security, protection, development and research purposes. Much of this data is transferred to Facebook via cookies. Cookies are small text files that are used to store data or

information is used in browsers. On the tools used and whether you are a Facebook member, different numbers of cookies are stored in your browser.

browser. We go into more detail about individual Facebook cookies in the descriptions of the individual Facebook tools. You can also find general information about the use of Facebook cookies at <https://www.facebook.com/policies/cookies>

How long and where is the data stored?

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

How can I delete my data or prevent data storage?

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

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

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

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

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

Legal basis

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

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

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

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

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

Facebook Login Privacy Policy

We have integrated the practical Facebook login on our site. This allows you to easily log in 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 Facebook social media network. There you can log in using your Facebook user data. Through this login procedure, data about you or your user behavior is stored and transmitted to Facebook.

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

Name: fr

Value: 0jiejh4c2GnlufEJ9..Bde09j...1.0.Bde09j

Purpose: This cookie is used to ensure that the social plugin on our website works as well as possible.

Expiration date: after 3 months

Name: datr

Wert: 4Jh7XUA2121963999SEmPsSfzCOO4JFFI

Intended use: Facebook sets the "datr" cookie when a web browser accesses facebook.com, and the cookie helps to identify login activity and track the

protect users.

Expiration 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.

Expiration date: after the end of the session

Note: The cookies listed are only a small selection of the cookies to Facebook. Other cookies are, for example, _fbp, sb or wd. A complete list is not possible, as Facebook has a large number of cookies and uses them variably.

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

- Your Facebook name
- Your profile picture
- a registered e-mail address
- Friends lists
- Button details (e.g. "" button)
- Birthday date
- Language
- Place of residence

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

By using Facebook Login, you consent to data processing. You can revoke this agreement at any time. If you would like more information about data processing by Facebook, we recommend that you read the Facebook privacy policy at <https://www.facebook.com/privacy/policy/>

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

Facebook social plug-ins privacy policy

Social plug-ins from Meta Platforms Inc. are integrated 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 plug-in is a small part of Facebook that is integrated into our site. Each plug-in has its own function. The most commonly used functions are the familiar "Like" and "Share" buttons.

The following social plug-ins are offered by Facebook:

- "Save" button
- "Like" button, share, send and quote
- Page plug-in
- Comments
- Messenger plug-in
- Embedded contributions and video player
- Group plug-in

You can find more information on how the individual plug-ins are used at <https://developers.facebook.com/docs/plugins>. We use the social plug-ins on the one hand to offer you a better user experience on our site, and on the other hand because Facebook can optimize our advertisements as a result.

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, 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 is 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.

To prevent Facebook from collecting a lot of data during your visit to our website and linking it to Facebook data, you must log out of Facebook during your visit to the website.

If you are not logged in to Facebook or do not have a Facebook account, your browser will send less information to Facebook because you have fewer Facebook cookies. Nevertheless, data such as your IP address or which website you visit may be transmitted to Facebook. We would like to expressly out that we do not the exact content of the data. However, to the best of our current knowledge, we try to inform you as much as possible about the data processing. You can also find out how Facebook uses the data in the company's data policy at <https://www.facebook.com/about/privacy/update>.

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

Name: dpr

Value: not specified

Purpose: This cookie is used to make the social plug-ins on our website work.

Expiration date: after the end of the session

Name: fr

Wert: 0jiejy4121963999c2GnlufEJ9..Bde09j...1.0.Bde09j

Intended use: The cookie is also necessary for the plug-ins to function properly.

Expiration 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 settings for advertisements yourself at <https://www.facebook.com/adpreferences/advertisers/> . If you are not a Facebook user, you can manage your usage-based online advertising at <https://www.youronlinechoices.com/de/praeferenzmanagement/?tid=121963999> . There you have the option of deactivating or activating providers.

If you want to find out more about Facebook's data protection, we recommend that you read the company's own data policy at <https://www.facebook.com/privacy/policy/>

Instagram privacy policy

Instagram privacy policy summary

Data subject: Visitors to the website

Purpose: Optimization of our service performance

Processes data: Data such as user behavior data, information on your device and your IP address.

You can find more details below in the privacy policy.

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

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

What is Instagram?

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

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

Instagram is one of the best-known social media networks in the world. Instagram combines the advantages of a blog with the benefits of audiovisual platforms such as YouTube or Vimeo. You can post on "Insta" (as many users casually call the platform).

upload photos and short videos, edit them with various filters and share them on other social networks. And if you don't want to be active yourself, you can also just follow other interesting users.

Why do we use Instagram on our website?

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

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

What data is stored by Instagram?

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

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

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

We assume that Instagram processes data in the same way as Facebook. This means that if you have an Instagram account or have visited www.instagram.com, Instagram has at least set a cookie. If this is the case, your browser sends information to Instagram via the cookie as soon as you come into contact with an Instagram function. This data is deleted or anonymized after 90 days at the latest (after reconciliation). Although we deal intensively with the data processing of

Instagram, 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 image). In our test, we assume that you do not have an Instagram account. If you are logged in to Instagram, significantly more cookies will of course be in your browser.

These cookies were used in our test:

Name: csrftoken

Value: ""

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

Expiration date: after one year

Name: mid

Value: ""

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

Expiration date: after the end of the session

Name: fbsr_121963999124024

Value: not specified

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

Expiration date: after the end of the session

Name: rur

Value: ATN

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

Expiration date: after the end of the session

Name: urlgen

Wert: “{”194.96.75.33”: 1901}:1iEtYv:Y833k2_UjKvXgYe121963999”

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

Expiration date: after the end of the session

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

How long and where is the data stored?

Instagram shares the information received between the Facebook companies with external partners and with people you connect with worldwide. Data processing is carried out in compliance with our own data policy. Your data is, under

Facebook servers the world for security reasons, among others. Most of these servers are located in the USA.

How can I delete my data or prevent data storage?

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

And this is how deleting your Instagram account works:

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

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

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

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

Legal basis

If you have consented to your data being processed and stored by integrated social media elements, this consent is the legal basis for data processing (**Art. 6 para. 1 lit. a GDPR**). In principle, your data is also stored and processed on the basis of our legitimate interest (**Art. 6 para. 1 lit. f GDPR**) in fast and good communication with you or other customers and business partners. Nevertheless, we only use the integrated social media elements if you have given your consent. Most social media platforms also set cookies in your browser to store data. We therefore recommend that you read our data protection text on cookies carefully and consult the privacy policy or cookie guidelines of the respective service provider.

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

As the basis for data processing with recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, i.e. in particular in the USA) or data transfer to these countries, Facebook uses data processing methods approved by the EU Commission.

Standard contractual clauses (= Art. 46 (2) and (3) GDPR). These clauses oblige Facebook to comply with the EU level of data protection when processing relevant data outside the EU. These clauses are based on an implementing decision of the EU Commission. You can find the decision and the clauses here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=en

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

Blogs and publication media Introduction

Blogs and publication media Privacy policy summary

Data subject: Visitors to the website

Purpose: Presentation and optimization of our services as well as communication between website visitors, security measures and administration

Processed data: Data such as contact details, IP address and published content.

You can find more details on this in the tools used.

Storage duration: depending on the tools used

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

What are blogs and publication media?

We use blogs or other means of communication on our website with which we can communicate with you on the one hand and you with us on the other. We may also store and process your data in the process. This may be necessary so that we can display content appropriately, communication works and security is increased. In our data protection text, we provide a general description of which of your data may be processed. Exact details on data processing always depend on the tools and functions used. You can find detailed information on data processing in the data protection notices of the individual providers.

Why do we use blogs and publication media?

Our greatest concern with our website is to offer you interesting and exciting content and at the same time your opinions and content are also important to us. That's why we want to create a good interactive exchange between us and you. With various blogs and publication options, we can achieve exactly that. For example, you can write comments on our content, comment on other comments or, in some cases, write articles yourself.

What data is processed?

Exactly which data is processed always depends on the communication functions we use. Very often, the IP address, user name and the

published content is stored. This is primarily done to ensure security protection, to prevent spam and to be able to take action against illegal content. Cookies can also be used for data storage. These are small text files that are stored with information in your browser. You can find more information on the data collected and stored in our individual sections and in the privacy policy of the respective provider.

Duration of data processing

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

Right of objection

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

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

Legal basis

We use the means of communication mainly on the basis of our legitimate interests (Art. 6 para. 1 lit. f GDPR) in fast and good communication with you or other customers, business partners and visitors. Insofar as the use serves the processing of contractual relationships or their initiation, the legal basis is also Art. 6 para. 1 sentence 1 lit. b. GDPR.

Certain processing operations, in particular the use of cookies and the use of comment or message functions, require your consent. If and insofar as you have consented to your data being processed and stored by integrated publication media, this consent is the legal basis for data processing (Art. 6 para. 1 lit. a GDPR). Most of the communication functions we use set cookies in your browser to store data.

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

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

Online Marketing Introduction

Online marketing privacy policy summary

Data subject: Visitors to the website

Purpose: Evaluation of visitor information to optimize the website.

Processed data: Access statistics containing data such as locations of access, device data, access duration and time, navigation behavior, click behavior and IP addresses.

Also personal data such as name or e-mail address can be processed. You can find more details on this in the respective

Online marketing tool.

Storage period: depending on the online marketing tools used

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

What is online marketing?

Online marketing refers to all measures that are carried out online in order to achieve marketing goals such as increasing brand awareness or closing a deal. Our online marketing measures are also aimed at drawing people's attention to our website. We therefore use online marketing to show our offer to many interested people. This usually involves online advertising, content marketing or search engine optimization. Personal data is also stored and processed so that we can use online marketing efficiently and in a targeted manner. On the one hand, the data helps us to show our content only to those people who are actually interested in it and, on the other hand, we can measure the advertising success of our online marketing measures.

Why do we use online marketing tools?

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

What data is processed?

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

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 agreed that we may also determine your location, we may also store and process this.

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

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

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

With all the advertising tools we use that store your data on their servers, we only ever receive aggregated information and never data that identifies you as an individual. The data only shows how well advertising measures worked. For example, we can see which measures 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 offer in the future and adapt it even more precisely to the needs and wishes of interested persons.

Duration of data processing

We will inform you about the duration of data processing below, if we have further information on this. In general, we only process personal data for as long as is absolutely necessary for the provision of our services and products. Data that is stored in cookies is for different lengths of time. Some cookies are deleted as soon as you leave the website, while others may be stored in your browser for several years. You can usually find detailed information about the individual cookies used by the provider in the respective data protection declarations of the individual providers.

Right of objection

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

As cookies can generally be used with online marketing tools, we also recommend that you read our general privacy policy on cookies. In order to

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 **Art. 6 para. 1 lit. a GDPR (consent)**, this consent constitutes the legal basis for the processing of personal data, as may occur when it is collected by online marketing tools.

We also have a legitimate interest in measuring online marketing measures in anonymized form in order to optimize our offer and our measures with the help of the data obtained. The legal basis for this is **Art. 6 para. 1 lit. f GDPR (legitimate interests)**. Nevertheless, we only use the tools if you have given your consent.

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

Google AdMob privacy policy

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

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

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

The data processing terms for Google advertising products (Google Ads Controller-Controller Data Protection 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 that processed through the use of Google AdMob in the privacy policy at <https://policies.google.com/privacy?hl=de>.

Google Marketing Platform (formerly: DoubleClick) Privacy Policy

We use Google Marketing Platform products on our website. These various marketing tools such as Data Studio, Surveys, Campaign Manager 360, Display & Video 360 and Search Ads 360. The service provider is the American company Google Inc. Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services in Europe.

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

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

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 that is processed through the use of Google Marketing Platform products in the privacy policy at <https://policies.google.com/privacy?hl=de>.

PayPal Marketing Solutions Privacy Policy

We use PayPal Marketing Solutions, a sales optimization tool, on our website. The service provider is the American company PayPal Pte. Ltd, 2211 North First Street, San Jose, California 95131, USA.

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

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

For more information on the standard contractual clauses and the data processed through the use of PayPal Marketing Solutions, please refer to the privacy policy at <https://www.paypal.com/webapps/mpp/ua/privacy-full>

Cookie Consent Management Platform Introduction

Cookie Consent Management Platform Summary

Affected: Website visitors

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

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

Storage duration: on the tool used, you have to be prepared for periods of several years

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

What is a Cookie Consent Management Platform?

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

Why do we use a cookie management tool?

Our aim is to offer you the best possible transparency in the area of data protection. We are also legally obliged to do so. We want to provide you with as much information as possible about all tools and all cookies that can store and process your data. It is also your right to decide for yourself which cookies you accept and which you do not. In order to grant you this right, we first need to know exactly which cookies have landed on our website in the first place. Thanks to a cookie management tool that regularly scans the website for all existing cookies, we know about all cookies and can provide you with GDPR-compliant information about them.

You can then accept or reject cookies via the consent system.

What data is processed?

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

Duration of data processing

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

Right of objection

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

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

Legal basis

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

Security & Anti-Spam

Security & Anti-Spam Privacy Policy Summary

Data subject: Visitors to the website

Purpose: Cybersecurity

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

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

Storage period: most of the data is stored until it is no longer needed to fulfill the service

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

What is security & anti-spam software?

With so-called security and anti-spam software, you and we can protect ourselves from various spam or phishing emails and possible other cyberattacks. Spam refers to advertising emails from a mass mailing that you did not request yourself. Such emails are also known as data junk and can also cause costs. Phishing emails, on the other hand, are messages that aim to build trust via fake messages or websites in order to obtain personal data. Anti-spam software generally protects against unwanted spam messages or malicious emails that could introduce viruses into our system. We also use general firewall and security systems to protect our computers from unwanted network attacks.

Why do we use security & anti-spam software?

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

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

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

Duration of data processing

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

Right of objection

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

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

Legal basis

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

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

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

Google reCAPTCHA privacy policy

Google reCAPTCHA privacy policy summary

^ Data subject: Visitors to the website

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

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

You can find more details below in this privacy policy.

Storage duration: depending on the stored data

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

What is reCAPTCHA?

Our primary goal is to secure and protect our website for you and for us in the best possible way. To ensure this, we use Google reCAPTCHA from Google Inc. For the European region, the company Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services. With reCAPTCHA we can determine whether you are really a flesh and blood person and not a robot or other spam software. By spam we mean any unsolicited information that is to us electronically. With the classic CAPTCHAs, you usually had to solve text or picture puzzles to verify your identity. With reCAPTCHA from Google, we don't usually have to bother you with such puzzles. In most cases, all you have to do is tick a box to confirm that you are not a bot. With the new Invisible reCAPTCHA version, you no longer even have to tick box. You can find out exactly how this works and, above , which data is used for this in the course of this privacy policy.

reCAPTCHA is a free captcha service from Google that protects websites from spam software and misuse by non-human visitors. This service is most commonly used when you fill out forms on the Internet. A Captcha service is a type of automatic Turing test that is designed to ensure that an action on the Internet performed by a human and not by a bot. In the classic Turing test (named after the computer scientist Alan Turing), a human determines the difference between a bot and a human. With captchas, this is also done by the computer or a software program.

Classic captchas work with small tasks that are easy for humans to solve but present considerable difficulties for machines. With reCAPTCHA, you no longer have to actively puzzles. The tool uses modern risk techniques to distinguish humans from bots. All you have to do here is tick the "I am not a robot" text field, and with Invisible reCAPTCHA even this is no longer necessary. With reCAPTCHA, a JavaScript element is integrated into the source code and then the tool runs in the background and analyzes your user behaviour. The software calculates a so-called captcha score from these user actions. Google uses this score to calculate the probability that you are human even before you enter the captcha. reCAPTCHA or captchas in general are always used when bots

manipulate or abuse certain actions (such as registrations, surveys, etc.).

Why do we use reCAPTCHA on our website?

We only want to welcome people of flesh and blood on our site. Bots and spam software of all kinds can safely stay at home. That's why we do everything we can to protect ourselves and offer you the best possible user-friendliness. For this reason, we use Google reCAPTCHA from Google. This way we can be pretty sure that we remain a "bot-free" website. By using reCAPTCHA, data is transmitted to Google to determine whether you are actually a human being. reCAPTCHA therefore serves to ensure the security of our website and, by extension, your security. For example, without reCAPTCHA it could happen that a bot registers as many e-mail addresses as possible during registration in order to subsequently "spam" forums or blogs with unwanted advertising content. With reCAPTCHA, we can prevent such bot attacks.

What data is stored by reCAPTCHA?

reCAPTCHA collects personal data from users in order to determine whether the actions on our website actually originate from people. The IP address and other data that Google requires for the reCAPTCHA service can therefore be sent to Google. IP addresses are almost always truncated within the member states of the EU or other signatory states to the Agreement on the European Economic Area before the data is sent to a server in the USA. The IP address is not combined with other Google data unless you are logged in with your Google account while using reCAPTCHA. First, the reCAPTCHA algorithm checks whether Google cookies from other Google services (YouTube, Gmail, etc.) have already been placed on your browser. Then reCAPTCHA places an additional cookie in your browser and takes a snapshot of your browser window.

The following list of collected browser and user data does not claim to be exhaustive. Rather, they are examples of data that, to our knowledge, are processed by Google.

- Referrer URL (the address of the page from which the visitor comes)
- IP address (e.g. 256.123.123.1)
- Information about the operating system (the software that enables your computer to operate. Common operating systems are Windows, Mac OS X or Linux)
- Cookies (small text files that store data in your browser)
- Mouse and keyboard behavior (every action you perform with the mouse or keyboard is saved)
- Date and language settings (which language or date you have preset on your PC is saved)
- All JavaScript objects (JavaScript is a programming language that enables websites to talk to the user. JavaScript objects can collect all kinds of data under one name)
- Screen resolution (indicates how many pixels the image display consists of)

It is undisputed that Google uses and analyzes this data even before you click on the "I am not a robot" checkbox. With the Invisible reCAPTCHA version, even

The entire recognition process in the background. Google does not tell you in detail exactly how much and what data it stores.

The following cookies are used by reCAPTCHA: Here we refer to the reCAPTCHA demo version from Google at <https://www.google.com/recaptcha/api2/demo> . All these cookies require a unique identifier for tracking purposes. Here is a list of cookies that Google reCAPTCHA has set on the demo version:

Name: IDE

Value: WqTUmlnmv_qXyi_DGNPLESKnRNrpgXoy1K-pAZtAkMbHI-121963999-8

Purpose: This cookie is set by the company DoubleClick (also owned by Google) to register and report the actions of a user on the website when interacting with advertisements. This allows the effectiveness of advertising to be measured and appropriate optimization measures to be taken. IDE is stored in browsers under the domain doubleclick.net.

Expiration date: after one year

Name: 1P_JAR

Value: 2019-5-14-12

Purpose: This cookie collects statistics on website usage and measures conversions. A conversion occurs, for example, when a user becomes a buyer. The cookie is also used to display relevant advertisements to users. The cookie can also be used to prevent a user from seeing the same ad more than once.

Expiration date: after one month

Name: ANID

Wert: U7j1v3dZa1219639990xgZFmiqWppRWKOr

Purpose: We were unable to out much information about this cookie. In Google's privacy policy, the cookie is mentioned in connection with "Advertising cookies" such as "DSID", "FLC", "AID", "TAID" are mentioned. ANID is stored under domain google.com.

Expiration date: after 9 months

Name: CONSENT

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

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

Expiration date: after 19 years

Name: NID

Wert: 0WmuWqy121963999zILzqV_nmt3sDXwPeM5Q

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

Expiration date: after 6 months

Name: DV

Wert: gEAABBCjJMXcI0dSAAAANbqc121963999-4

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

Expiration date: after 10 minutes

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

How long and where is the data stored?

By inserting reCAPTCHA, data is transferred from you to the Google server. Where exactly this data is stored is not made clear by Google, even after repeated requests. Without having received confirmation from Google, it can be assumed that data such as mouse interaction, time spent on the website or language settings are stored on the European or American Google servers. The IP address that your browser transmits to Google is not merged with other Google data from other Google services. However, if you are logged in to your Google account while using the reCAPTCHA plug-in, the data will be merged. The deviating data protection provisions of Google apply to this.

How can I delete my data or prevent data storage?

If you do not want any data you and your behavior to be transmitted to Google, you must log out of Google completely and delete all Google cookies before you visit our website or use the reCAPTCHA software. In principle, the data is automatically transmitted to Google as soon as you visit our website. To delete this data again, you must Google support at <https://support.google.com/?hl=de&tid=121963999>.

By using our website, you agree that Google LLC and its representatives may automatically collect, process and use data.

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

Legal basis

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

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

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

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

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

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

Payment provider introduction

Payment provider privacy policy summary

Data subject: Visitors to the website

Purpose: Enabling and optimizing the payment process on our website

Processed data: Data such as name, address, bank details (account number, credit card number, passwords, TANs, etc.), IP address and contract data More details can be found in the respective payment provider tool used.

Storage period: depending on the payment provider used

Legal basis: Art. 6 para. 1 lit. b GDPR (fulfillment of a contract)

What is a payment provider?

We use online payment systems on our website that enable us and you to make secure and smooth payments. Among other things, personal data may be sent to the respective payment provider, stored and processed there. Payment providers are online payment systems that enable you to place an order via online banking. Payment processing is carried out by the payment provider you have selected. We then receive information about the payment made. This method can be used by any user who has an active online banking account with PIN and TAN. There are hardly any banks that do not offer or accept such payment methods.

Why do we use payment providers on our website?

We naturally want to offer the best possible service with our website and our integrated online store so that you feel comfortable on our site and take advantage of our offers. We know that your time is valuable and that payment processes in particular must function quickly and smoothly. For these reasons, we offer you various payment providers. You can choose your preferred payment provider and pay in the usual way.

What data is processed?

Exactly which data is processed depends of course on the respective payment provider. However, data such as name, address, bank details (account number, credit card number, passwords, TANs, etc.) are generally stored. This is necessary data in order to be able to carry out a transaction at all. In addition, any contract data and user data, such as when you visit our website, what content you are interested in or which subpages you click on, may also be stored. Your IP address and information about the computer you are using are also stored by most payment providers.

The data is usually stored and processed on the payment provider's servers. We as the website operator do not receive this data. We are only informed whether the payment has worked or not. For identity and credit checks, payment providers may forward data to the relevant body. The business and data protection principles of the respective provider always apply to all payment transactions. Therefore, please always take a look at the payment provider's general terms and conditions and privacy policy. You also have the right to have data deleted or corrected at any time. Contact the respective service provider regarding your rights (right of withdrawal, right to information and right to be affected).

Duration of data processing

We will inform you about the duration of data processing below if we have further information on this. In general, we only process personal data for as long as is absolutely necessary for the provision of our services and products. If it is required by law, for example in the case of accounting, this storage period may also be exceeded. For example, we store accounting documents relating to a contract (invoices, contract documents, account statements, etc.) for 10 years (§ 147 AO) and other relevant business documents for 6 years (§ 247 HGB) after they are created.

Right of objection

You always have the right to information, correction and deletion of your personal data. If you have any questions, you can also contact the person responsible for the payment provider used at any time. Contact details can be found either in our specific privacy policy or on the website of the relevant payment provider.

You can delete, deactivate or manage cookies that payment providers use for their functions in your browser. Depending on which browser you use, this works in different ways. Please note, however, that the payment process may then no longer work.

Legal basis

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

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

American Express Privacy Policy

We use American Express, a global financial services provider, on our website. The service provider is the American Express Company. The company American Express Europe S.A. (Avenida Partenón 12-14, 28042, Madrid, Spain) is responsible for the European region.

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

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

Under the "European Implementing Principles (<https://www.americanexpress.com/en-pl/company/legal/privacy-centre/european-implementing-principles/>) you will find more detailed information on the standard contractual clauses at American Express.

You can find out more about the data through the use of American Express in the Privacy Policy at <https://www.americanexpress.com/de-en/company/legal/datenschutz-center/online-datenschutzerklarung/>.

giropay privacy policy

We use the online payment provider giropay on our website. The service provider is the German company paydirekt GmbH, Stephanstraße 14-16, 60313 Frankfurt am Main, Germany.

You can find out more about the data that is processed through the use of giropay in the privacy policy at <https://www.giropay.de/agb/index.html>

Google Pay privacy policy

We use the online payment provider Google Pay on our website. The service provider is the American company Google Inc. For the European region, 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. We would like to point out that, in the opinion of the European Court of Justice, there is currently no adequate level of protection for data transfers to the USA. This may entail various risks for the legality and security of data processing.

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

The data processing terms for Google advertising products (Google Ads Controller-Controller Data Protection Terms), which refer to the standard contractual clauses, can be found at <https://business.safety.google/adscontrollerterms/>.

You can find out more about the data that is processed through the use of Google Pay in the privacy policy at <https://policies.google.com/privacy>. -

Klarna Checkout privacy policy

Klarna Checkout privacy policy summary

Data subject: Visitors to the website

Purpose: Optimization of the payment process on our website

Processed data: Data such as name, address, bank details (account number, credit card number, passwords, TANs, etc.), IP address and contract data More details can be found below in this privacy policy.

Storage period: Data is stored for as long as Klarna needs it for processing purpose.

Legal basis: Art. 6 para. 1 lit. c GDPR (Legal obligation), Art. 6 para. 1 lit. f GDPR (Legitimate interests)

What is Klarna Checkout?

We use the online payment system Klarna Checkout from the Swedish company Klarna Bank AB on our website. Klarna Bank has its head office at Sveavägen 46, 111 34 Stockholm, Sweden. If you choose to use this service, personal data will be sent to Klarna, stored and processed. In this privacy policy we would like to give you an overview of the data processing by Klarna.

Klarna Checkout is a payment system for orders in an online store. The user selects the payment method and Klarna Checkout takes care of the entire payment process. Once a user made a payment via the checkout system and entered the relevant data, future online purchases can be made even more quickly and easily. The Klarna system then recognizes the existing customer after the email address and zip code have been entered.

Why do we use Klarna Checkout for our website?

Our aim with our website and our integrated online store is to offer you the best possible service. In addition to the overall experience on the website and our offers, this also includes smooth, fast and secure payment processing of your orders. To ensure this, we use the Klarna Checkout payment system.

What data is stored by Klarna Checkout?

As soon as you decide to use the Klarna payment service and pay via the Klarna Checkout payment method, you also transmit personal data to the company. On the Klarna Checkout page, technical data such as browser type, operating system, our Internet address, date and time, language settings, time zone settings and IP address are collected from you and transmitted to Klarna's servers and stored there. This data is stored even if you have not yet completed an order.

When you order a product or service via our store, you must enter your personal data in the fields provided. This data is processed by Klarna for payment processing. The following personal data in particular (as well as general product information) may be stored and processed by Klarna for credit and identity checks:

- Contact information: Name, date of birth, national ID number, title, billing and shipping address, e-mail address, telephone number, nationality or salary.
- Payment information such as credit card details or your bank account number
- Product information such as shipment number, type of item and price of the product

There is also data that can be collected optionally if you make a conscious decision to do so. These include political, religious or ideological beliefs or various health data.

Klarna may also collect data about the goods or services you purchase or order itself or via third parties (such as us or via public databases) in addition to the above-mentioned data. This may include, for example, the consignment number or the type of item ordered, but also information about your creditworthiness, your income or the granting of credit. Klarna may also pass on your personal data to service providers such as software providers, data storage providers or us as a merchant.

If data is automatically entered into a form, cookies are always involved. If you do not wish to use this function, you can deactivate these cookies at any time. Further down in the text you will find instructions on how to delete, deactivate or manage cookies in your browser. Our tests have shown that Klarna does not set any cookies directly. If you select the payment method "Klarna Sofort" and click on "Order", you will be redirected to the Sofort website. After successful payment, you will be taken to our thank you page. The following cookie is set there by sofort.com:

Name: SOFUEB

Value: e8cipp378mdscn9e17kajlfhv7121963999-4 **Purpose:** This cookie stores your session ID. **Expiration date:** after the end of the browser session

How long and where is the data stored?

Klarna endeavors to store your data only within the EU or the European Economic Area (EEA). However, data may also be transferred outside the EU/EEA. If this happens, Klarna ensures that the data protection is in accordance with the GDPR and that the third country is covered by an adequacy decision of the European Union. The data is always stored as long as Klarna needs it for the processing purpose.

How can I delete my data or prevent data storage?

You can revoke your consent to Klarna processing your personal data at any time. You also always have the right to information, correction and deletion of your personal data.

personal data. All you have to do is contact the company or the company's data protection team by sending an email to datenschutz@klarna.de . You can also contact Klarna directly via the Klarna website "[My data protection request](#)".

You can delete, deactivate or manage cookies that Klarna may use for its functions in your browser. Depending on which browser you use, this works in different ways. Under the section "Cookies" you will find the corresponding links to the respective instructions for the most popular browsers.

Legal basis

We therefore offer the payment service provider Klarna Checkout in addition to the conventional banking/credit institutions for the processing of contractual or legal relationships (**Art. 6 para. 1 lit. b GDPR**).

We hope we have provided you with a good overview of data processing by Klarna. If you would like to find out more about how your data is handled, we recommend that you read Klarna's privacy policy at https://cdn.klarna.com/1.0/shared/content/legal/terms/0/de_at/privacy.

PayPal privacy policy

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

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

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

For more information on the standard contractual clauses and the data through the use of PayPal, please refer to the privacy policy at <https://www.paypal.com/webapps/mpp/ua/privacy-full>

Visa privacy policy

We use Visa, a global payment provider, on our website. The service provider is the American company Visa Inc. Visa Europe Services Inc. (1 Sheldon Square, London W2 6TT, United Kingdom) is responsible for the European region.

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

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

You can find more information on Visa's standard contractual clauses at <https://www.visa.de/nutzungsbedingungen/visa-globale-datenschutzmitteilung/mitteilung-zu-zustandigkeitsfragen-fur-den-ewr.html>.

You can find out more about the data through the use of Visa in the Privacy Policy at <https://www.visa.de/nutzungsbedingungen/visa-privacy-center.html>

Audio & Video Introduction

Audio & Video Privacy Policy Summary

Data subject: Visitors to the website

Purpose: Optimization of our service performance

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

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

Storage period: Data is generally stored for as long as it is necessary for the processing purpose.

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

What are audio and video elements?

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

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

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

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

Of course we want to provide you with the best offer on our website. And we are aware that content is no longer just conveyed in text and static images. Instead of simply giving you a link to a video, we offer you audio and video formats directly on our website that are entertaining or informative and ideally even both. This expands our service and makes easier for you to access interesting content. We therefore offer video and/or audio content in addition to our texts and images.

What data is stored by audio & video elements?

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

Duration of data processing

You can find out exactly how long the data is stored on the servers of the third-party providers either below in the data protection text of the respective tool or in the

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

Right of objection

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

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

Legal basis

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

Video conferencing & streaming Introduction

Video conferencing & streaming privacy policy summary

Affected parties: Users who use our video conferencing or streaming tool

Purpose: Communication and presentation of content

Processed data: Access statistics that contain data such as name, address, contact details, email address, telephone number or your IP address. You can find more details on this in the respective video conferencing or streaming tool used.

Storage period: depending on the video conferencing or streaming tool used

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

What are video conferencing & streaming?

We use software programs that enable us to hold video conferences, online meetings, webinars, display sharing and/or streaming. During a video conference or streaming, information is transmitted simultaneously via sound and moving images. With the help of such video conferencing or streaming tools, we can communicate with customers, business partners, clients and even employees quickly and easily via the Internet. When selecting the service provider, we naturally pay attention to the specified legal framework conditions.

In principle, third-party providers can process data as soon as you interact with the software program. Third-party providers of video conferencing and streaming solutions use your data and metadata for various purposes. For example, the data helps to make the tool more secure and to improve the service. In most cases, the data may also be used for the third-party provider's own marketing purposes.

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

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

What data is processed?

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

Exactly which data is stored depends on the solutions used. Each provider stores and processes a different amount of data. As a rule however, most providers store your name, address, contact details such as your email address or telephone number and your IP address.

Furthermore, information about the device you are using, usage data such as which websites you visit, when you visit a website or which buttons you click on may also be stored. Data that is shared within the video conference (photos, videos, texts) can also be stored.

Duration of data processing

We will inform you about the duration of data processing below in connection with the service used, if we have further information on this. In general, we only process personal data for as long as absolutely necessary for the provision of our services and products. The provider may store your data according to its own specifications, over which we have no influence.

Right of objection

You always have the right to information, correction and deletion of your personal data. If you have any questions, you can also contact the person responsible for the video conferencing or streaming tool used at any time. You can find contact details

either in our specific privacy policy or on the website of the relevant provider.

You can delete, deactivate or manage cookies that providers use for their functions in your browser. Depending on which browser you use, this works in different ways. Please note, however, that not all functions may then work as usual.

Legal basis

If you have consented to your data being processed and stored by the video or streaming solution, this consent is the legal basis for data processing (**Art. 6 para. 1 lit. a GDPR**). In addition, we can also offer a video conference as part of our services if this has been contractually agreed with you in advance (**Art. 6 para. 1 lit. b 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 fast and good communication with you or other customers and business partners, but only if you have at least given your consent. Most video and streaming solutions also set cookies in your browser to store data. We therefore recommend that you read our data protection text on cookies carefully and consult the privacy policy or cookie guidelines of the respective service provider.

Information on special video conferencing and streaming solutions, if available, can be found in the following sections.

Survey and interview systems Introduction

Survey and interview systems Privacy policy Summary

Data subject: Visitors to the website

Purpose: Evaluation of surveys on the website

Processed data: Contact data, device data, access duration and time, IP addresses. You can find more details on this in the respective survey and questionnaire system used.

Storage duration: depending on the tool used

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

What are survey and interview systems?

We are also happy to conduct various surveys and questionnaires via our website. These are always evaluated anonymously. A survey or questionnaire system is a tool integrated into our website that asks you questions (e.g. about our products or services) which you can answer if you participate. Your answers are always analyzed anonymously. However, personal data may also be stored and processed after you have given your consent to data processing.

Why do we use survey and interview systems?

We want to offer you the best products and services in our industry. Surveys provide us with perfect feedback and tell us what you expect from us and our services. Based on these anonymous evaluations, we can adapt our products and services to best suit your wishes and expectations.

Furthermore, the information also helps us to direct our advertising and marketing measures in a more targeted manner to those people who are really interested in our offer.

What data is processed?

Personal data is only processed if it is necessary for the technical implementation or if you have consented to the processing of personal data. For example, your IP address is stored so that the survey can be displayed in your browser. Cookies may also be used so that you can continue your survey at a later date without any problems.

If you have consented to data processing, contact data such as your e-mail address or telephone number may be processed in addition to your IP address. Data that you enter in an online form, for example, will also be stored and processed. Some providers also store information about the web pages you have visited (on our website), when you started and ended the survey and various technical information about your computer.

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 privacy policies of the providers usually state exactly which data is stored and processed and for how long. In principle, personal data is only processed for as long as is necessary for the provision of our services. If data is stored in cookies, the storage period varies greatly. The data can be deleted immediately after leaving a website, but it can also remain stored for several years. You should therefore look at each individual cookie in detail if you want to know more about data storage. In most cases, you will also find informative information about the individual cookies in the data protection declarations of the individual providers.

Right of objection

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

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

Legal basis

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

In addition to consent, we have a legitimate interest in conducting surveys on our topic. The legal basis for this is **Art. 6 para. 1 lit. f GDPR (legitimate interests)**. Nevertheless, we only use the tools if you have given your consent.

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

Information on the individual survey systems, if available, can be found in the following sections.

Google form privacy policy

We use Google Form, a service for Google Cloud Forms, for our website. The service provider is the American company Google Inc. For the European area, the company Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services.

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

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

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

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

Evaluation platforms Introduction

Evaluation platforms Summary

Data subject: Visitors to the website or a rating platform

Purpose: Feedback on our products and/or services

Processed data: IP address, e-mail address, name, among others. More details can be found below or on the respective rating platforms used.

Storage duration: depending on the respective platform

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

What are rating platforms?

You can rate our products or services on various rating platforms. We participate in some of these platforms so that we can receive feedback from you and thus optimize our offer. If you rate us via a rating platform, the privacy policy and general terms and conditions of the respective rating service apply. Very often you will also need to register in order to submit a review. Evaluation technologies (widgets) can also be integrated into our website. By using such an integrated tool, data is also transferred to the corresponding provider, processed and stored.

Many of these integrated programs work on a similar principle. After you have ordered a product or used a service from us, you will be asked to leave a review by e-mail or on the website. You are usually redirected to a review page via a link and can quickly and easily create a review there. Some rating systems also offer an interface to various social media channels to make the feedback accessible to more people.

Why do we use rating platforms?

Rating platforms collect feedback and ratings about our offers. Your reviews provide us with quick feedback and enable us to improve our products and/or services much more efficiently. The reviews therefore help us to optimize our offers on the one hand and on the other hand they give you and all our future customers a good overview of the quality of our products and services.

What data is processed?

With your consent, we transmit information about you and the services you have used to the relevant evaluation platform. We do this to ensure that you have actually used one of our services.

have taken. Only then can you provide real feedback. The transmitted data is only used to identify the user. Exactly which data is stored and processed depends, of course, on the providers used. In most cases, the review platforms are also provided with personal data such as IP address, e-mail address or your name. Order information, such as the order number of a purchased item, is also forwarded to the relevant platform after you have submitted your review. If your e-mail address is transmitted, this is done so that the review platform can send you an e-mail after you have purchased a product. So that we can also incorporate your review into our website, we also provide the providers with the information that you have accessed our site.

The evaluation platform used is responsible for the personal data collected.

How long and where is the data stored?

You can find out more about the duration of data processing below in the relevant provider's privacy policy, if we have further information on this. In general, we only process personal data for as long as is absolutely necessary for the provision of our services and products.

Personal data that is mentioned in a review is usually anonymized by employees of the platform used and is therefore only visible to administrators of the company. The data collected is stored on the provider's servers and is deleted by most providers once the order has been completed.

Right of objection

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

Legal basis

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

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

We hope we have been able to provide you with the most important general information about the data processing of rating platforms. You can find more detailed information below in the data protection texts or in the linked data protection declarations of the company.

Google Customer Reviews Privacy Policy

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

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

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

The data processing terms for Google advertising products (Google Ads Controller-Controller Data Protection 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 that is processed through the use of Google in the privacy policy at <https://policies.google.com/privacy?hl=de>.

Trusted Shops privacy policy

We also use the Trusted Shops rating platform for our website. The service provider is the German company Trusted Shops GmbH, Subbelrather Straße 15c, 50823 Cologne, Germany.

You can find out more about the data that processed through the use of Trusted Shops in the privacy policy at <https://www.trustedshops.de/impressum-datenschutz/#datenschutz>.

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 region.

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

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

You can find more information on the data processed and the standard contractual clauses at Adobe at <https://.www.adobe.com/de/privacy/eudatatransfers.html>

Google Fonts privacy policy

Google Fonts privacy policy summary

Data subject: Visitors to the website

Purpose: Optimization of our service performance

Processed data: Data such as IP address and CSS and font requests More details can be found below in this privacy policy.

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 of GDPR (legitimate interests)

What are Google Fonts?

We use Google Fonts on our website. These are the "Google fonts" of Google Inc. For the European area, the company Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services.

You do not need to log in or enter a password to use Google fonts. Furthermore, no cookies are in your browser. The files (CSS, 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 data will be transmitted to Google while you are 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 exactly how the data is stored.

Google Fonts (formerly Google Web Fonts) is a directory of over 800 fonts that [Google](#) makes available to its users free of charge.

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

Why do we use Google Fonts on our website?

With Google Fonts, we can use fonts on our own website without having 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 great 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 sometimes visually distort texts or entire websites. Thanks to the fast Content Delivery Network (CDN), there are no cross-platform problems with Google Fonts. Google Fonts supports all common 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 present our entire online service as beautifully and uniformly as possible.

What data is stored by Google?

When you visit our website, the fonts are reloaded via a Google server. This external call transmits data to the Google server. In this way, Google also recognizes that you or your IP address is visiting our website. The Google Fonts API was developed to reduce the use, storage and collection of end user data to what is necessary for the proper provision of fonts. Incidentally, API stands for "Application Programming Interface" and is used, among other things, as a data transmitter in the software sector.

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

However, it should also be borne in mind that every Google Font request also includes information such as language settings, IP address, browser version, screen resolution of the

browser and the name of the browser are automatically transmitted to the Google servers. Whether this data is also stored cannot be clearly determined and 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 with the help of a Google stylesheet. A stylesheet is a format template that can be used 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 aim is to fundamentally improve the loading time of websites. If millions of websites refer to the same fonts, they are cached after the first visit and immediately reappear on all other websites visited later. Sometimes Google updates font files to reduce the file size, increase language coverage and improve the design.

How can I delete my data or prevent data storage?

The data that Google stores for one day or one year cannot simply be deleted. The data is automatically transmitted to Google when the page is accessed. To delete this data prematurely, you must contact Google support at <https://support.google.com/?hl=de&tid=121963999>. In this case, you can only prevent data storage if you do not visit our site.

Unlike other web fonts, Google allows us unrestricted access to all fonts. This means we have unlimited access to a sea of fonts and can therefore get the most out of our website. You can find out more about Google Fonts and other issues at <https://developers.google.com/fonts/faq?tid=121963999>. Although Google addresses data protection issues there, it does not provide any really detailed information about data storage. It is relatively difficult to get really precise information from Google about stored data.

Legal basis

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

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

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

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

The Google Ads Data Processing Terms, which also correspond to the standard contractual clauses for Google Fonts, can be found at <https://business.safety.google/adsprocessorterms/>.

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

Google Fonts Local Privacy Policy

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

What are Google Fonts?

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

Online map services Introduction

Online map services Privacy policy summary

Affected parties: Visitors to the website

Purpose: Improvement of the user experience

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

Storage duration: depending on the tools used

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

What are online map services?

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

Why do we use online map services on our website?

Generally speaking, our aim is to offer you a pleasant time on our website. And your time is only pleasant if you can easily find your way around our website and find all the information you need quickly and easily.

We therefore thought that an online map system could be a significant improvement to our service on the website. Without leaving our website, you can use the map system to easily view route descriptions, locations or even places of interest. Of course, it is also very practical that you can see at a glance where we are based so that you can find us quickly and safely. As you can see, there are simply many advantages and we clearly regard online map services on our website as part of our customer service.

What data is stored by online map services?

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

How long and where is the data stored?

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

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

Right of objection

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

Legal basis

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

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

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

Google Maps privacy policy

Google Maps privacy policy summary

Data subject: Visitors to the website

Purpose: Optimization of our service performance

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

You can find more details below in this privacy policy.

Storage duration: depending on the stored data

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

What is Google Maps?

We use Google Maps Google Inc. on our website. Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services in Europe. With Google Maps, we can show you locations better and thus adapt our service to your needs. By using Google Maps, data is transmitted to Google and stored on Google servers. We would now like to explain in more detail what Google Maps is, why we use this Google service, what data is stored and how you can prevent this.

Google Maps is an internet map service from Google. With Google Maps, you can search online for exact locations of cities, places of interest, accommodation or businesses using a PC, tablet or app. If companies are represented on Google My Business, further information about the company is displayed in addition to the location. To display directions, map sections of a location can be integrated into a website using HTML code. Google Maps shows the earth's surface as a street map or as an aerial or satellite image. Thanks to the Street View images and the high-quality satellite images, very accurate representations are possible.

Why do we use Google Maps on our website?

All our efforts on this site are aimed at providing you with a useful and meaningful time on our website. By integrating Google Maps, we can provide you with the most important information on various locations. You can see at a glance where we are based. The directions always show you the best or quickest way to reach us. You can call up the directions for routes by car, public transport, on foot or by bike. For us, providing Google Maps is part of our customer service.

What data is stored by Google Maps?

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

website, Google sets at least one cookie (name: NID) in your browser. This cookie stores data about your user behavior. Google uses this data primarily to optimize its own services and to provide you with individual, personalized advertising.

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

Name: NID

Wert: 188=h26c1Ktha7fCQTx8rXgLyATyITJ121963999-5

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

Expiration date: after 6 months

Note: We cannot guarantee the completeness of the stored data. Changes can never be ruled out, especially when using cookies. In order to identify the NID cookie, a separate test page was created where only Google Maps was integrated.

How long and where is the data stored?

Google servers are located in data centers all over the world. However, most of the servers are located in America. For this reason, your data is increasingly stored in the USA. Here you can read exactly where the Google data centers are located:

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

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

Google stores some data for a fixed period of time. For other data, Google only offers the option of deleting it manually. Furthermore, the company also anonymizes information (such as advertising data) in server logs by deleting part of the IP address and cookie information after 9 and 18 months respectively.

How can I delete my data or prevent data storage?

With the automatic deletion function for location and activity data introduced in 2019, location and web/app activity information is stored for either 3 or 18 months - depending on your decision - and then deleted. You can also manually delete this data from your history at any time via your Google account. If you want to completely prevent your location from being recorded, you must pause the "Web and app activity" section in your Google account. Click on "Data and personalization" and then on the "Activity settings" option. Here you can switch the activities on or off.

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

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

Legal basis

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

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

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

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

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

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

Content search providers Introduction

Content search provider privacy policy summary

Data subject: Visitors to the website

Purpose: Improvement of the user experience

Processed data: Which data is processed heavily on the services used. It is usually IP address, search interests and/or technical data. You can find more details on this in the respective tools used.

Storage duration: depending on the tools used

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

What is a content search provider?

We have already published a lot of content on our website. And of course we don't want it to be forgotten just because it can't be found. That's why we use a content search provider on our website. You are probably familiar with major search engines such as Google. A content search provider is basically also a search engine, but unlike Google, it does not search the entire web for content, but only the website you on. You can use a text field to enter terms that match the content you are looking for and the search program will find the desired articles for you. If you use the integrated search function, your personal data may also be processed.

Why do we use a content search provider?

If you take a look around our website, you will quickly realize how much useful content we already published over the years. There are some real treasures and we want you to find them quickly without having to click around. With a content search function directly on our website, you can quickly and easily find the content you are looking for using keywords that match the topic you are searching for. This feature is really practical and we also see it as our task to make your life on our website as pleasant and helpful as possible. That is why we have decided to integrate a content search program into our website.

What data is processed?

If you use the search function on our website, the integrated content search provider (such as Algolia Places or Giphy) may automatically receive and store data from you. This involves technical data about your browser as well as data such as your IP address, device ID and the search terms entered. Please note that IP addresses are personal data. The providers' privacy policies state that this information is collected and stored in order to increase security and improve their own services. The automatically collected usage data, which does not contain any personal data and is processed in anonymized form, can also be used for analysis purposes. Some providers also pass this anonymized data on to third parties. To find out more about this, we recommend that you read the specific data protection declarations of the individual providers carefully. Cookies are usually also in your browser to ensure that the services function properly. More

You can find out more about cookies in our general "Cookies" section. You can find out whether and which cookies the individual search tools use - if available - below or in the corresponding data protection declarations of the integrated tools.

How long and where is the data stored?

As a general rule, every content search provider processes different data. It is therefore not possible to go into the specific data processing of the individual tools in this general section. However, the services usually only store personal data for as long as this is necessary for the smooth functioning of the tools. Some services (such as Giphy) also store personal data for longer if this is necessary due to legal obligations. In depersonalized form, data is also stored for longer most providers. Content search providers may also use cookies to store various data. You can find out more about this in our general section on cookies. If you want to know more about the specific cookies used by a search provider, we recommend that you read the privacy policies of the providers we use. You will usually find an exemplary list of the cookies used there.

Right of objection

Always be aware: if you do not want your personal data to be processed, it may not be processed. You always have the right to access your personal data and to object to its use. You can also withdraw your consent at any time using the cookie consent tool or other opt-out options. You can also easily manage, delete or deactivate the cookies used yourself via your browser. If you delete cookies, some of the tool's functions may no longer work. So please do not be surprised. How you manage cookies in your browser also depends on the browser you are using. In the "Cookies" section you will also find links to the instructions for the most important browsers.

Legal basis

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

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

Information on specific content search providers - if available - can be found in the following sections.

Custom Google Search Privacy Policy

Custom Google Search Privacy Policy Summary

Data subject: Visitors to the website

Purpose: Optimization of our service performance

Processed data: Data such as IP address and search terms entered are stored by Google

You can find more details below in this privacy policy.

Storage period: the storage period varies depending on the data stored

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

What is Google Custom Search?

We have integrated the Google plug-in for user-defined searches on our website. Google is the largest and best-known search engine in the world and is operated by the US company Google Inc. Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for the European area. Through the user-defined Google search, data may be transferred from you to Google. In this privacy policy, we inform you why we use this plug-in, what data is processed and how you can manage or prevent this data transfer.

The custom Google search plug-in is a Google search bar directly on our website. The search place as on www.google.com, only the search results focus on our content and products or on a limited search area.

Why do we use Google Custom Search on our website?

A website with a lot of interesting content often becomes so large that you may lose track of it. Over time, we have also accumulated a lot of valuable material and as part of our service, we want you to find our content as quickly and easily as possible. Custom Google search makes finding interesting content a breeze. The built-in Google plug-in improves the overall quality of our website and makes searching easier for you.

What data is saved by the custom Google search?

With the user-defined Google search, your data is only transmitted to Google if you actively use the Google search integrated on our website. This means that only when you enter a search term in the search bar and then confirm this term (e.g. by clicking on "Enter") will your IP address be sent to Google, stored and processed there in addition to the search term. On the basis of the cookies set (e.g. `IP_JAR`), it can be assumed that Google also receives data on website usage. If you search for content during your visit to our website using the integrated Google search function and are logged in with your Google account at the same time, Google can also assign the data collected to your Google account. As the website operator, we have no influence on what Google does with the data collected or how Google processes the data.

The following cookies are set in your browser if you use the customized Google search and are not logged in with a Google account:

Name: 1P_JAR

Value: 2020-01-27-13121963999-5

Purpose: This cookie collects statistics on website usage and measures conversions. A conversion occurs, for example, when a user a buyer. The cookie is also used to display relevant advertisements to users.

Expiration date: after one month

Name: CONSENT

Value: WP.282f52121963999-9

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

Expiration date: after 18 years

Name: NID

Value: 196=pwIo3B5fHr-8

Purpose: NID is used by Google to customize advertisements to your Google search. With the help of the cookie, Google "remembers" the search queries you have entered or your previous interaction with ads. So you always get customized ads.

Expiration date: after 6 months

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

How long and where is the data stored?

Google servers are located all over the world. As Google an American company, most of the data is stored on American servers. At <https://www.google.com/about/datacenters/locations/?hl=de> you can see exactly where the Google servers are located.

Your data is distributed on various physical data carriers. This means that the data can be accessed more quickly and is better against possible manipulation. Google also has appropriate emergency programs for your data. For example, if there are internal technical problems at Google and servers stop working as a result, the risk of service interruption and data loss remains low.

Depending on the data in , Google stores it for different lengths of time. You can delete some data yourself, others are automatically deleted or anonymized by Google. However, there is also data that Google stores for longer if this is necessary for legal or business reasons.

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. There is some data that you can delete at any time. If you have a Google account, you can delete data about your web activity there or specify that it should be deleted after a certain period of time.

In your browser, you also have the option of deactivating or deleting cookies or managing them according to your wishes and preferences. In the "Cookies" section, you will find the relevant links to the instructions for the most popular browsers.

Legal basis

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

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

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

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

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

We hope we have been able to provide you with the most important information about data processing by Google. If you would like to find out more, we recommend Google's comprehensive privacy policy at <https://policies.google.com/privacy?hl=de>.

Other Introduction

Miscellaneous Privacy policy summary

Data subject: Visitors to the website

Purpose: Improvement of the user experience

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

Storage duration: depending on the tools used

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

What falls under "Other"?

The "Other" category includes services that do not fit into one of the above categories. These are usually various plugins and integrated elements that improve our website. As a rule, these functions are obtained from third-party providers 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-party providers?

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 companies. Rather, it is a place to help you find what you are looking for. To make our website even more interesting and helpful for you, we use various third-party services.

What data is processed?

Whenever elements are integrated into our website, your IP address is transmitted to the respective provider, stored and processed there. This is necessary because otherwise the content will not be sent to your browser and will therefore not be displayed accordingly. It may also happen that service providers also use pixel tags or use web beacons. These are small graphics on websites that record a log file and can also create analyses of this file. Providers can use the information obtained to improve their own marketing measures. In addition to pixel tags, such information (such as which button you click or when you visit which page) can also be stored in cookies. In addition to analysis data on your web behavior, technical information such as your browser type or operating system can also be stored in cookies. 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. As a matter of principle, we endeavor to only use services that handle the issue of data protection very carefully.

Duration of data processing

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

Legal basis

If we ask for your consent and you also agree that we may use the service, this is 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 in order to improve our offer technically and economically. The legal basis for this is Art. 6 para. 1 lit. f GDPR (legitimate interests). Nevertheless, we only use the tools if you have given your consent.

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

Explanation of terms used

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

Processor

Definition according to Article 4 of the GDPR

For the purposes of this Regulation:

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

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

Consent

Definition according to Article 4 of the GDPR

For the purposes of this Regulation:

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

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

In principle, consent can of course also be given in writing, i.e. not via a tool.

Personal data

Definition according to Article 4 of the GDPR

For the purposes of this Regulation:

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

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

- Name
- Address
- E-mail address
- Postal address
- Phone number
- Date of birth
- Identification numbers such as social security number, tax identification number, identity card number or matriculation number
- Bank data such as account number, credit information, account balances and much more.

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

- racial and ethnic origin
- political opinions
- religious or ideological convictions
- trade union membership
- genetic data such as data taken from blood or saliva samples
- biometric data (i.e. information on mental, physical or behavioral characteristics that can identify a person). Health data
- Data on sexual orientation or sexual life

Profiling

Definition according to Article 4 of the GDPR

For the purposes of this Regulation:

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

Explanation: Profiling involves collecting various pieces of information about a person in order to find out more about them. In the web sector, profiling is often used for advertising purposes or for credit checks. For example, web and advertising analysis programs 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.

Person responsible

Definition according to Article 4 of the GDPR

For the purposes of this Regulation:

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

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

Processing

Definition according to Article 4 of the GDPR

For the purposes of this Regulation:

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

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

All texts are protected by copyright.

Source: Created with the [data protection generator](#) from AdSimple