

# Legal Notice

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

Artichoke Computing GmbH  
Göstling 51,  
3345 Musterhausen,  
Österreich

**Object of the company:** IT Dienstleistungen, Handel mit Medizinprodukten

**VAT-Number:** ATU75057518

**GLN:** 9110028271564

**GISA:** 32536911

**Corporate register number:** 524692g

**Corporate register court:** Landesgericht St. Pölten

**Company location:** 3345, Göstling an der Ybbs

**Phone:** +43 720 980 990

**Email:** [office@artichoke-computing.com](mailto:office@artichoke-computing.com)

**Member of:** WKO

**Laws re. professions:** Gewerbeordnung: [www.ris.bka.gv.at](http://www.ris.bka.gv.at)

**Supervisory/Trade authority:** Bezirkshauptmannschaft Scheibbs

**Awarding country:** Österreich

## Chief executive

Boris Johannes Fahrnberger, Raphael Pontus, Ferenc Ráduly

## Ownership structure

Boris Johannes Fahrnberger 40%, Raphael Pontus 20%, Martin Käfer 20%, Raphael Tobias Zöscher 20%

## Contact details of the data protection controller

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

Daniel Hauß, BA

E-Mail: [datenschutz@covidfighters.com](mailto:datenschutz@covidfighters.com)

Phone: +43 720 980 990

## EU Dispute Resolution

We would like to inform you about the Online Dispute Resolution platform (ODR platform) in

accordance with the regulation on Online Dispute Resolution in consumer matters (ODR Regulation).

Consumers have the option of submitting complaints to the European Commission's Online Dispute Resolution platform at <https://ec.europa.eu/consumers/odr/main/?event=main.home2.show>. You will find the necessary contact details in our imprint above.

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

## **Liability for the Contents of this Website**

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

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

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

## **Liability for Links on this Website**

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

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

## **Copyright Notice**

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

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

## **Picture Credits**

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

All texts are copyrighted.

# Privacy Policy

## Table of contents

- [Privacy Policy Introduction and Overview](#)
- [Scope](#)
- [Legal bases](#)
- [Contact details of the data protection controller](#)
- [Contact details of our data protection officer](#)
- [Storage Period](#)
- [Rights in accordance with the General Data Protection Regulation](#)
- [Data transfer to third countries](#)
- [Security of data processing operations](#)
- [Communications](#)
- [Data Processing Agreement \(DPA\)](#)
- [Cookies](#)
- [Web hosting](#)
- [Website Builders Introduction](#)
- [Web Analytics](#)
- [Email-Marketing](#)
- [Push Messages](#)
- [Messenger & Communication Introduction](#)
- [Social Media](#)
- [Online Marketing](#)
- [Cookie Consent Management Platform](#)
- [Payment providers](#)
- [Credit Checkers Introduction](#)
- [Audio & Video](#)
- [Recruiting Tools Privacy Policy](#)
- [Survey- and Poll Systems Overview](#)
- [Review Platforms Overview](#)
- [Miscellaneous Overview](#)

## Privacy Policy Introduction and Overview

We have written this privacy policy (version 18.08.2022-122087503) in order to explain to you, in accordance with the provisions of the [General Data Protection Regulation \(EU\) 2016/679](#) and applicable national laws, which personal data (data for short) we as the controller – and the processors commissioned by us (e.g. providers) – process, will process in the future and what legal options you have. The terms used are to be considered gender-neutral.

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

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

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

## Scope

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

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

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

## Legal bases

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

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

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

1. **Consent** (Article 6 Paragraph 1 lit. a GDPR): You have given us your consent to process data for a specific purpose. An example would be the storage of data you entered into a contact form.
2. **Contract** (Article 6 Paragraph 1 lit. b GDPR): We process your data in order to fulfill a contract or pre-contractual obligations with you. For example, if we conclude a sales contract with you,

we need personal information in advance.

3. **Legal obligation** (Article 6 Paragraph 1 lit. c GDPR): If we are subject to a legal obligation, we will process your data. For example, we are legally required to keep invoices for our bookkeeping. These usually contain personal data.
4. **Legitimate interests** (Article 6 Paragraph 1 lit. f GDPR): In the case of legitimate interests that do not restrict your basic rights, we reserve the right to process personal data. For example, we have to process certain data in order to be able to operate our website securely and economically. Therefore, the processing is a legitimate interest.

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

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

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

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

## Contact details of the data protection controller

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

Daniel Hauß, BA

E-Mail: [datenschutz@covidfighters.com](mailto:datenschutz@covidfighters.com)

Phone: [+43 720 980 990](tel:+43720980990)

## Contact details of our data protection officer

You can find the contact details of our data protection officer below:

E-Mail: [datenschutz@covidfighters.com](mailto:datenschutz@covidfighters.com)

Phone: [+43 720 980 990](tel:+43720980990)

## Storage Period

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

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

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

## **Rights in accordance with the General Data Protection Regulation**

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

- According to Article 15 DSGVO, you have the right to information about whether we are processing data about you. If this is the case, you have the right to receive a copy of the data and to know the following information:
  - for what purpose we are processing;
  - the categories, i.e. the types of data that are processed;
  - who receives this data and if the data is transferred to third countries, how security can be guaranteed;
  - how long the data will be stored;
  - the existence of the right to rectification, erasure or restriction of processing and the right to object to processing;
  - that you can lodge a complaint with a supervisory authority (links to these authorities can be found below);
  - the origin of the data if we have not collected it from you;
  - Whether profiling is carried out, i.e. whether data is automatically evaluated to arrive at a personal profile of you.
- You have a right to rectification of data according to Article 16 GDPR, which means that we must correct data if you find errors.
- You have the right to erasure (“right to be forgotten”) according to Article 17 GDPR, which specifically means that you may request the deletion of your data.
- According to Article 18 of the GDPR, you have the right to restriction of processing, which means that we may only store the data but not use it further.
- According to Article 20 of the GDPR, you have the right to data portability, which means that we will provide you with your data in a standard format upon request.
- According to Article 21 DSGVO, you have the right to object, which entails a change in processing after enforcement.
  - If the processing of your data is based on Article 6(1)(e) (public interest, exercise of official authority) or Article 6(1)(f) (legitimate interest), you may object to the processing. We will then check as soon as possible whether we can legally comply with this objection.
  - If data is used to conduct direct advertising, you may object to this type of data processing at any time. We may then no longer use your data for direct marketing.
  - If data is used to conduct profiling, you may object to this type of data processing at any time. We may no longer use your data for profiling thereafter.

- According to Article 22 of the GDPR, you may have the right not to be subject to a decision based solely on automated processing (for example, profiling).
- You have the right to lodge a complaint under Article 77 of the GDPR. This means that you can complain to the data protection authority at any time if you believe that the data processing of personal data violates the GDPR.

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

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

## **Austria Data protection authority**

**Manager:** Mag. Dr. Andrea Jelinek

**Address:** Barichgasse 40-42, 1030 Wien

**Phone number.:** +43 1 52 152-0

**E-mail address:** [dsb@dsb.gv.at](mailto:dsb@dsb.gv.at)

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

## **Data transfer to third countries**

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

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

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

# Security of data processing operations

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

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

## TLS encryption with https

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

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

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

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

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

## Communications

### Communications Overview

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

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

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

## **Affected persons**

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

## **Telephone**

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

## **Email**

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

## **Online forms**

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

## **Legal bases**

Data processing is based on the following legal bases:

- Art. 6 para. 1 lit. a GDPR (consent): You give us your consent to store your data and to continue to use it for the purposes of the business case;
- Art. 6 para. 1 lit. b GDPR (contract): For the performance of a contract with you or a processor such as a telephone provider, or if we have to process the data for pre-contractual activities, such as preparing an offer;
- Art. 6 para. 1 lit. f GDPR (legitimate interests): We want to conduct our customer inquiries and business communication in a professional manner. Thus, certain technical facilities such as email programs, Exchange servers and mobile network operators are necessary to efficiently operate our communications.

## **Data Processing Agreement (DPA)**

In this section, we would like to explain what a Data Processing Agreement is and why it is needed. As the term "Data Processing Agreement" is quite lengthy, we will often only use the acronym DPA here in this text. Like most companies, we do not work alone, but also use the services of other companies or individuals. By involving different companies or service providers, we may pass on personal data for processing. These partners then act as processors with whom we conclude a

contract, the so-called Data Processing Agreement (DPA). Most importantly for you to know is that any processing of your personal data takes place exclusively according to our instructions and must be regulated by the DPA.

## Who are the processors?

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

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

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

## Contents of a Data Processing Agreement

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

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

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

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

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

# Cookies

## Cookies Overview

 Affected parties: visitors to the website

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

 Processed data: depends on the cookie used. More details can be found below or from the manufacturer of the software that sets the cookie.

 Storage duration: can vary from hours to years, depending on the respective cookie

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

## What are cookies?

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

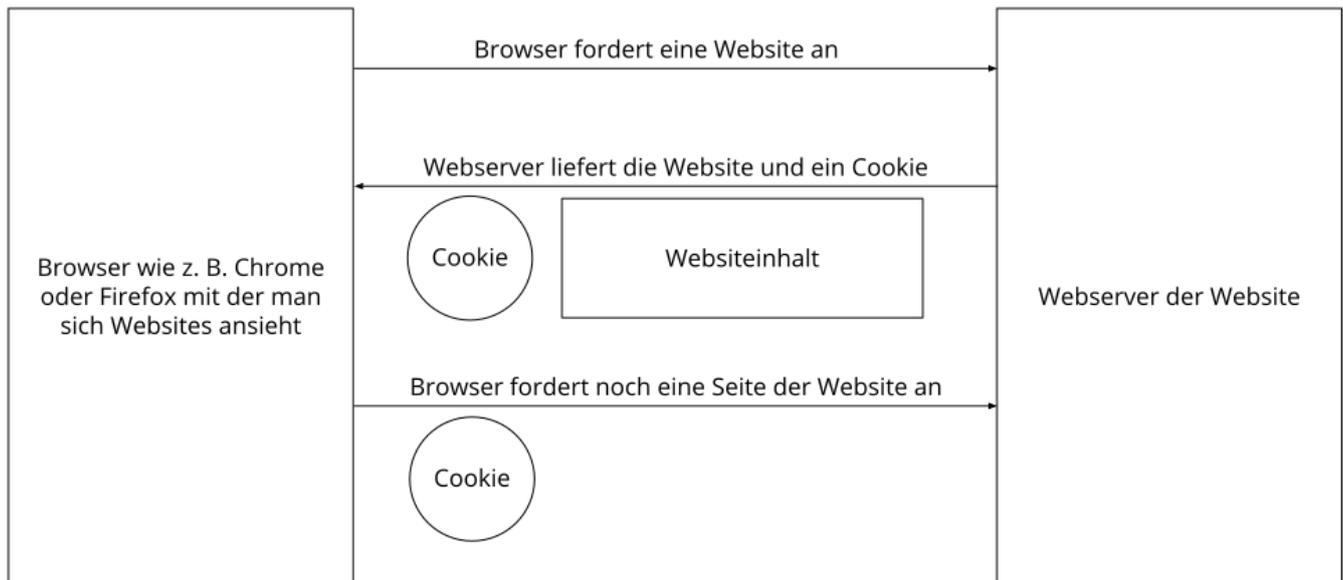
In the following we explain what cookies are and why they are used, so that you can better understand the following privacy policy.

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

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

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

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



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

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

**Name:** \_ga

**Value:** GA1.2.1326744211.152122087503-9

**Purpose:** Differentiation between website visitors

**Expiry date:** after 2 years

A browser should support these minimum sizes:

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

## Which types of cookies are there?

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

There are 4 different types of cookies:

### Essential cookies

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

### **Purposive cookies**

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

### **Target-orientated cookies**

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

### **Advertising cookies**

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

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

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

### **Purpose of processing via cookies**

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

### **Which data are processed?**

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

### **Storage period of cookies**

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

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

### **Right of objection – how can I erase cookies?**

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

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

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

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

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

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

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

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

## Legal basis

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

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

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

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

## Web hosting

### Web hosting Overview

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

## What is web hosting?

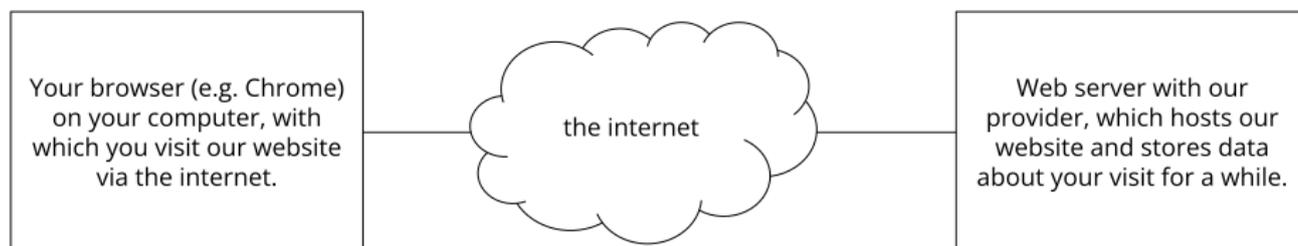
Every time you visit a website nowadays, certain information – including personal data – is automatically created and stored, including on this website. This data should be processed as sparingly as possible, and only with good reason. By website, we mean the entirety of all websites on your domain,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

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

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

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

Illustration:



## Why do we process personal data?

The purposes of data processing are:

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

## Which data are processed?

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

- the full address (URL) of the accessed website (e. g.

<https://www.examplepage.uk/examplesubpage.html?tid=122087503>)

- browser and browser version (e.g. Chrome 87)
- the operating system used (e.g. Windows 10)
- the address (URL) of the previously visited page (referrer URL) (e. g. <https://www.examplepage.uk/icamefromhere.html/>)
- the host name and the IP address of the device from the website is being accessed from (e.g. COMPUTERNAME and 194.23.43.121)
- date and time
- in so-called web server log files

## How long is the data stored?

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

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

## Legal basis

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

## Hetzner Privacy Policy

We use Hetzner for our website, which is a web hosting provider, among other things. The provider of this service is the German company Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany. You can find out more about the data that is processed through the use of Hetzner in their Privacy Policy at <https://www.hetzner.com/de/rechtliches/datenschutz>.

## Data Processing Agreement (DPA) Hetzner

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

This contract is required by law because Hetzner processes personal data on our behalf. It clarifies that Hetzner may only process data they receive from us according to our instructions and must comply with the GDPR. You can find the link to the Data Processing Agreement (DPA) under <https://docs.hetzner.com/de/general/general-terms-and-conditions/data-privacy-faq/>.

# Website Builders Introduction

## Website Builders Privacy Policy Overview

 Affected parties: website visitors

 Purpose: service optimisation

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

 Storage duration: depends on the provider

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

## What are website builders?

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

## Why do we use website builders for our website?

The greatest advantage of modular website builders is their ease of use. We want to offer you a clear, simple and nicely designed website that we can easily operate and maintain by ourselves – without needing any external support. Nowadays website builders offer many helpful functions that we can use even without having any programming knowledge. This enables us to design our website according to our wishes and therefore, to give you an informative and pleasant experience on our website.

## Which data are stored by website builders?

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

## How long and where are the data stored?

Provided that we have any further information on this, we will inform you below about the duration of the data processing associated with the website builder we use. You can find detailed

information on this in the provider's Privacy Policy. Generally, we only process personal data for as long as is absolutely necessary to provide our services and products. The provider may store your data according to their own specifications, over which we have no influence.

## Right to object

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

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

## Legal Bases

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

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

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

## Web Analytics

### Web Analytics Privacy Policy Overview

 Affected parties: visitors to the website

 Purpose: Evaluation of visitor information to optimise the website.

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

 Storage period: depending on the respective web analytics tool used

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

## What is Web Analytics?

We use software on our website, which is known as web analytics, in order to evaluate website visitor behaviour. Thus, data is collected, which the analytic tool provider (also called tracking tool) stores, manages and processes. Analyses of user behaviour on our website are created with this data, which we as the website operator receive. Most tools also offer various testing options. These

enable us, to for example test which offers or content our visitors prefer. For this, we may show you two different offers for a limited period of time. After the test (a so-called A/B test) we know which product or content our website visitors find more interesting. For such testing as well as for various other analyses, user profiles are created and the respective data is stored in cookies.

## **Why do we run Web Analytics?**

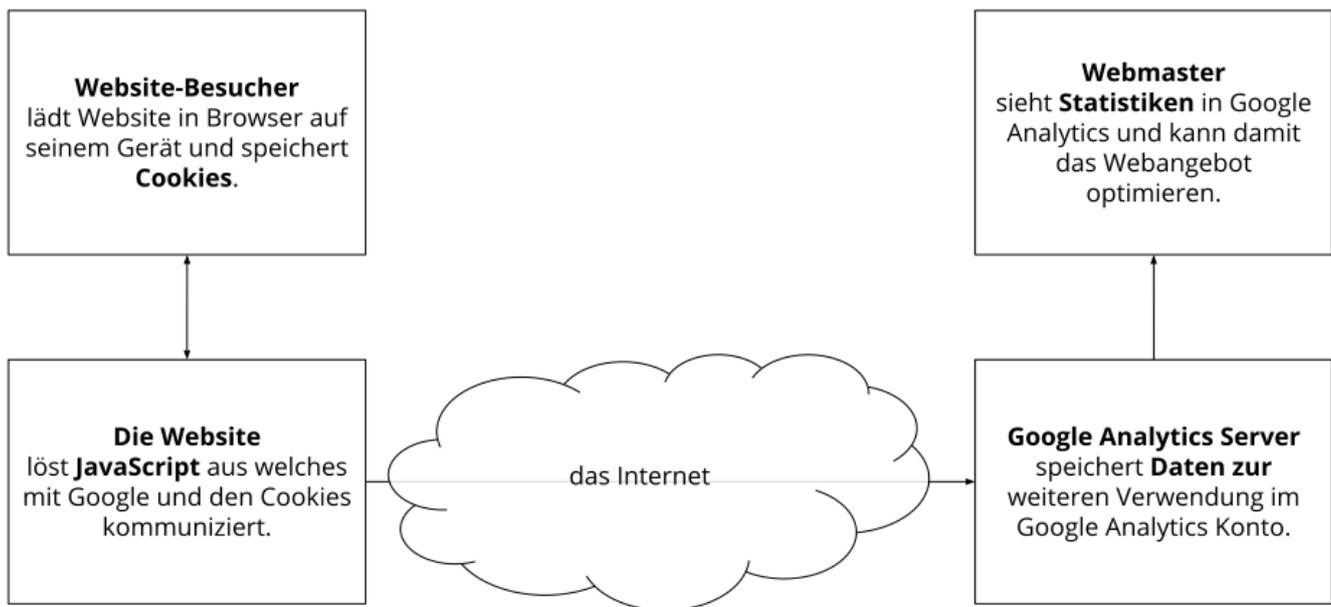
We have a clear goal in mind when it comes to our website: we want to offer our industry's best website on the market. Therefore, we want to give you both, the best and most interesting offer as well as comfort when you visit our website. With web analysis tools, we can observe the behaviour of our website visitors, and then improve our website accordingly for you and for us. For example, we can see the average age of our visitors, where they come from, the times our website gets visited the most, and which content or products are particularly popular. All this information helps us to optimise our website and adapt it to your needs, interests and wishes.

## **Which data are processed?**

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

Moreover, your IP address is also stored. According to the General Data Protection Regulation (GDPR), IP addresses are personal data. However, your IP address is usually stored in a pseudonymised form (i.e. in an unrecognisable and abbreviated form). No directly linkable data such as your name, age, address or email address are stored for testing purposes, web analyses and web optimisations. If this data is collected, it is retained in a pseudonymised form. Therefore, it cannot be used to identify you as a person.

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



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

## Duration of data processing

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

## Right to object

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

## Legal basis

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

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

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

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

## Jetpack Privacy Policy

### Jetpack Privacy Policy Overview

 Affected parties: visitors to the website

 Purpose: Evaluation of visitor information to optimise the website.

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

 Storage period: until the data is no longer required for the services

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

### What is Jetpack?

We use the WordPress plug-in Jetpack on our website. Jetpack is a software that provides us with an array of services such as web analyses. Jetpack is operated by Automattic (Inc. 132 Hawthorne Street San Francisco, CA 94107, USA), which uses Quantcast (Inc., 201 3rd St, Floor 2, San Francisco, CA 94103-3153, USA). The integrated tracking tool also collects, stores and processes your personal data. In this privacy policy, we will show you exactly which data are involved, why we use Jetpack and how you can prevent this data storage.

Jetpack is a plug-in for WordPress websites and has many different functions and modules. All these tools help us not only to design our website more beautifully, but also to make it safer and to welcome more visitors. Jetpack for example allows to display related posts and to share content. On top of that it can also improve our website's loading speed. All functions are hosted and provided by WordPress.

### Why do we use Jetpack?

It is crucial for us that you feel comfortable on our website and find what you are looking for. We can only be successful if you are satisfied with our services. And for us to know how and where we can improve our website, we need information. With Jetpack we can for example see how often and for how long you are on a single site or which buttons you tend to click. With the help of this information, we can improve our website and adapt it to your wishes and preferences.

### Which data are stored by Jetpack?

Your personal data will be identified, stored and processed, which is done especially through the built-in tracking tool WordPress.com-statistics. In order for Jetpack to work, Jetpack will set a cookie in your browser when you open a website with built-in components of the tool. The collected data will be synchronised with Automattic and stored there.

In addition to your IP address (which is anonymised before storage), the retained data includes data on your user behaviour, which is for example your browser type, unique device identifier, preferred language, the date and time of page entry, your operating system and information about your mobile network. Jetpack uses this information to improve its own services and offers and to get better insights on the use of its services. The following data may also be synchronised and stored:

- For Google Ads customers, email address and physical address of the account will be synchronised
- Successful and unsuccessful login attempts. Your IP address and the user agent will also be stored for this purpose
- User IDs, usernames, email addresses, roles, and skills of the registered users. However, no passwords will be retained
- The user ID of users who make changes to the website
- Twitter username, if it has been configured with Jetpack

Jetpack also uses cookies to store data. In the following we will show you a few exemplary cookies that Jetpack may use:

**Name:** eucookielaaw

**Value:** 1613651061376122087503-6

**Purpose:** Stores the status of the user's consent to the use of cookies.

**Expiry date:** after 180 days

**Name:** tk\_ai

**Value:** 0

**Purpose:** This cookie stores a randomly generated anonymous ID. It is only used within the admin area to keep track of general analyses.

**Expiry date:** after end of the session

**Name:** tk\_tc

**Value:** E3%2Bgj1Pw6iYKk%2Fvj122087503-3

**Purpose:** This is a so-called referral cookie. With it, the connection between WooCommerce and a website with a Jetpack plugin is analysed.

**Expiry date:** after end of the session

**Note:** Jetpack uses many different cookies. Which cookies are actually used depends on what Jetpack functions are used and on what your actions are on the websites that have an integrated Jetpack plug-in. At <https://jetpack.com/support/cookies/> you will see a list of possible cookies used by Jetpack.

## How long and where are the data stored?

Automattic retains the collected data until it is no longer used for its own services. Beyond this period, your data will only stay stored if the company is obliged to keep it for legal reasons. Certain data are deleted after about 30 days. These include web server logs such as your IP address,

browser type and operating system. The data are stored on the company's American servers.

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

As mentioned above, Jetpack uses cookies to retain data. If you do not want Jetpack to collect your data in the future, you can request an "Opt-Out" cookie at <https://www.quantcast.com/opt-out/>. Quantcast will then place this cookie and none of your visitor data will be stored. This will be the case until you delete this cookie again.

Alternatively, you can easily manage, deactivate or delete cookies yourself in your browser if you want to. Cookie management works a little differently depending on the browser type you are using. In the following, you will find instructions to do this in the most common browsers.

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

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

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

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

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

## Legal basis

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

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

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

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

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

If you want to find out more about the privacy guidelines and data processing by Jetpack or Automattic, we recommend you to read the privacy policy at <https://automattic.com/privacy/>, the cookie guidelines at <https://automattic.com/cookies/> and also the information page at <https://jetpack.com/support/what-data-does-jetpack-sync/>. We hope we could provide you with a good overview on Jetpack's data processing.

## Email-Marketing

### Email Marketing Overview

 Affected parties: newsletter subscribers

 Purpose: direct marketing via email, notification of events that are relevant to the system

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

 Storage duration: for the duration of the subscription

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

### What is Email-Marketing?

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

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

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

### Why do we use Email-Marketing?

Of course, we want to stay in contact with you and keep you in the loop of the most important news about our company. For this, we use email marketing – often just referred to as "newsletters" – as an essential part of our online marketing. If you agree to this or if it is permitted by law, we will send you newsletters, system emails or other notifications via email. Whenever the term "newsletter" is used in the following text, it mainly refers to emails that are sent regularly. We of course don't want to bother you with our newsletter in any way. Thus, we genuinely strive to offer only relevant and interesting content. In our emails you can e.g. find out more about our company

and our services or products. Since we are continuously improving our offer, our newsletter will always give you the latest news, or special, lucrative promotions. Should we commission a service provider for our email marketing, who offers a professional mailing tool, we do this in order to offer you fast and secure newsletters. The purpose of our email marketing is to inform you about new offers and also to get closer to our business goals.

## **Which data are processed?**

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

## **Duration of data processing**

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

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

## **Withdrawal – how can I cancel my subscription?**

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

## **Legal basis**

Our newsletter is sent on the basis of your **consent** (Article 6 (1) (a) GDPR). This means that we are only allowed to send you a newsletter if you have actively registered for it beforehand. Moreover, we may also send you advertising messages on the basis of Section 7 (3) UWG (Unfair Competition Act), provided you have become our customer and have not objected to the use of your email address for direct mail.

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

# Mailgun Privacy Policy

On our website we use Mailgun, which is a service for our email marketing. The provider of this service is the American company Mailgun Technologies Inc., 112 E Pecan St #1135, San Antonio, TX 78205, US.

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

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

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

In Mailgun's privacy policy at <https://www.activecampaign.com/legal/privacy-policy>, you can find out more about the data that are being processed by using Mailgun.

## Push Messages

### Push Messages Overview

-  Affected parties: subscribers to push messages
-  Purpose: to notify you about interesting events that are relevant to the system
-  Processed data: data that was entered during registration, usually also location data. You can find more details on this at the respective push notification tool.
-  Storage period: data are usually stored for as long as is necessary for the service provision.
-  Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. b GDPR (contract)

## What are push notifications?

We use so-called push notification services on our website, which help us to keep our users up to date. Thus, if you have agreed to the use of such push notifications, we can send you short news using a software tool. Push messages are text messages that appear on your smartphone or on other devices such as tablets or PCs, provided you have registered for them. You can also receive these messages if you are not on our website at this point in time, or are not actively using our offer. Moreover, data about your location and your user behaviour may also be collected and stored.

## Why do we use push notifications?

On the one hand, we use push notifications to be able to fully provide the services we have contractually agreed to with you. On the other hand, they are helpful to our online marketing. This

is because we can show you our services or products better with them. Thus, we can inform you immediately if there is e.g. any news in our company. We also want to get to know our users' preferences and habits as well as possible, in order to continuously improve our offer.

## **Which data are processed?**

For you to receive push notifications, you must confirm that you want to receive them. Any data accumulated during the process of confirming your consent is stored, managed and processed. This is necessary to recognise and proof users' consent to receiving push notifications. Hence, a so-called device token or push token is stored in your browser. Along with this, your location data or the location of your device are usually also retained.

We also statistically evaluate how you handle our messages, so we can always send you push messages that are important and interesting. Thus, we can e.g. see when you open a message. With this knowledge we can adapt our communication strategy to your wishes and interests. Although this stored data could be assigned to you, we do not want to screen you as an individual. Rather, we are interested in the collected data from all our users so we can optimise further. In the privacy policies of the respective service providers, you can find out which data is stored exactly.

## **Duration of data processing**

The duration of data processing and retention depends primarily on the tool we use. Below you can find out more about data processing of the individual tools. The providers' privacy policies usually state exactly which data is stored and processed and for how long. Generally, 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 duration can vary greatly. On the one hand, this data may be deleted immediately after leaving a website, and on the other hand it may get stored for several years. Therefore, if you want to know more about data storage, you should look at each individual cookie in detail. In most cases, you will also find informative information on individual cookies in the privacy policies of the respective providers.

## **Legal basis**

It may be possible, that push messages may be necessary for us to be able to fulfill certain obligations in a contract. An example would be us notifying you about technical or organisational news. In this case, the legal basis is Art. 6 paragraph 1 lit. b of the GDPR.

Should this not be the case, push notifications will only be sent on the basis of your consent. Our push messages may particularly include advertising content. Furthermore, push notifications may also be sent depending on your location displayed on your device. The above-mentioned analytical evaluations are also based on your consent to their receipt. The legal basis for this is Article 6 (1) (a) of the GDPR. Of course, you can either revoke your consent at any time in the settings, or change various settings.

# Firestore Cloud-Messaging Privacy Policy

For our website, we use Firestore Cloud-Messaging, a cross-platform messaging solution. The provider of this service is the American company Google Inc. The responsible party for all Google service in Europe, is Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland).

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

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

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

The data processing agreement, which refers to the standard contractual clauses, can be found at <https://firebase.google.com/terms/firebase-sccs-eu-c2p>.

You can find out more on Firestore's data processing in their Privacy Policy at <https://policies.google.com/privacy>.

## Messenger & Communication Introduction

### Messenger & Communication Privacy Statement Overview

 Affected parties: website visitors

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

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

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

 Storage duration: depends on the messenger & communication functions

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

## What are Messenger & Communication functions?

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

In addition to classic means of communication such as email, contact forms or telephone, we also use chats or messengers. The most commonly used messenger function at the moment is

WhatsApp, but of course, there are many different providers who offer messenger functions for websites. If content is end-to-end encrypted, it will be indicated in our individual privacy policies or in the privacy policy of the respective provider. End-to-end encryption means that the content of a message is not visible to the provider themselves. However, information about your device, location settings and other technical data can still be processed and stored.

## **Why do we use Messenger & Communication functions?**

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

We generally assume our responsibility under data protection law, even if we use the services of any social media platform. However, the European Court of Justice has decided that in certain cases the operator of the social media platform be jointly responsible alongside us in the scope of Art. 26 GDPR. Should this be the case, we will point it out separately and work on the basis of a relevant agreement. You will find the essence of the agreement for the respective platforms below.

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

## **Which data is processed?**

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

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

## **How long is data stored?**

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

know more about data storage. In most cases, you will also find helpful information about individual cookies in the privacy policies of the individual providers.

## Right to object

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

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

## Legal Basis

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

## HubSpot Customer Service Privacy Policy

We use HubSpot on our website, which is a customer service tool among other things. The provider of this service is the American company HubSpot, Inc., 25 First St 2nd Floor Cambridge, MA, USA. The company also has headquarters in Ireland at 1 Sir John Rogerson's Quay, Dublin 2, Ireland.

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

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

clauses here: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847).

Their Data Processing Agreement, which corresponds to the standard contractual clauses, can be found at <https://legal.hubspot.com/dpa>.

You can find out more about the data that is processed by using HubSpot in their Privacy Policy at <https://legal.hubspot.com/privacy-policy>.

## **HubSpot (Chatbot) Privacy Policy**

We also use the chatbot function HubSpot. The provider of this service is the American company HubSpot, Inc., 25 First St., 2nd floor, Cambridge, Massachusetts 02141, USA.

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

HubSpot uses standard contractual clauses approved by the EU Commission as the basis for data processing by recipients based in third countries (i. e. outside the European Union, Iceland, Liechtenstein, Norway, and thus especially in the USA) or data transfer there (= Art. 46, paragraphs 2 and 3 of the GDPR). Standard Contractual Clauses (SCC) are legal templates provided by the EU Commission. Their purpose is to ensure that your data complies with European data privacy standards, even if your data is transferred to and stored in third countries (such as the USA). With these clauses, HubSpot commits to comply with the EU's level of data protection when processing relevant data, even if it is stored, processed and managed in the USA. These clauses are based on an implementing order by the EU Commission. You can find the order and the standard contractual clauses here: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847).

You can find HubSpot's Data Processing Agreement, which corresponds to the standard contractual clauses at <https://legal.hubspot.com/dpa>.

You can find out more about the data that is processed by using HubSpot in their Privacy Policy at <https://legal.hubspot.com/privacy-policy>.

## **Data Processing Agreement (DPA) HubSpot (Chatbot)**

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

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

# Social Media

## Social Media Privacy Policy Overview

 Affected parties: website visitors

 Purpose: Service presentation and optimisation, staying in contact with visitors, interested parties, etc. as well as advertising

 Processed data: data such as telephone numbers, email addresses, contact data, data on user behaviour, information about your device and your IP address.

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

 Storage period: depending on the social media platforms used

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

## What is Social Media?

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

## Why do we use Social Media?

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

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

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

Please note that when you use social media platforms or our built-in elements, your data may also be processed outside the European Union, as many social media channels, such as Facebook or

Twitter, are American companies. As a result, you may no longer be able to easily claim or enforce your rights regarding your personal data.

## **Which data are processed?**

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

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

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

## **Duration of data processing**

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

## **Right to object**

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

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

## **Legal basis**

If you have consented to the processing and storage of your data by integrated social media elements, this consent serves as the legal basis for data processing (**Art. 6 para. 1 lit. a GDPR**). Generally, provided you have given your consent, your data will also be stored and processed on

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

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

## Facebook Privacy Policy

### Facebook Privacy Policy Overview

 Affected parties: website visitors

 Purpose: service optimisation

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

You can find more details in the Privacy Policy below.

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

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

### What are Facebook tools?

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

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

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

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

- Facebook-Pixel

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

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

## **Why do we use Facebook tools on our website?**

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

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

## **What data is stored by Facebook tools?**

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

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

Moreover, not only contact data, but also “event data” is transferred. These data are the information we receive about you on our website. To give an example, it allows us to see what subpages you visit or what products you buy from us. Facebook does not disclose the obtained information to third parties (such as advertisers), unless the company has an explicit permission or

is legally obliged to do so. Also, “event data” can be linked to contact information, which helps Facebook to offer improved, customised adverts. Finally, after the previously mentioned matching process, Facebook deletes the contact data.

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

## **How long and where are the data stored?**

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

## **How can I erase my data or prevent data retention?**

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

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

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

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

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

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

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

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

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

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

## Legal basis

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

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

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

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

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

## Instagram Privacy Policy

### Instagram Privacy Policy Overview

 Affected parties: website visitors

 Purpose: optimising our service

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

More details can be found in the privacy policy below.

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

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

## **What is Instagram?**

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

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

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

## **Why do we use Instagram on our website?**

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

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

## **What data is stored by Instagram?**

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

Facebook distinguishes between customer data and event data. We assume this is also the case for

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

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

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

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

The following cookies were used in our test:

**Name:** csrftoken

**Value:** ""

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

**Expiry date:** after one year

**Name:** mid

**Value:** ""

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

**Expiry date:** after end of session

**Name:** fbsr\_122087503124024

**Value:** no information

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

**Expiry date:** after end of session

**Name:** rur

**Value:** ATN

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

**Expiry date:** after end of session

**Name:** urlgen

**Value:** "{194.96.75.33": 1901};1iEtYv:Y833k2\_UjKvXgYe122087503"

**Purpose:** This cookie serves Instagram's marketing purposes.

**Expiry date:** after end of session

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

## How long and where are these data stored?

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

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

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

And this is how an Instagram account can be deleted:

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

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

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

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

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

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

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

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

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

## Legal basis

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

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

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

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

We have tried to give you the most important information about data processing by Instagram. On <https://help.instagram.com/519522125107875> you can take a closer look at Instagram's data guidelines.

## LinkedIn Privacy Policy

### LinkedIn Privacy Policy Overview

-  Affected parties: website visitors
-  Purpose: optimisation of our service
-  Processed data: includes data on user behaviour, information about your device and IP address.  
More details can be found in the privacy policy below.
-  Storage period: the data is generally deleted within 30 days
-  Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

## What is LinkedIn?

On our website we use social plugins from the social media network LinkedIn, of the LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA. Social plugins can be feeds, content sharing or a link to our LinkedIn page. Social plugins are clearly marked with the well-known LinkedIn logo and for example allow sharing interesting content directly via our website.

Moreover, LinkedIn Ireland Unlimited Company Wilton Place in Dublin is responsible for data processing in the European Economic Area and Switzerland.

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

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

### **Why do we use LinkedIn on our website?**

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

### **What data are stored by LinkedIn?**

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

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

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

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

**Name:** bcookie

**Value:** =2&34aab2aa-2ae1-4d2a-8baf-c2e2d7235c16122087503-

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

**Expiry date:** after 2 years

**Name:** lang

**Value:** v=2&lang=en-gb

**Purpose:** This cookie saves your default or preferred language.

**Expiry date:** after end of session

**Name:** lidc

**Value:** 1818367:t=1571904767:s=AQF6KNnJ0G122087503...

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

**Expiry date:** after 24 hours

**Name:** rtc

**Value:** kt0Irv3NF3x3t6xvDgGrZGDkKX

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

**Expiry date:** after 2 minutes

**Name:** JSESSIONID

**Value:** ajax:1220875032900777718326218137

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

**Expiry date:** after end of session

**Name:** bscookie

**Value:** "v=1&201910230812...

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

**Expiry date:** after 2 years

**Name:** fid

**Value:** AQHj7li23ZBcqAAAA...

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

**Expiry date:** after 7 days

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

## How long and where are the data stored?

In general, LinkedIn retains your personal data for as long as the company considers it necessary for providing its services. However, LinkedIn deletes your personal data when you delete your account. In some exceptional cases, LinkedIn keeps some summarised and anonymised data, even account deletions. As soon as you delete your account, it may take up to a day until other people

can no longer see your data. LinkedIn generally deletes the data within 30 days. However, LinkedIn retains data if it is necessary for legal reasons. Also, data that can no longer be assigned to any person remains stored even after the account is closed. The data are stored on various servers in America and presumably also in Europe.

## How can I delete my data or prevent data retention?

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

How to access account data in your LinkedIn profile:

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

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

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

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

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

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

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

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

## Legal basis

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

LinkedIn also processes data in the USA, among other countries. We would like to note, that

according to the European Court of Justice, there is currently no adequate level of protection for data transfers to the USA. This can be associated with various risks to the legality and security of data processing.

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

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

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

## Online Marketing

### Online Marketing Privacy Policy Overview

 Affected parties: visitors to the website

 Purpose: Evaluation of visitor information for website optimisation

 Processed data: Access statistics containing data such as access location, device data, access duration and time, navigation behaviour, click behaviour and IP addresses. Personal data such as name or email address may also be processed. You can find more details on this from the respective Online Marketing tool.

 Storage period: depending on the Online Marketing tools used

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

## What is Online Marketing?

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

## Why do we use Online Marketing tools?

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

to our target group. The ultimate purpose of these Online Marketing tools is to optimise our offer.

## **Which data are processed?**

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

Your IP address is stored in pseudonymised form (i.e. shortened). What is more, distinct data that directly identify you as a person, such as your name, address or email address, are only stored in pseudonymised for advertising and Online Marketing purposes. With this data we cannot identify you as a person and only retain the pseudonymised information that is stored in your user profile.

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

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

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

## **Duration of data processing**

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

## **Right of withdrawal**

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

providers at any time. This can be done either via our cookie management tool or via other opt-out functions. You can for example also prevent data collection by cookies if you manage, deactivate or erase cookies in your browser. The legality of the processing remains unaffected to the point of revocation.

Since Online Marketing tools usually use cookies, we also recommend you to read our privacy policy on cookies. If you want to find out which of your data is stored and processed, you should read the privacy policies of the respective tools.

## Legal basis

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

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

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

## Google Ads (Google AdWords) Conversion Tracking Privacy Policy

### Google Ads (Google AdWords) Conversion Tracking Privacy Policy Overview

 Affected parties: visitors to the website

 Purpose: economic success and service optimisation.

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

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

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

## What is Google Ads conversion tracking?

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

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

But what is a conversion actually? A conversion occurs, when you turn from an interested visitor into an acting website visitor. This happens every time you click on our ad and then make another action, such as paying a visit to our website. With Google's conversion tracking tool, we can understand what happens after a user clicks our Google ad. It shows us for instance if products get bought, services are used or whether users have subscribed to our newsletter.

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

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

## **What data is stored with Google Ads conversion tracking?**

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

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

**Name:** Conversion

**Value:** EhMI\_aySuoyv4gIVled3Ch0llweVGAEgt-mr6aXd7dYISAGQ122087503-3

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

**Expiry date:** after 3 months

**Name:** \_gac

**Value:** 1.1558695989.EAlalQobChMliOmEgYO04gIVj5AYCh2CBAPrEAAYASAAEgIYQfD\_BwE

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

**Expiry date:** after 3 months

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

As soon as you complete an action on our website, Google identifies the cookie and saves your action as a so-called conversion. For as long as you surf our website, provided the cookie has not

expired, both Google and us can determine that you found your way to us via a Google ad. Then, the cookie is read and sent back to Google Ads, together with the conversion data. Moreover, other cookies may also be used for measuring conversions. Google Ads' conversion tracking can be fine-tuned and improved with the aid of Google Analytics. Furthermore, ads which Google displays in various places across the web, might be placed under our domain with the name “\_\_gads” or “\_gac”. Since September 2017, analytics.js retains various campaign information with the \_gac cookie. This cookie stores data, as soon as you open one of our sites that has been set up for Google Ads' auto-tagging. In contrast to cookies that are placed for Google domains, Google can only read these conversion cookies when you are on our website. We do neither collect nor receive any personal data. We do obtain a report with statistical evaluations by Google. With the help thereof, we can not only see the total number of users who clicked our ad, but also what advertising measures were well received.

## **How long and where is the data stored?**

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

## **How can I erase my data or prevent data retention?**

You have the possibility to opt out of Google Ads' conversion tracking. The conversion tracking can be blocked by deactivating the conversion tracking cookie via your browser. If you do this, you will not be considered for the statistic of the tracking tool. You can change the cookie settings in your browser anytime. Doing so, works a little different in every browser. Hence, in the following you will find an instruction on how to manage cookies in your browser:

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

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

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

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

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

If you generally do not want to allow any cookies at all, you can set up your browser to notify you whenever a potential cookie is about to be set. This lets you decide upon permitting or denying the cookie's placement. By downloading and installing the browser plugin at <https://support.google.com/ads/answer/7395996> you can also deactivate all “advertising cookies”. Please consider that by deactivating these cookies, you cannot prevent all advertisements, only personalised ads.

## Legal basis

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

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

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

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

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

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

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

## HubSpot privacy policy

On our website, we use HubSpot, which is a tool for digital marketing. The provider of this service is the American company HubSpot Inc.. The responsible entity for the European region is the Irish company HubSpot (1 Sir John Rogerson's Quay, Dublin 2, Ireland).

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

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

EU Commission. You can find the order and the clauses here:

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

You can find out more about HubSpot's data processing in their privacy policy at

<https://legal.hubspot.com/de/privacy-policy>.

## Data Processing Agreement (DPA) HubSpot

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

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

<https://legal.hubspot.com/dpa>.

## Cookie Consent Management Platform

### Cookie Consent Management Platform Overview

 Affected parties: Website visitors

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

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

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

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

## What is a cookie consent management platform?

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



## Why do we use a cookie management tool?

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

## Which data are processed?

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

## Duration of data processing

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

## Right of objection

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

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

## Legal basis

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

## AdSimple Cookie Manager Privacy Policy

### AdSimple Cookie Manager Privacy Policy Overview

 Affected parties: Website visitors

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

 Processed data: data for managing cookie settings such as IP address, time of consent, type of consent and individual consent. You can find more details on this under in the privacy policy below.

 Storage period: the used cookie expires after one year

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

## What is the AdSimple Cookie Manager?

On our website we use the AdSimple Cookie Manager of the software development and online marketing company AdSimple GmbH, Fabriksgasse 20, 2230 Gänserndorf, Austria. The AdSimple Cookie Manager offers us, among other things, the opportunity to provide you with a cookie notice that is comprehensive and compliant with data protection laws. This gives you the opportunity to decide which cookies you want to allow or deny. By using this software, data is sent from you to AdSimple, where it is stored. In this privacy policy we inform you on why we use the AdSimple Cookie Manager, which data is transferred and stored and how you can prevent this data transfer.

The AdSimple Cookie Manager is a software that scans our website to identify and categorise all existing cookies. Additionally, you as the website visitor will be informed on the use of cookies via a cookie notice script. Then you can decide yourself which cookies you want to allow or deny.

## Why do we use the AdSimple Cookie Manager on your website?

We want to offer you maximum transparency when it comes to data protection. Before we can do so, we need to exactly determine which cookies have ended up on our website over time. Since the AdSimple cookie manager regularly scans our website and locates all cookies, we have full control over these cookies and can therefore act in compliance with the GDPR. This enables us to inform you precisely on the use of cookies on our website.

Moreover, you will always receive an up-to-date cookie notice that is data-protection compliant. This enables you to decide yourself which cookies you want to allow or deny via the checkbox system.

## Which data are stored by the AdSimple Cookie Manager?

If you agree to cookies on our website, AdSimple Cookie Manager will set the following cookie:

**Name:** acm\_status

**Value:** `":true,"statistics":true,"marketing":true,"socialmedia":true,"settings":true}`

**Purpose:** This cookie saves the status of your consent. This enables our website to read and adhere to the latest status, even during future visits.

**Expiry date:** after one year

## How long and where are the data stored?

All data collected by the AdSimple Cookie Manager is transferred and stored exclusively within the European Union. The collected data is stored on the AdSimple servers at Hetzner GmbH in Germany. Therefore, only AdSimple GmbH and Hetzner GmbH have access to the data.

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

You have the right to access and delete your personal data at any time. You can prevent data collection and storage by for example rejecting the use of cookies via the cookie notification script. Another option to prevent data processing or to manage it according to your wishes is your browser. Depending on the browser you use, managing cookies differs slightly. Below you will find links to the instructions for the most common browsers:

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

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

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

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

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

## Legal basis

If you agree to cookies, your personal data will be processed and stored via these cookies. If we are allowed to use cookies with your **consent** (Article 6 (1) (a) GDPR), this consent is also the legal basis for the use of cookies and the processing of your data. The AdSimple Cookie Manager 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 is a **legitimate interest** (Article 6 (1) lit.f GDPR).

We hope we were able to provide you with a good overview of data traffic and data processing by AdSimple Cookie Manager. If you want to learn more about this tool, we recommend the description page at <https://www.adsimple.at/adsimple-cookie-manager/>.

## Payment providers

### Payment Providers Privacy Policy Overview

 Affected parties: visitors to the website

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

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

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

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

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

## What is a payment provider?

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

## Why do we use payment providers on our website?

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

## Which data are processed?

What exact data that is processed of course depends on the respective payment provider.

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

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

## **Duration of data processing**

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

## **Right to object**

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

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

## **Legal basis**

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

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

## PayPal Privacy Policy

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

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

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

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

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

## Shop Pay Privacy Policy

On our website we use Shop Pay, which is a service for online payment solutions. The provider of this service is the American company Shopify Inc. The responsible entity for the European region is the company Shopify International Limited (Victoria Buildings, 2nd floor, 1-2 Haddington Road, Dublin 4, D04 XN32, Ireland).

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

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

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

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

# Stripe Privacy Policy

## Stripe Privacy Policy Overview

 Affected parties: website visitors

 Purpose: optimising the payment process on our website

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

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

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

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

## What is Stripe?

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

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

## Why do we use Stripe on our website?

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

## What data are stored by Stripe?

If you choose Stripe as your payment method, your personal data (transaction data) will be transmitted to Stripe where it will be stored. These data include the payment method (i.e. credit card, debit card or account number), bank sort code, currency, as well as the amount and the payment date. During a transaction, your name, email address, billing or shipping address and sometimes your transaction history may also be transmitted. These data are necessary for authentication. Furthermore, Stripe may also collect relevant data for the purpose of fraud prevention, financial reporting and for providing its services in full. These data may include your name, address, telephone number as well as your country in addition to technical data about your device (such as your IP address).

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

**Name:** m

**Value:** edd716e9-d28b-46f7-8a55-e05f1779e84e040456122087503-5

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

**Expiry date:** after 2 years

**Name:** \_\_stripe\_mid

**Value:** fc30f52c-b006-4722-af61-a7419a5b8819875de9122087503-1

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

**Expiry date:** after one year

**Name:** \_\_stripe\_sid

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

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

**Expiry date:** after end of the session

## How long and where are the data stored?

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

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

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

You always reserve the right to information, correction and deletion of your personal data. Should you have any questions, you can contact the Stripe team at

<https://support.stripe.com/contact/email>.

You can erase, deactivate or manage cookies in your browser that Stripe uses for its functions. This works differently depending on which browser you are using. Please note, however, that if you do

so the payment process may no longer work. The following instructions will show you how to manage cookies in your browser:

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

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

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

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

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

## Legal basis

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

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

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

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

We have now given you a general overview of Stripe's data processing and retention. If you want more information, Stripe's detailed privacy policy at <https://stripe.com/at/privacy> is a good source.

## shopify Privacy Policy

We use the online marketplace shopify. The provider of this service is the American company Shopify International Limited, Victoria Buildings, 2nd floor, 1-2 Haddington Road, Dublin 4, D04 XN32, Ireland.

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

shopify uses standard contractual clauses approved by the EU Commission as the basis for data processing by recipients based in third countries (i. e. outside the European Union, Iceland, Liechtenstein, Norway, and thus especially in the USA) or data transfer there (= Art. 46, paragraphs 2 and 3 of the GDPR). Standard Contractual Clauses (SCC) are legal templates provided by the EU Commission. Their purpose is to ensure that your data complies with European data privacy standards, even if your data is transferred to and stored in third countries (such as the USA). With these clauses, shopify commits to comply with the EU's level of data protection when processing relevant data, even if it is stored, processed and managed in the USA. These clauses are based on an implementing order by the EU Commission. You can find the order and the standard contractual clauses here: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847).

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

## Credit Checkers Introduction

### Credit Checkers Privacy Policy Overview

 Affected parties: Customers

 Purpose: Credit score and credit rating

 Processed data: inventory data, payment data, contact data, contract data

 Storage duration: depends on the test centers used

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

### What are credit check agencies?

In some cases, we use credit check agencies for our online transactions so that we can obtain information about your creditworthiness if we pay in advance. The test centers calculate a statistical probability of non-payment. This means we receive information about how likely it is that you will be able to pay your bill, for example. This information enables us to better decide whether or not to make certain advance payments. We can therefore also refuse advance payments (such as paying on account) if the result of the credit check is negative.

### Why do we use credit check agencies?

In our business, it often happens that we perform a service before the contractually stipulated consideration or accept similar economic risks. This is always the case with an order on account. In order to protect our legitimate interests, we can obtain so-called identity and creditworthiness information. The credit risk is assessed using a mathematical-statistical process by credit rating agencies (credit agencies).

### What data is processed?

The decision to pay in advance or not is made by software that works with the information from the credit check office on the basis of an automated decision on a case-by-case basis (= Art. 22 GDPR). The data that is usually processed includes name, address, bank details, invoices, payment history,

contact details such as email address and telephone number, as well as contract data such as term, customer information and the subject matter of the contract. You can find more information about data processing in the data protection declarations of the respective credit rating agencies.

## Duration of data processing

How long the data is processed and stored depends mainly on the credit check agencies we use. Below you can find out more about the data processing of the individual providers. The data protection declarations of the providers usually state exactly which data is stored and processed for how long. In principle, personal data is only processed for as long as is necessary to provide our services. When data is stored in cookies, the storage period varies greatly. In most cases, you will also find informative information about the individual cookies in the data protection declarations of the individual providers.

## Legal Basis

If we obtain consent from our contractual partners, this is also the legal basis (Article 6 Paragraph 1 lit. a GDPR) for the credit report and also for the data transmission of the customer to a testing agency. If this consent does not exist, the legal basis is our legitimate interest (Article 6 Paragraph 1 lit. f GDPR) in failsafety. If we obtain your consent, this is also the legal basis for creditworthiness information and data transmission.

We have no influence on the specific verification process or the profiling of the credit assessment agencies we use and thus on the correctness or appropriateness of the result. In this respect, we are not responsible under data protection law. In this respect, the responsibility remains solely with the credit check office, to whose data protection information we refer below. We are only responsible for obtaining and using a credit report prepared by a third party in individual cases.

## KSV1870 Privacy Policy

We use KSV1870 for our business, which is a credit check agency. The provider of this service is the Austrian company KSV1870 Holding AG, Wagenseilgasse 7, 1120 Vienna, Austria. You can find out more about the data that is processed by using KSV1870 in their Privacy Policy at <https://www.ksv.at/en/data-protection-notice>.

## Audio & Video

### Audio & Video Privacy Policy Overview

 Affected parties: website visitors

 Purpose: service optimisation

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

You can find more details in the Privacy Policy below.

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

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

## **What are audio and video elements?**

We have integrated audio and video elements to our website. Therefore, you can watch videos or listen to music/podcasts directly via our website. This content is delivered by service providers and is obtained from the respective providers' servers.

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

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

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

We of course want to provide you with the best offer on our website. And we are aware that content is no longer just conveyed in text and static images. Instead of just giving you a link to a video, we offer you audio and video formats directly on our website. These are entertaining or informative, but ideally they are both. Our service therefore gets expanded and it gets easier for you to access interesting content. In addition to our texts and images, we thus also offer video and/or audio content.

## **Which data are retained by audio & video elements?**

When you visit a page on our website with e.g. an embedded video, your server connects to the service provider's server. Thus, your data will also be transferred to the third-party provider, where it will be stored. Certain data is collected and stored regardless of whether you have an account with the third party provider or not. This usually includes your IP address, browser type, operating system and other general information about your device. Most providers also collect information on your web activity. This e.g. includes the session duration, bounce rate, the buttons you clicked or information about the website you are using the service on. This data is mostly stored via cookies or pixel tags (also known as web beacons). Any data that is pseudonymised usually gets stored in your browser via cookies. In the respective provider's Privacy Policy, you can always find more information on the data that is stored and processed.

## **Duration of data processing**

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

## Right to object

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

Since the integrated audio and video functions on our site usually also use cookies, we recommend you to also read our general Privacy Policy on cookies. You can find out more about the handling and storage of your data in the Privacy Policies of the respective third party providers.

## Legal basis

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

## Recruiting Tools Privacy Policy

### Recruiting Tools Privacy Policy Overview

 Affected parties: Users who conduct a job application process online or use a recruiting tool

 Purpose: job application process handling

 Processed data: data such as name, address, contact details, email address or telephone number. You can find more details about this directly from the respective recruiting tool.

 Storage period: if the application is successful, data is retained until the end of the employment relationship. Otherwise the data will be erased after the application process.

 Legal bases: Art. 6 paragraph 1 lit. a GDPR (consent), Art. 6 paragraph 1 lit. b GDPR (contract), Art. 9 paragraph 2 lit. a. GDPR (processing of special categories)

## What are recruiting tools?

Various companies offer software programs that can make application processes much easier. Most systems offer options to filter searches through databases of potential candidates. This enables us to quickly and efficiently find employees who are a great fit for our company. When using recruiting tools or online forms, applicants' personal data is transmitted, retained and managed. In this general Privacy Policy we also refer to the classic application process via email or online form in addition to recruiting tools. You can find more detailed information on recruiting tools in the Privacy Policies of the respective providers.

## **Why do we use recruiting tools?**

To search for suitable applicants and to administer all application documents, we use software programs and platforms that specialize in application management, taking into account all legal guidelines. So-called recruiting tools usually make the application process easier because the software takes on many administrative tasks and optimizes processes in the application process. In some cases, this enables us to find suitable employees for our company more quickly.

For the conditions of the recruiting process, we refer in detail to the respective job advertisements.

## **Which data are processed?**

If you apply with us, you of course also have to provide us with your data so we can assess your application accordingly. The exact details you provide us depends on the job posting or on the information required in the online form.

Generally, this involves data such as name, address, date of birth and proof of the qualifications required for the job. During the application process, however, not only basic personal data such as name or address may be transmitted, but information about applicants' health or ethnicity may also be requested so both parties can exercise the applicant's rights in relation to labor law, social security and social protection, while ensuring to meet the corresponding obligations. These data are called "data of special categories".

Your application's data are sent to us via the online form in encrypted nature. Alternatively, you can send your application to us by email. If you opt for the latter, your data will be transmitted in encrypted form, but will not be retained in encrypted form by the servers used to send and receive it.

## **Duration of data processing**

If your application is successful, we can process the data you provide for the employment relationship. If the application does not meet the requirements, we will erase the data we received. The data will also be erased if you withdraw your application. If you agree to join our pool of applicants, we will store your data in this context until you leave the pool of applicants. The same rules apply to the withdrawal as well as to the revocation of your consent.

## **Right to object**

You always have the right and the option to withdraw your consent. The data will be deleted after 6 months at the latest, so we can answer any questions you may have about the application and meet our obligations to provide proof. We also archive invoices for possible reimbursement of travel expenses due to tax law requirements.

## **Legal basis**

If we include you in our application pool, this is done on the basis of your consent (Art. 6 para. 1 lit. a GDPR). We would like to note, that your consent to our application pool is voluntary and has no

influence on the application process. Moreover, you can revoke your consent at any time.

In the event of the protection of vital interests, data processing takes place in accordance with Article 9 (2) c. GDPR. For the purposes of health care, occupational medicine, medical diagnostics, care or treatment in the health or social sector or for the administration of systems and services in the health or social sector, personal data is processed in accordance with Art. 9 para. 2 lit. h. GDPR. If you voluntarily provide data of special categories, data processing takes place on the basis of Art. 9 Para. 2 lit. a. GDPR.

Provided this information is available, you can find out more about the special recruiting tools in the following sections.

## **LinkedIn Recruiter Privacy Policy**

On our website we use the LinkedIn Recruiter recruiting tool. The provider of this service is the American company LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA.

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

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

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

You can find out more about the data that is processed by LinkedIn Recruiter in their Privacy Policy at <https://www.linkedin.com/legal/privacy-policy>.

## **Stepstone Privacy Policy**

We use StepStone, which is a job application management software. The provider of this service is the Austrian company StepStone Österreich GmbH, Prinz-Eugen-Strasse 8-10, A-1040 Vienna, Austria. You can find out more about the data that is processed by the use of StepStone in their Privacy Policy at <https://www.stepstone.at/about-us/legal-information/privacy-statement/>.

## **Survey- and Poll Systems Overview**

## Survey- and Poll Systems Privacy Policy Overview

 Affected parties: website visitors

 Purpose: Evaluation of surveys on the site

 Processed data: contact details, device data, access duration and time, IP addresses. You can find more details directly at the respective survey and poll systems.

 Storage duration: depending on the tool that is used

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

## What are survey and poll systems?

We are eager to conduct various surveys and polls via our website. These are always evaluated anonymously. A survey or poll system is a tool embedded on our website that can ask you questions (e.g. about our products or services) which you can answer if you would like to participate. Your answers will always be evaluated anonymously. However, after your consent to data processing, your personal data may also be stored and processed.

## Why do we use survey and poll systems?

We aim to offer you the best products and services in our industry. With the help of surveys, we can get your valuable feedback and find out what you expect from us and our services. Based on these anonymous evaluations, we can adapt our products and services to your wishes and ideas. Furthermore, the information also helps us to direct our advertising and marketing measures towards people who are really interested in our offer.

## Which data is processed?

First of all, your personal data will only be processed if it is either necessary for the technical implementation, or if you have consented to your data being processed. In the instance of your data being processed, e.g. your IP address will be stored, which enables the survey to be displayed in your browser. Cookies may also be used so you can easily continue your survey at a later point in time.

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

## How long is data stored?

How long your data is processed and stored depends primarily on the tools we use. Below you can find out more about the data processing of individual tools. The 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 to provide our services. When data is stored in cookies, the storage period varies greatly. This data could be deleted immediately after leaving a

website, but it could also be stored for several years. Therefore, if you want to know more about data storage, you should look at each individual cookie in detail. In most cases, you will also find information on the individual cookies in the respective providers' Privacy Policies.

## Right to object

You also have the right and the option to revoke your consent to the use of cookies or embedded survey systems at any time. This can be done either via our cookie management tool or via other opt-out functions. For example, you can also prevent data collection by cookies if you manage, deactivate or erase the cookies in your browser.

Since cookies can be used in survey systems, we also recommend you to read our general Privacy Policy on cookies. You should read the Privacy Policies of the respective tools to find out exactly which of your data is stored and processed.

## Legal Basis

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

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

Since cookies are used in survey systems, we also recommend you to 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.

You can find information on the individual survey systems – if available – in the following sections.

## Google Form Privacy Policy

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

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

Google uses standard contractual clauses approved by the EU Commission as the basis for data processing by recipients based in third countries (i. e. outside the European Union, Iceland, Liechtenstein, Norway, and thus especially in the USA) or data transfer there (= Art. 46, paragraphs 2 and 3 of the GDPR). Standard Contractual Clauses (SCC) are legal templates provided by the EU Commission. Their purpose is to ensure that your data complies with European data privacy

standards, even if your data is transferred to and stored in third countries (such as the USA). With these clauses, Google commits to comply with the EU's level of data protection when processing relevant data, even if it is stored, processed and managed in the USA. These clauses are based on an implementing order by the EU Commission. You can find the order and the standard contractual clauses here: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847).

You can find Google Ads' Data Processing Terms, which correspond to the standard contractual clauses as well as to Google forms at <https://business.safety.google/adsprocessor/terms/>.

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

## Typeform Privacy Policy

We use Typeform for our website, which is a survey software. The provider of this service is the Spanish company Typeform, 163 Carrer de Bac de Roda, Barcelona, Spain. You can find out more about the data that is processed by the use of Typeform in their Privacy Policy at <https://admin.typeform.com/to/dwk6gt>.

## Review Platforms Overview

### Review Platforms Overview

-  Affected parties: Website or rating platform visitors
-  Purpose: Feedback on our products and/or services
-  Processed data: IP address, email address and name, among other things. You can find more details below or directly on the respective review platforms.
-  Storage duration: depends on the respective platform
-  Legal bases: Article 6 paragraph 1 lit. a GDPR (consent), Article 6 paragraph 1 lit. f GDPR (legitimate interests),

## What are review platforms?

You can rate our products or services on various review platforms. We are registered on some of these platforms so we can get feedback from you, which can help us to optimise our offer. If you rate us via a review platform, the Privacy Policy and the General Terms and Conditions of the respective review service apply. In many instances, you also have to register in order to submit a review. We may also have rating technologies (widgets) integrated into our website. By using such tools, data is transmitted to the relevant provider, where it is processed and stored.

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

## **Why do we use review platforms?**

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

## **Which data is processed?**

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

## **How long and where is the data stored?**

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

## **Right to object**

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

## **Legal Basis**

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

We also have a legitimate interest in using a review platform to optimise our online service. The

corresponding legal basis for this is Article 6 (1) (f) GDPR (legitimate interests). However, we only use any given review platform if you have consented to it.

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

## **Google Reviews Privacy Policy**

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

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

Google uses standard contractual clauses approved by the EU Commission as the basis for data processing by recipients based in third countries (i. e. outside the European Union, Iceland, Liechtenstein, Norway, and thus especially in the USA) or data transfer there (= Art. 46, paragraphs 2 and 3 of the GDPR). Standard Contractual Clauses (SCC) are legal templates provided by the EU Commission. Their purpose is to ensure that your data complies with European data privacy standards, even if your data is transferred to and stored in third countries (such as the USA). With these clauses, Google commits to comply with the EU's level of data protection when processing relevant data, even if it is stored, processed and managed in the USA. These clauses are based on an implementing order by the EU Commission. You can find the order and the standard contractual clauses here: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847).

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

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

## **kununu Privacy Policy**

We also use the rating platform kununu for our website. The provider of this service is the German company New Work SE, Dammtorstrasse 30, 20354 Hamburg, Germany. You can find out more about the data that is processed through the use of kununu in their Privacy Policy at <https://privacy.xing.com/de/datenschutzerklaerung>.

## **Google Maps Privacy Policy**

### **Google Maps Privacy Policy Overview**

 Affected parties: website visitors

 Purpose: service optimisation

 Processed data: data such as entered search terms, IP address as well as latitude and longitude coordinates.

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

 Storage duration: depending on the retained data

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

## **What is Google Maps?**

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

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

## **Why do we use Google Maps on our website?**

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

## **What data is stored by Google Maps?**

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

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

**Name:** NID

**Value:** 188=h26c1Ktha7fCQTx8rXgLyATyITJ122087503-5

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

**Expiration date:** after 6 months

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

## How long and where is the data stored?

There are Google servers in data centres across the entire planet. However, most servers are in America. For this reason, your data is widely stored in the USA. Here you can read in detail about where the Google servers are located:

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

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

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

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

Due to the automatic delete function for location and activity data, which was introduced in 2019, information that is used for determining your location and web or app activity is saved for either 3 or 18 months, depending on your preferred decision, and is deleted thereafter. Furthermore, it is possible to delete this data manually from your browser history via your Google account anytime. If you want to prevent the determination of your location altogether, you must pause the category "Web and app activity" in your Google account. Click on "Data and personalisation" and then choose the option "Activity controls". Here you can switch the activities on or off.

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

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

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

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

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

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

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

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

## Legal basis

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

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

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

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

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

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

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

# Miscellaneous Overview

## Miscellaneous Privacy Policy Overview

 Affected parties: website visitors

 Purpose: Improvement of user experience

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

 Storage duration: depends on the tools used

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

## What is included in “Miscellaneous”?

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

## Why do we use these third parties?

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

## Which data is processed?

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

## Duration of data processing

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

for the provision of our services and products.

## **Legal Basis**

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

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

All texts are copyrighted.