

Privacy policy

Table of contents

- [Introduction and overview](#)
- [Scope of application](#)
- [Legal basis](#)
- [Contact details of the responsible person](#)
- [Contact details of the data protection officer](#)
- [Storage period](#)
- [Rights under the General Data Protection Regulation](#)
- [Data transfer to third countries](#)
- [Data processing security](#)
- [Communication](#)
- [Order processing contract \(AVV\)](#)
- [Cookies](#)
- [Application data](#)
- [Customer data](#)
- [Registration](#)
- [Web hosting introduction](#)
- [Website Building Block Systems Introduction](#)
- [Web Analytics Introduction](#)
- [Email Marketing Introduction](#)
- [Push Messages Introduction](#)
- [Messenger & Communication Introduction](#)
- [Chatbots Introduction](#)
- [Social Media Introduction](#)
- [Blogs and publication media Introduction](#)
- [Online Marketing Introduction](#)
- [Affiliate programmes Introduction](#)
- [Content Delivery Networks Introduction](#)
- [Cookie Consent Management Platform Introduction](#)
- [Security & Anti-Spam](#)
- [Cloud services](#)
- [Payment provider introduction](#)
- [External online platforms Introduction](#)
- [Credit Assessment Bodies Introduction](#)
- [Audio & Video Introduction](#)
- [Video Conferencing & Streaming Introduction](#)
- [Recruiting Tools Introduction](#)
- [Single sign-on logins Introduction](#)
- [Survey and polling systems Introduction](#)
- [Assessment platforms Introduction](#)
- [Web design introduction](#)
- [Online map services Introduction](#)
- [Content Search Provider Introduction](#)
- [Online booking systems Introduction](#)
- [Miscellaneous Introduction](#)
- [Explanation of terms used](#)
- [Closing words](#)

Introduction and overview

We have drawn up this data protection declaration (version 24.08.2023-312569961) in order to explain to you, in accordance with the requirements of the [General Data Protection Regulation \(EU\) 2016/679](#) and applicable national laws, which personal data (data for short) we as the controller - and the processors (e.g. providers) commissioned by us - process, will process in future and what lawful options you have. The terms used are to be understood as gender-neutral.

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

Data protection statements usually sound very technical and use legal terminology. This privacy statement, on the other hand, is intended to describe the most important things to you as simply and transparently as possible. As far as it is conducive to transparency, technical **terms are explained in a reader-friendly manner**, links to further information are provided and **graphics are used**. In this way, we inform you in clear and simple language that we only process personal data in the course of our business activities if there is a corresponding legal basis. This is certainly not possible by providing the most concise, unclear and legalistic explanations possible, as is often standard practice on the Internet when it comes to data protection. I hope you find the following explanations interesting and informative and perhaps there is one or two pieces of information you did not know yet. If you still have questions, we would like to ask you to contact us at the address below or in the imprint.

responsible body, to follow the links provided and to view further information on third party sites. Of course, you will also find our contact details in the imprint.

Scope of application

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

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

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

Legal basis

In the following data protection declaration, we provide you with transparent information on the legal principles and regulations, i.e. the legal basis of the basic data protection regulation, which enable us to process personal data.

As far as EU law is concerned, we refer to REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016. These You can of course read the EU's General Data Protection Regulation online on EUR-Lex, the gateway to EU law, at <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32016R0679>.

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

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

Further conditions such as the performance of recordings in the public interest and the exercise of public authority as well as the protection of vital interests do not generally occur with us. If such a legal basis should be relevant, it will be indicated at the appropriate place.

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

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

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

Contact details of the responsible person

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

Oliver Große
Gartenstr.11
82152 Krailling
Germany

E-mail: info@grosse-consulting.de Phone:
[+49 177 321 5320](tel:+491773215320)
Imprint: <https://www.grosse-consulting/impressum/>

Contact details of the data protection officer

Below you will find the contact details of the data protection officer: Oliver

Große
Gartenstr. 11
82152 Krailling
Germany

E-mail: info@grosse-consulting.de Phone:
[+49 177 321 5320](tel:+491773215320)

Storage period

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

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

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

Rights under the General Data Protection Regulation

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

- According to Article 15 of the GDPR, you have the right to know whether we are processing data about you. If this is the case, you have the right to receive a copy of the data and the following information:
 - the purpose for which we carry out the processing;
 - the categories, i.e. the types of data that are processed;
 - who receives this data and if the data 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 complain to 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 rectify data under Article 16 of the GDPR, which means that we must correct data if you find errors.
- According to Article 17 of the GDPR, you have the right to erasure ("right to be forgotten"), 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 any 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 common format upon request.
- According to Article 21 of the GDPR, you have a right to object, which, once enforced, entails a change in processing.
 - 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 carry out direct marketing, you can object to this type of data processing at any time. We are then no longer allowed to use your data for direct marketing.
 - If data is used to carry out profiling, you can object to this type of data processing at any time. We are then no longer allowed to use your data for profiling.
- You may have the right under Article 22 of the GDPR not to be subject to a decision based solely on automated processing (for example profiling).
- According to Article 77 of the GDPR, you have the right to lodge a complaint. This means that you can complain to the data protection authority at any time if you believe that the data processing of personal data violates the GDPR.

In short: You have rights - do not hesitate to contact the responsible body listed above with us!

If you believe that the processing of your data violates data protection law or that your data protection rights have been violated in any other way, you can 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 commissioner 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:

Bavaria Data Protection Authority

State Commissioner for Data Protection: Prof. Dr. Thomas Petri

Address: Wagnmüllerstr. 18, 80538 Munich

Telephone no.: 089/21 26 72-0

E-mail address: poststelle@datenschutz-bayern.de

Website: <https://www.datenschutz-bayern.de/>

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 contractually necessary and in any case only to the extent that this is generally permitted. Your consent is in most cases the most important reason for us to have data processed in third countries. Processing personal data in third countries such as the US, where many software vendors provide services and have their server locations, may mean that personal data is processed and stored in unexpected ways.

We expressly point out that according to the opinion of 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 not being processed and stored anonymously. Furthermore, US government authorities may be able to access individual data. In addition, it is possible that collected data may be linked to data from other services of the same provider, provided you have a corresponding user account. Where possible, we try to use server locations within the EU, if this is offered.

We will provide you with more detailed information about data transfers to third countries, where applicable, at the appropriate points in this privacy policy.

Data processing security

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

Article 25 of the GDPR speaks of "data protection through technical design and through data protection-friendly default settings" and thus means that both software (e.g. forms) and hardware (e.g. access to the server room) should always be designed with security in mind and that appropriate measures should be taken. In the following, we will go into more detail on specific measures, if necessary.

TLS encryption with https

TLS, encryption and https sound very technical and they are. We use HTTPS (Hypertext Transfer Protocol Secure, which stands for "secure hypertext transfer protocol") to transfer data over the internet in a tap-proof way.

This means that the complete transmission of all data from your browser to our web server is secured - no one can "listen in".

In this way, we have introduced an additional layer of security and comply with data protection by design of technology ([Article 25\(1\) DSGVO](#)). Through the use of TLS

(Transport Layer Security), an encryption protocol for secure data transmission on the Internet, we can ensure the protection of confidential data.

You can recognise the use of this data transmission protection by the small

Lock symbol at the top left of the browser, to the left of the internet address (e.g. beispieleseite.de) and the use of the https scheme (instead of http) as part of our internet address.

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

Communication

Communication Summary

Affected persons: All those who communicate with us by telephone, e-mail or online form.

Processed data: e.g. telephone number, name, e-mail address, form data entered. You can find more details on this in the respective contact type used.

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

Storage period: duration of the business case and legal requirements

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. b DSGVO (Contract), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

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

The data is processed for the handling and processing of your question and the related business transaction. The data is stored for as long as it is required by law.

Persons concerned

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

Phone

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

E-mail

If you communicate with us by e-mail, data may be stored on the respective end device (computer, laptop, smartphone,...) and data is stored on the e-mail server. The data is deleted as soon as the business case has been completed and legal requirements permit.

Online forms

If you communicate with us using an online form, data is stored on our web server and, if necessary, forwarded to an e-mail address of ours. The data is deleted as soon as the business case has been terminated and legal requirements permit.

Legal basis

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

- Art. 6 para. 1 lit. a DSGVO (consent): You give us your consent to store your data and to use it for purposes related to the business case;
- Art. 6 para. 1 lit. b DSGVO (contract): There is a need for the performance of a contract with you or a processor such as the telephone provider, or we need to process the data for pre-contractual activities, such as preparing an offer;
- Art. 6 para. 1 lit. f DSGVO (Legitimate Interests): We want to operate customer enquiries and business communication in a professional framework. For this purpose, certain technical facilities such as e-mail programmes, exchange servers and mobile phone operators are necessary in order to be able to operate the communication efficiently.

Order processing contract (AVV)

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

Who are processors?

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

For a better understanding of the terminology, here is an overview of the three roles in the GDPR:

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

Content of a processing order

As already mentioned above, we have concluded an AVV with our partners who act as processors. This states first and foremost that the processor processes the data to be processed exclusively in accordance with the GDPR. The contract must be concluded in writing; however, in this context, the electronic conclusion of the contract is also considered to be "in writing". Only on the basis of the contract will the processing of personal data take place. The contract must contain the following:

- Binding to us as the responsible party
- Duties and rights of the responsible person
- Categories of persons concerned
- Nature of the personal data
- Nature and purpose of data processing
- Subject and duration of data processing
- Place of implementation of the data processing

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


- To ensure data security measures
- take possible technical and organisational measures to protect the rights of the data subject
- keep a data processing register
- cooperate with the data protection supervisory authority at its request
- Conduct a risk analysis in relation to the personal data received
- Sub-processors may only be engaged with the written consent of the responsible person


You can see what such an AVV looks like in concrete terms, for example, at <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag-auftragsverarbeitung.html>. A sample contract is presented here.

Cookies

Cookies Summary

 Data subjects: Visitors to the website

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

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

 Storage time: depending on the cookie, can range from hours to years.

vary

Y Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What are cookies?

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

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

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

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

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

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

There are both first-party cookies and third-party cookies. First-party cookies are created directly by our site, third-party cookies are created by partner websites (e.g. Google Analytics). Each cookie is to 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 programmes and do not contain viruses, Trojans or other "pests". Cookies also cannot access information on your PC.

Cookie data, for example, can look like this:

Name: _ga

Value: GA1.2.1326744211.152312569961-9

Intended use: differentiation of website visitors

Expiry date: after 2 years

A browser should be able to support these minimum sizes:

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

What are the different types of cookies?

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

One can distinguish between 4 types of cookies:

Essential cookies

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

Purposeful cookies

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

Targeting cookies

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

Advertising cookies

These cookies are also called targeting cookies. They are used to deliver individually adapted advertising to the user. This can be very practical, but also very annoying.

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

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

Purpose of processing via cookies

The purpose ultimately depends on the cookie in question. More details can be found below or from the manufacturer of the software that sets the cookie.

What data is processed?

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

Storage period of cookies

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

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

Right of objection - how can I delete cookies?

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

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

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

[Safari: Managing Cookies and Website Data with Safari](#)

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

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

[Microsoft Edge: Delete and manage cookies](#)

If you generally do not want cookies, you can set up your browser so that it always informs you when a cookie is to be set. In this way, you can decide for each individual cookie whether you allow the cookie or not. The procedure varies depending on the browser. It is best to search for the instructions in Google with the search term "Delete Cookies Chrome" or "Deactivate Cookies Chrome" in the case of a Chrome browser.

Legal basis

The so-called "Cookie Guidelines" have been in place since 2009. These state that the storage of cookies requires your **consent** (Article 6 para. 1 lit. a DSGVO). Within the EU countries, however, there are still very different reactions to these directives. In Austria, however, this directive was implemented in § 96 para.

3 of the Telecommunications Act (TKG). In Germany, the Cookie Directive was not implemented as national law. Instead, this directive was largely implemented in § 15 para.3 of the Telemedia Act (TMG).

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

If cookies are used that are not absolutely necessary, this only happens in the case of your consent. The legal basis in this respect is Art. 6 para. 1 lit. a DSGVO.

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

Application data

Application data summary

✓ Affected persons: Users who apply for a job with us.

Purpose: Handling of an application procedure

Data processed: Name, address, contact details, e-mail address, telephone number, qualifications (certificates), any special category data.

■ Storage period: in the case of a successful application, until the end of the employment relationship. Otherwise, the data will be deleted after the application procedure or stored for a certain period with your consent.

Legal basis: Art. 6 para. 1 lit. a DSGVO (consent), legitimate interest (Art. 6 para. 1 lit. f DSGVO), Art. 6 para. 1 lit. b DSGVO (contract), Art. 9 para. 2 lit. a.

GDPR (processing of special categories)

What are application data?

You can apply to us by e-mail, online form or via a recruiting tool for a job in our company. All data that we receive and process from you as part of an application counts as application data. In doing so, you always disclose personal data such as your name, date of birth, address and telephone number.

Why do we process application data?

We process your data so that we can run a proper selection procedure in relation to the advertised position. In addition, we also like to keep your application documents in our application archive. This is because it often happens that a cooperation for the advertised position does not work out for a variety of reasons, but we are impressed by you and your application and can very well imagine a future cooperation. Provided you give us your consent, we will archive your documents so that we can easily contact you for future tasks in our company.

We guarantee that we will handle your data with particular care and only ever process your data within the legal framework. Even within our company, your data will only be passed on to people who are directly involved with your application. In short: Your data is in safe hands with us!

What data is processed?

If you apply to us by e-mail, for example, we will of course also receive personal data, as mentioned above. Even the e-mail address counts as personal data. However, in the course of an application procedure, we only process the data that is relevant for our decision as to whether or not we want to welcome you to our team.

Exactly what data is processed depends primarily on the job advertisement. Mostly, however, it is a matter of name, date of birth, contact details and proof of qualifications. If you submit the application via an online form, the data is passed on to us in encrypted form. If you send us the application by e-mail, this encryption does not take place. We cannot therefore accept any responsibility for the way in which the data is transmitted. However, once the data is on our servers, we are responsible for the lawful handling of your data.

During an application process, in addition to the data mentioned above, information about your health or ethnic origin may also be requested so that we and you can exercise the rights relating to labour law, social security and social protection and, at the same time, comply with the corresponding obligations. These data are special category data.

Here is a list of possible data we receive from you and process:

- Name
- Contact address
- E-mail address
- Telephone number
- Date of birth
- Information that emerges from the cover letter and CV
- Proof of qualifications (e.g.) Certificates
- Special category data (e.g. ethnic origin, health data, religious beliefs)
- Usage data (websites visited, access data ect.)
- Metadata (IP address, device information)

How long will the data be stored?

If we accept you as a team member in our company, your data will be further processed for the purpose of the employment relationship and kept with us at least until the employment relationship ends. All application documents are then placed in your employee file.

If we do not offer you the job, if you reject our offer or withdraw your application, we may, on the basis of legitimate interest (Art. 6 para. 1 lit. f DSGVO), retain your data for up to 6 months after the end of the application process.

retain. After that, both your electronic data and all data from physical application documents will be completely deleted or destroyed. We keep your data for example so that we can still answer any follow-up questions or so that we can provide evidence of the application in the event of a legal dispute. If a legal dispute arises and we may still need the data after the 6 months have expired, we will only delete the data when there is no longer any reason to retain it. If there are legal retention obligations to fulfil, we must generally store the data for longer than 6 months.

Furthermore, we can also keep your data longer if you have given us special permission to do so. We do this, for example, if we can well imagine working with you in the future. Then it is helpful to have your data archived so that we can contact you without any problems. In this case, the data will be added to our applicant pool. Of course, you can revoke your consent to the longer storage of your data at any time. If you do not revoke your consent and do not give new consent, your data will be deleted after 2 years at the latest.

Legal basis

The legal basis for processing your data is Art. 6 para. 1 lit. a DSGVO (consent), Art. 6 para. 1 lit. b DSGVO (contract or pre-contractual measures), Art. 6 para. 1 lit. f DSGVO (legitimate interests) and Art. 9 para. 2 lit. a. DSGVO (processing of special categories).

If we include you in our application tool, this is done on the basis of your consent (Art. 6 para. 1 lit. a DSGVO). We would like to point out that your consent to our application pool is voluntary, has no influence on the application process and you have the option to revoke your consent at any time. The lawfulness of the processing up to the time of the revocation remains unaffected.

In the case of the protection of vital interests, data processing is carried out in accordance with Art. 9 para. 2 lit. c. DSGVO. For the purposes of health care, occupational medicine, medical diagnosis, health or social care or treatment, or the management of health or social care systems and services, the processing of personal data is carried out in accordance with Art. 9 (2) (h) of the GDPR.

DSGVO. If you voluntarily provide special category data, the processing is based on Art. 9 para. 2 lit. a. DSGVO.

Customer data

Customer data summary

VAffected parties: customers or business and contractual partners

Purpose: Provision of the contractually or pre-contractually agreed services, including related communication.

Data processed: Name, address, contact details, email address, telephone number, payment information (such as invoices and bank details), contract data (such as Term and subject of the contract), IP address, order data

Storage period: the data is deleted as soon as it is required for the provision of our

business purposes are no longer required and there is no legal obligation to retain data.

Y Legal basis: Legitimate interest (Art. 6 para. 1 lit. f DSGVO), contract (Art. 6 para. 1 lit. b DSGVO)

What is customer data?

In order to be able to offer our service or our contractual services, we also process data of our customers and business partners. This data always includes personal data. Customer data is all information that is processed on the basis of a contractual or pre-contractual cooperation in order to be able to provide the services offered. Customer data is therefore all collected information that we collect and process about our customers.

Why do we process customer data?

There are many reasons why we collect and process customer data. The most important is that we simply need different data to provide our services. Sometimes your email address is enough, but if you purchase a product or service, for example, we also need data such as your name, address, bank details or contract details. We also use the data for marketing and sales optimisation so that we can improve our overall service to our customers. Another important point is our customer service, which is always very important to us. We want you to be able to come to us at any time with questions about our offers, and for this we need at least your e-mail address.

What data is processed?

The exact data that is stored can only be described here on the basis of categories. This always depends on the services you receive from us. In some cases, you only give us your e-mail address so that we can contact you or answer your questions, for example. In other cases, you purchase a product or service from us and we need much more information, such as your contact details, payment details and contract details.

Here is a list of possible data we receive from you and process:

- Name
- Contact address
- E-mail address
- Telephone number
- Date of birth
- Payment data (invoices, bank data, payment history etc.)
- Contract data (term, content)
- Usage data (websites visited, access data ect.)
- Metadata (IP address, device information)

How long will the data be stored?

As soon as we no longer need the customer data to fulfil our contractual obligations and our purposes and the data is also no longer necessary for possible warranty and liability obligations, we delete the corresponding customer data. This is the case, for example, when a business contract ends. After that, the limitation period is usually 3 years, although longer periods are possible in individual cases. Of course, we also comply with the statutory retention obligations. Your customer data will certainly not be passed on to third parties unless you have explicitly given your consent.

Legal basis

The legal basis for processing your data is Art. 6 para. 1 lit. a DSGVO (consent), Art. 6 para. 1 lit. b DSGVO (contract or pre-contractual measures), Art. 6 para. 1 lit. f DSGVO (legitimate interests) and in special cases (e.g. medical services) Art. 9 para. 2 lit. a. DSGVO (processing of special categories).

In the case of the protection of vital interests, data processing is carried out in accordance with Art. 9 para. 2 lit. c. DSGVO. For the purposes of health care, occupational medicine, medical diagnosis, health or social care or treatment, or the management of health or social care systems and services, the processing of personal data is carried out in accordance with Art. 9 (2) (h) of the GDPR.

DSGVO. If you voluntarily provide special category data, the processing is based on Art. 9 para. 2 lit. a. DSGVO.

Registration

Registration Summary

Affected persons: All persons who register, create an account, log in and use the account.

Processed data: Email address, name, password and other data collected in the course of registration, login and account use.

Purpose: To provide our services. Communication with customers in connection with the services.

Storage period: As long as the company account linked to the texts exists and thereafter usually 3 years.

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

When you register with us, personal data may be processed if you enter personal data or data such as the IP address is collected in the course of processing. You can read more about what we mean by the rather unwieldy term "personal data" below.

Please only enter data that we need for registration and for which you have the release of a third party, if you are registering on behalf of a third party. If possible, use a secure password that you do not use anywhere else and an email address that you check regularly.

In the following, we inform you about the exact type of data processing, because we want you to feel comfortable with us!

What is registration?

When you register, we take certain data from you and allow you to simply log in to us online later and use your account with us. Having an account with us has the advantage that you don't have to re-enter everything every time. Saves time, effort and ultimately prevents errors in the provision of our services.

Why do we process personal data?

In short, we process personal data to enable the creation and use of an account with us. If we didn't do that, you would have to enter all the data every time, wait for us to approve it and then enter it all again. We and many, many customers would not like that. What would you think?

What data is processed?

All data that you have provided in the course of registration, enter during registration or enter in the course of managing your data in the account.

We process the following types of data during registration:

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

When you log in, we process the data you enter when logging in, such as username and password, and data collected in the background, such as device information and IP addresses.

During account use, we process data that you enter during account use and which is created in the course of using our services.

Storage period

We store the data entered at least for as long as the account linked to the data exists with us and is used, as long as contractual obligations exist between us and, if the contract ends, until the respective claims arising from it have become time-barred. In addition, we store your data as long as and insofar as we are subject to legal obligations to store it. Thereafter, we retain accounting records pertaining to the contract (invoices, contract documents, account statements, etc.) as well as other relevant business documents for the legally prescribed period (usually several years).

Right of objection

You have registered, entered data and would like to revoke the processing? No problem. As you can read above, the rights under the General Data Protection Regulation also exist during and after registration, login or account with us. Contact the data protection officer above to exercise your rights. If you already have an account with us, you can easily view and manage your data and texts in your account.

Legal basis

By carrying out the registration process, you enter into a pre-contractual agreement with us to enter into a contract of use via our platform (although no automatic obligation to pay arises). You invest time to enter data and register and we offer you our services after logging into our system and viewing your customer account. We also fulfil our contractual obligations. Finally, we need to keep registered users informed of important changes by email. Thus, Art. 6 para. 1 lit. b DSGVO (performance of pre-contractual measures, fulfilment of a contract) applies.

If necessary, we also obtain your consent, e.g. if you voluntarily provide more data than is absolutely necessary or if we are allowed to send you advertising. Art. 6 para. 1 lit. a DSGVO (consent) therefore applies.

We also have a legitimate interest in knowing who we are dealing with in order to contact them in certain cases. In addition, we need to know who is using our services and whether they are being used as specified in our terms of use, so Art. 6 para. 1 lit. f DSGVO (Legitimate Interests) applies.

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

Registration with a clear name

As we need to know who we are dealing with in business operations, registration is only possible with your real name (clear name) and not with pseudonyms.

Registration with pseudonyms

Pseudonyms can be used for registration, which means that you do not have to register with us using your real name. This ensures that your name cannot be processed by us.

Storage of the IP address

In the course of registration, login and account use, we store the IP address in the background for security reasons in order to be able to determine lawful use.

Public profile

The user profiles are publicly visible, i.e. parts of the profile can be seen on the internet without entering a user name and password.

2-factor authentication (2FA)

Two-factor authentication (2FA) provides additional security when logging in, as it prevents you from logging in without a smartphone, for example. This technical measure to secure your account thus protects you against the loss of data or unauthorised access even if the user name and password were known. You will find out which 2FA is used during registration, login and in the account itself.

Web hosting introduction

Web hosting summary

Data subjects: Visitors to the website

Purpose: professional hosting of the website and securing of the operation

Processed data: IP address, time of website visit, browser used and other data. More details can be found below or at the respective web hosting provider used.

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

Legal basis: Art. 6 para. 1 lit.f DSGVO (Legitimate Interests)

What is web hosting?

When you visit websites 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 justification. By website, by the way, we mean the totality of all web pages on a domain, i.e. everything from the home page (homepage) to the very last subpage (like this one). By domain, we mean, for example, example.de or example.com.

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

To display the website, the browser must connect to another computer where the website's code is stored: the web server. Operating a web server is a complicated and costly task, which is why it is usually done by professional providers. These offer web hosting and thus ensure reliable and error-free storage of website data. A whole lot of technical terms, but please stay tuned, it gets better!

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

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

Why do we process personal data?

The purposes of the data processing are:

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

What data is processed?

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

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

How long is data stored?

As a rule, the above data is stored for a fortnight and then automatically deleted. We do not pass on this data, but we cannot rule out the possibility that this data may be viewed by the authorities in the event of unlawful conduct.

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

Legal basis

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

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

STRATO Privacy Policy

We use the web hosting service STRATO for our website. The service provider is the German company STRATO AG, Otto-Ostrowski-Straße 7, 10249 Berlin, Germany.

You can find out more about the data processed by using STRATO in the data protection information at <https://www.strato.de/datenschutz/>.

Website Building Block Systems Introduction

Website Building Block Systems Privacy Policy Summary

Parties concerned: Visitors to the website

Purpose: optimisation of our service performance

Processed data: Data such as technical usage information such as browser activity, clickstream activity, session heatmaps as well as contact details, IP address or your geographical location. More details can be found below in this privacy policy and in the privacy policy of the providers.

Storage duration: depends on the provider

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

What are website construction kits?

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

Why do we use website building systems for our website?

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

What data is stored by a modular system?

Exactly which data is stored depends, of course, on the website construction kit system used. Each provider processes and collects different data from the website visitor. But as a rule, technical usage information such as operating system, browser, screen resolution, language and keyboard settings,

hosting provider and the date of your website visit. Furthermore, tracking data (e.g. browser activity, clickstream activity, session heatmaps, etc.) may also be processed. In addition, personal data may also be collected and stored. This is mostly contact data such as email address, telephone number (if you have provided it), IP address and geographical location data. You can find out exactly what data is stored in the provider's privacy policy.

How long and where is the data stored?

We will inform you about the duration of the data processing below in connection with the website construction kit system used, provided we have further information on this. You will find detailed information about this in the provider's privacy policy. In general, we only process personal data for as long as is absolutely necessary for the provision of our services and products. It may be that the provider stores data from you according to its own specifications, over which we have no influence.

Right of objection

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

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

Legal basis

We have a legitimate interest in using a website construction kit system to optimise our online service and to present it to you in an efficient and user-friendly manner. The corresponding legal basis for this is Art. 6 para. 1 lit. f DSGVO (Legitimate Interests). However, we only use the modular system if you have given your consent.

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

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

Wordpress.com Privacy Policy

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

What is WordPress?

In 2003, the company saw the light of day and in a relatively short time developed into one of the best-known content management systems (CMS) worldwide. A CMS is software that helps us to design our website and present content in a beautiful and orderly way. The content can be text, audio and video.

Through the use of WordPress, personal data may also be collected from you, stored and processed. As a rule, mainly technical data such as operating system, browser, screen resolution or hosting provider are stored. However, personal data such as IP address, geographical data or contact data may also be processed.

Why do we use WordPress?

Programming is not one of our core competences. Nevertheless, we want to have a powerful and attractive website that we can also manage and maintain ourselves. With a website builder or content management system like WordPress, that is exactly what is possible. With WordPress, we don't have to be programming aces to offer you a beautiful website. Thanks to WordPress, we can operate our website quickly and easily even without any previous technical knowledge. If technical problems arise or we have special wishes for our website, there are always our experts who feel at home in HTML, PHP, CSS and Co.

How secure is the data transfer with WordPress?

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

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

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

The Data Processing Agreements, which correspond to the standard contractual clauses, can be found at <https://wordpress.com/support/data-processing-agreements/>.

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

Order processing agreement (AVV) Wordpress.com

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have concluded a Data Processing Agreement (DPA) with WordPress.com. What exactly is a GCU and, above all, what must be included in a GCU, you can read in our general section "Order processing agreement (GCU)".

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

Web Analytics Introduction

Web Analytics Privacy Policy Summary

✓ Parties concerned: Visitors to the website

Purpose: Evaluation of visitor information to optimise the web offer.

Processed data: Access statistics containing data such as access locations, device data, access duration and time, navigation behaviour, click behaviour and IP addresses. More details can be found in the respective web analytics tool used.

Storage duration: depending on the web analytics tool used.

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What is Web Analytics?

We use software on our website to evaluate the behaviour of website visitors, called web analytics for short. This involves collecting data that the respective analytic tool provider (also called tracking tool) stores, manages and processes. With the help of the data, analyses of user behaviour on our website are created and made available to us as the website operator. In addition, most tools offer various test options. For example, we can test which offers or contents are best received by our visitors. For this purpose, we show you two different offers for a limited period of time. After the test (so-called A/B test), we know which product or content our website visitors find more interesting. For such test procedures, as for other analytics procedures, user profiles can also be created and the data stored in cookies.

Why do we do web analytics?

With our website we have a clear goal in mind: we want to deliver the best web offer on the market for our industry. In order to achieve this goal, we want to offer the best and most interesting offer on the one hand, and on the other hand, we want to make sure that you will find yourself on

feel completely at ease on our website. With the help of web analysis tools, we can take a closer look at the behaviour of our website visitors and then improve our website accordingly for you and us. For example, we can see how old our visitors are on average, where they come from, when our website is visited the most or which content or products are particularly popular. All this information helps us to optimise the website and thus best adapt it to your needs, interests and wishes.

What data is processed?

Exactly what data is stored depends, of course, on the analysis tools used. But as a rule, for example, which content you view on our website, which buttons or links you click on, when you call up a page, which browser you use, which device (PC, tablet, smartphone, etc.) you use to visit the website or which computer system you use are stored. If you agreed that location data may also be collected, these may also be processed by the web analysis tool provider.

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

The following example shows schematically how Google Analytics works as an example of client-based web tracking with Java-ScriHow long the respective data is stored always depends on the provider. Some cookies only store data for a few minutes or until you leave the website again, other cookies can store data for several years.

Duration of data processing

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

Right of objection

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, deactivating or deleting cookies in your browser.

Legal basis

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

In addition to consent, there is a legitimate interest on our part to analyse the behaviour of website visitors and thus to improve our offer technically and economically. With the help of web analytics, we detect website errors, can identify attacks and improve economic efficiency. The legal basis for this is **Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)**. Nevertheless, we only use the tools insofar as you have given your consent.

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

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

etracker privacy policy

etracker Privacy Policy Summary

Data subjects: Visitors to the website

Purpose: Evaluation of visitor information to optimise the web offer.

Data processed: including pseudonymised IP address, technical information on browser, operating system and end device, duration of visit, interactions on the website.

Storage duration: depending on the web analytics tool used.

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What is etracker?

On our website, we use the analysis tracking tool etracker Analytics from the German company etracker GmbH, Erste Brunnenstraße 1, D-20459 Hamburg. etracker Analytics is software that collects and evaluates data about your actions on our website. We receive analysis reports on how you use our website and can thus adapt our offer ever better to your wishes. In this data protection declaration, we go into more detail about the analysis tool and show you in particular which data is stored when, how and where.

etracker Analytics is an analysis tool that can measure and analyse the performance of our website and online campaigns. For example, the software programme collects data on how long you stay on our website, how many users visit our website and from where you came to our website. We also receive precise evaluations of visitor behaviour on our website. For example, we can find out which buttons you like to click.

or which subpages you like and which you tend to avoid. All this information is anonymous. This means that we do not identify you as a person through this data, but only receive general user information and statistics.

Why do we use etracker on our website?

We use the software tool to improve the quality of our website and our services. Our goal is to provide you with the best possible service. We want you to feel comfortable on our website and get exactly what you expect. To achieve this, we must of course adapt our offer as well as possible to your wishes and requirements.

The data also helps us to carry out our online marketing and advertising measures more cheaply and individually. Because of course we only want to show our offer to people who are interested in it.

What data is stored by etracker?

In order for tracking to work, a JavaScript code must be integrated into the website. etracker works on a pixel technology.

By default, etracker does not use cookies or technologies for tracking on a website, as this has been implemented in the so-called cookie-less mode by privacy-by-design. In this case, only absolutely necessary cookies are set. However, if you have actively agreed to the use of cookies, etracker will also use cookies.

The following data is stored and processed when you access the page:

- Your pseudonymised IP address
- Technical information about your browser, operating system and the terminal device you are using
- Location information up to city level
- the URL called up with the corresponding page title and optional information on the page content
- Referrer website: this is the website from which you came to our website
- the following page: this is the website where you click afterwards
- how long you stay on our website (dwell time)
- Interactions on the website. These can be, for example, clicks on the website, search terms entered, files downloaded, videos or items ordered.

This means that web page data from the web server is used here and information that the web browser transmits to the web server to retrieve web pages. This information is transmitted with each individual page request.

Unlike other technologies, etracker does not read any information from the memory of your end device and does not store any data on your end device. The data is not used by etracker for any other purposes or passed on to third parties.

The cookies used do not receive any information that can identify you as a person. Data such as IP address, device and domain data are encrypted or shortened during storage. This means that neither we nor etracker can identify individual persons.

If you have consented to the use of cookies, the following cookies may be set:

Name: GS3_v

Value: 146480958312569961-9

Purpose: This cookie is set by the etracker Optimizer web service.

Expiry date: after one year

Name: _et_coid

Value: e9cc2b3efbf7807c6157e8b151baa2f3312569961-1

Purpose: This cookie is used for cookie recognition and is only set when the cookie is activated.

Expiry date: after 3 years

Name: pll_language

Value: de

Purpose: This cookie is used to save the preset language.

Expiry date: after one year

Note: Please note that the list given here only represents a selection of cookies used and cannot claim to be complete. Which cookies are set in a specific case depends on the evaluation mechanisms used in each case. You can view a list of all cookies under the following link: <https://www.etracker.com/docs/integration-setup/einstellungen-accounts/etracker-cookies/usage-cookies-count/>

How long and where is the data stored?

The data centre (the servers) is in Hamburg and all system administration also takes place in Hamburg. This means that all data is stored exclusively on German servers. The data is stored by etracker until the contract with us as a customer expires. After a short time following the end of the contract, all data is permanently deleted.

How can I delete my data or prevent data storage?

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

If you basically want to deactivate, delete or manage cookies, you will find the corresponding links to the respective instructions of the most popular browsers under the section "Cookies".

Legal basis

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

In addition to consent, we have a legitimate interest in analysing the behaviour of website visitors in order to improve our services technically and economically. With the help of etracker, we can detect website errors, identify attacks and improve the economic efficiency. The legal basis for this is **Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)**. Nevertheless, we only use etracker if you have given your consent.

We hope we have been able to provide you with the most important information about etracker's data processing. If you would like to learn more about the tracking service, we recommend that you read the company's privacy policy at <https://www.etracker.com/datenschutz/>.

Order processing agreement (AVV) etracker

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have concluded an order processing agreement (OPA) with etracker. What exactly is a GCU and, above all, what must be included in a GCU, you can read in our general section "Order processing agreement (GCU)".

This contract is required by law because etracker processes personal data on our behalf. It clarifies that etracker may only process data they receive from us according to our instructions and must comply with the DSGVO. You can find the link to the order processing agreement (AVV) at <https://www.etracker.com/av-vertrag/>.

Email Marketing Introduction

Email Marketing Summary

✓ Concerned parties: Newsletter subscribers

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

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

✗ Storage period: duration of the existence of the subscription

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

What is email marketing?

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

If you want to take part in our email marketing (mostly via newsletter), you usually just have to register with your email address. To do this, you fill out an online form and send it off. However, it may also happen that we ask you for your title and name so that we can write to you personally.

In principle, the registration for newsletters works with the help of the so-called "double opt-in procedure". After you have registered for our newsletter on our website, you will receive an email to confirm your newsletter registration. This ensures that the e-mail address belongs to you and that no one has registered with a third-party e-mail address. We or a notification tool we use logs each individual subscription. This is necessary so that we can prove that the registration process is legally correct. As a rule, the time of registration, the time of the registration confirmation and your IP address are saved. In addition, it is also logged when you make changes to your stored data.

Why do we use email marketing?

Of course, we want to stay in touch with you and always present you with the most important news about our company. For this purpose, we use, among other things, e-mail marketing - often just called "newsletter" - as an essential part of our online marketing. If you agree to this or if it is legally permitted, we will send you newsletters, system e-mails or other notifications by e-mail. When we use the term "newsletter" in the following text, we mainly mean regularly sent e-mails. Of course, we do not want to annoy you in any way with our newsletters. That's why we really do try to provide only relevant and interesting content. For example, you can learn more about our company, our services or products. Since we are always improving our offers, you will always find out through our newsletter when there is news or when we are offering special, lucrative promotions. If we use a service provider who offers a professional mailing tool for our email marketing, we do so in order to be able to offer you fast and secure newsletters. The purpose of our email marketing is basically to inform you about new offers and also to get closer to our corporate goals.

What data is processed?

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

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

In addition, information about your device or about your preferred

content is stored on our website. You can find out more about how data is stored when you visit a website in the section "Automatic data storage". We record your declaration of consent so that we can always prove that this complies with our laws.

Duration of data processing

If you unsubscribe your email address from our email/newsletter distribution list, we may store your address for up to three years based on our legitimate interests so that we can still prove your consent at the time. We may only process this data if we need 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 deletion request at any time. If you permanently object to the consent, we reserve the right to store your email address in a blacklist. As long as you have voluntarily subscribed to our newsletter, we will of course also keep your email address.

Right of objection

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 one or two clicks. In most cases, you will find a link to cancel your newsletter subscription directly at the end of each email. If you really can't find the link in the newsletter, please contact us by mail and we will cancel your newsletter subscription immediately.

Legal basis

The sending of our newsletter is based on your consent (Article 6 para. 1 lit. a DSGVO). This means that we may only send you a newsletter if you have actively registered for it beforehand. If applicable, we may also send you advertising messages, provided you have become our customer and have not objected to the use of your email address for direct advertising.

Information on specific email marketing services and how they process personal data, if any, is provided in the following sections.

CleverReach Privacy Policy

We use the CleverReach email marketing tool on our website. The service provider is the German company CleverReach GmbH & Co KG, Schafjückenweg 2, 26180 Rastede, Germany.

What is CleverReach?

The company was founded in 2007 and now serves over 320,000 customers worldwide. In addition to the classic newsletter dispatch, CleverReach also offers us other integrations and plug-ins to CRM, CMS and shop systems.

Why do we use CleverReach?

The tool is built in such a way that we can design pretty newsletters very easily and quickly without having to have any special web design skills. With CleverReach we can develop target group-oriented newsletter campaigns and inform you about news in our company. In addition, we also get to know your needs and interests better. For example, if we send out a newsletter that is hardly noticed by you, we will better adapt our offer to your needs in the future.

What data is processed?

If you register for our newsletter, personal data such as your email address, name, date of birth and place of residence will also be requested and processed during the registration process. In addition to the time and date of registration, your IP address is also recorded and stored on CleverReach servers. Web analytics data on your usage behaviour with the newsletter (e.g. whether you click on a link) may also be processed.

At CleverReach, data security has top priority. For this reason, all systems are regularly maintained and, if necessary, renewed. In this way, CleverReach can guarantee high stability, performance and maximum security.

You can find out more about the data processed through the use of CleverReach in the privacy policy at <https://www.cleverreach.com/de-en/datenschutz/>.

CleverReach Order Processing Agreement (AVV)

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have concluded a contract processing agreement (CPA) with CleverReach. What exactly is a GCU and, above all, what must be included in a GCU, you can read in our general section "Order processing agreement (GCU)".

This contract is required by law because CleverReach processes personal data on our behalf. It clarifies that CleverReach may only process data they receive from us according to our instructions and must comply with the GDPR.

Push Messages Introduction

Push Messages Summary

VAffected: Push Messages Subscribers

Purpose: notification of system-relevant and interesting events

Processed data: Data entered during registration, usually also location data. You can find more details on this in the respective push message tool used.

Storage period: Data is usually stored for as long as is necessary for the provision of the services.

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

What are push messages?

We also use so-called push notification services on our website, with which we can always keep our users up to date. This means that if you have agreed to the use of such push messages, we can send you short news items using a software tool. Push messages are a form of text message that appear directly to you on your smartphone or other devices such as tablets or PCs if you have signed up for them. You will receive these messages even if you are not on our website or not actively using our services.

In the process, data about your location and usage behaviour may also be collected and stored.

Why do we use push messages?

On the one hand, we use push messages to be able to fully provide the services we have contractually agreed with you. On the other hand, the messages also serve our online marketing. We can use these messages to give you an understanding of our service or our products. Especially when there are news in our company, we can inform you about it immediately. We want to get to know the preferences and habits of all our users as well as possible in order to continuously improve our offer.

What data is processed?

In order to receive push messages, you must also confirm that you want to receive these messages. The data accumulated during the consent process is also stored, managed and processed. This is necessary so that it can be proven and recognised that a user has agreed to receive the push messages. For this purpose, a so-called device token or push token is stored in your browser. Usually, the data of your location or the location of the terminal device you are using is also stored.

To ensure that we always send interesting and important push messages, the handling of the messages is also statistically evaluated. For example, we can then see whether and when you open the message. With the help of these insights, we can adapt our communication strategy to your wishes and interests. Although this stored data can be assigned to you, we do not want to check you as an individual. Rather, we are interested in the collected data of all our users so that we can make optimisations. You can find out exactly what data is stored in the data protection declarations of the respective service providers.

Duration of data processing

How long the data is processed and stored depends primarily on the tool we use. You can find out more about the data processing of the individual tools below. The privacy statements of the providers usually state exactly,

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

Legal basis

It may also be that the push messages are necessary so that certain obligations that are in a contract can be fulfilled. For example, so that we can provide you with technical or organisational news. In this case, the legal basis is Art. 6 para. 1 lit. b DSGVO.

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

The legal basis in this respect is Art. 6 para. 1 lit. a DSGVO. Of course, you can revoke your consent or change various settings in the settings at any time.

Messenger & Communication Introduction

Messenger & Communication Privacy Policy Summary

¶ Data subjects: Visitors to the website

Purpose: contact requests and general communication between us and you

¶ Data processed: Data such as name, address, email address, telephone number, general content data, IP address if applicable.

More details can be found in the respective tools used.

¶ Storage time: depending on the messenger & communication functions used.

Legal basis: Art. 6 para. 1 lit. a DSGVO (consent), Art. 6 para. 1 lit. f DSGVO (legitimate interests), Art. 6 para. 1 p. 1 lit. b. DSGVO (contractual or pre-contractual obligations)

What are messenger & communication functions?

We offer various options on our website (such as messenger and chat functions, online or contact forms, e-mail, telephone) to communicate with us. In doing so, your data will be processed and stored to the extent necessary to respond to your enquiry and our subsequent measures.

In addition to classic means of communication such as e-mail, contact forms or telephone, we also use chats or messengers. The currently most frequently used messenger

function is WhatsApp, but there are of course many different providers that offer messenger functions specifically for websites. If content is encrypted end-to-end, this is indicated in the individual data protection texts or in the privacy policy of the respective provider. End-to-end encryption means nothing other than that the content of a message itself is not visible to the provider. However, information about your device, location settings and other technical data can still be processed and stored.

Why do we use messenger & communication functions?

Communication possibilities with you are of great importance to us. After all, we want to talk to you and answer all possible questions about our service in the best possible way. Well-functioning communication is an important part of our service. With the practical messenger & communication functions, you can always choose the ones you prefer. In exceptional cases, however, we may not be able to answer certain questions via chat or messenger. This is the case, for example, when it comes to internal contractual matters. In this case, we recommend other communication options such as e-mail or telephone.

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

Insofar as this is the case, we point this out separately and work on the basis of an agreement in this respect. The essence of the agreement is set out below for the platform concerned.

Please note that when using our built-in elements, data from you may also be processed outside the European Union, as many providers, for example Facebook Messenger or WhatsApp are American companies.

This may make it less easy for you to claim or enforce your rights in relation to your personal data.

What data is processed?

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

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

How long is data stored?

How long the data is processed and stored depends primarily on the tools we use. Further below you can find out more about the data processing of the

individual tools. The data protection statements 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 it is necessary for the provision of our services. If data is stored in cookies, the storage period varies greatly. The data can be deleted immediately after leaving a website, but it can also remain stored for several years. You should therefore look at each individual cookie in detail if you want to know more about data storage. In most cases, you will also find informative information about the individual cookies in the data protection declarations of the individual providers.

Right of objection

You also have the right and the 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, deactivating or deleting cookies in your browser. For more information, please refer to the consent section.

As cookies may be used in messenger & communication functions, we also recommend that you read our general privacy policy on cookies. To find out exactly which of your data is stored and processed, you should read the privacy statements of the respective tools.

Legal basis

If you have consented that data from you can be processed and stored through integrated messenger & communication functions, this consent is considered the legal basis for data processing (**Art. 6 para. 1 lit. a DSGVO**). We process your enquiry and manage your data in the context of contractual or pre-contractual relationships in order to fulfil our pre-contractual and contractual obligations or to answer enquiries. The basis for this is **Art. 6 para. 1 p. 1 lit. b.**

DSGVO. In principle, your data will also be stored and processed on the basis of our legitimate interest (**Art. 6 para. 1 lit. f DSGVO**) in fast and good communication with you or other customers and business partners if consent has been given.

Chatbots Introduction

Chatbots Privacy Policy Summary

👤 Parties concerned: Visitors to the website

Purpose: contact requests and general communication between us and you

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

More details can be found in the respective tools used.

📅 Storage duration: depending on the chatbots & chat functions used.

📖 Legal basis: Art. 6 para. 1 lit. a DSGVO (consent), Art. 6 para. 1 lit. f

DSGVO (legitimate interests), Art. 6 para. 1 p. 1 lit. b. DSGVO (contractual or pre-contractual obligations)

What are chatbots?

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

Why do we use chatbots?

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

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

Please note that when you use our built-in elements, data about you may also be processed outside the European Union, as many providers are American companies. This may make it less easy for you to claim or enforce your rights in relation to your personal data.

What data is processed?

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

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

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

If you have agreed that a chatbot can send you a message, you can of course deactivate this activation at any time. The chatbot also serves as a help here and shows you how you can unsubscribe from this function. All your relevant data will then be deleted from the list of recipients.

We use the above-mentioned data in order to be able to address you personally via the chat, to answer your questions and enquiries or to send you possible content. It also allows us to improve our chat services in general.

How long is data stored?

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

Right of objection

You also have the right and the 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, deactivating or deleting cookies in your browser.

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

Legal basis

We ask for your permission via a pop-up window to process your data within the scope of the chat services. If you consent, this consent also serves as the legal basis (**Art. 6 para. 1 lit. a DSGVO**) for data processing. In addition, we process your enquiries and manage your data in the context of contractual or pre-contractual relationships in order to fulfil our pre-contractual and contractual obligations or to process your data in the context of contractual or pre-contractual relationships.

to answer enquiries. The basis for this is **Art. 6 para. 1 p. 1 lit. b. DSGVO**. In principle, your data is also stored and processed on the basis of our legitimate interest (**Art. 6 para. 1 lit. f DSGVO**) in fast and good communication with you or other customers and business partners. Nevertheless, we only use the tools if you have given your consent.

Social Media Introduction

Social Media Privacy Policy Summary

👤 Persons concerned: Visitors to the website

Purpose: Presentation and optimisation of our service, contact with visitors, interested parties, etc., advertising.

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

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

📅 Storage duration: depending on the social media platforms used.

📜 Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What is social media?

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

Why do we use social media?

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

The data that is stored and processed through your use of a social media channel is primarily for the purpose of being able to carry out web analyses. The aim of these analyses is to be able to develop more precise and personalised marketing and advertising strategies.

Depending on your behaviour on a social media platform, appropriate conclusions can be drawn about your interests with the help of the evaluated data and so-called user profiles can be created. This also enables the platforms to present you with customised advertisements. Cookies are usually set in your browser for this purpose, which store data on your usage behaviour.

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

Insofar as this is the case, we point this out separately and work on the basis of a

agreement in this regard. The essence of the agreement is then reproduced below for the platform concerned.

Please note that when using the social media platforms or our built-in elements, data of you may also be processed outside the European Union, as many social media channels, for example Facebook or Twitter, are American companies. This may make it less easy for you to claim or enforce your rights in relation to your personal data.

What data is processed?

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

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

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

Duration of data processing

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

Right of objection

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

Since cookies may be used with social media tools, we also recommend that you read our general privacy policy on cookies. To find out what data is collected from

You should read the privacy statements of the respective tools to find out exactly how your data is stored and processed.

Legal basis

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

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

LinkedIn Privacy Policy

LinkedIn Privacy Policy Summary

Parties concerned: Visitors to the website

Purpose: optimisation of our service performance

Processed data: Data such as user behaviour data, information about your device and your IP address. More details can be found below in the privacy policy.

Storage period: the data is deleted within 30 days as a matter of principle

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What is LinkedIn?

We use social plugins of the social media network LinkedIn, of the company LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA on our website. Through these functions, you can, for example, share content on LinkedIn directly via our website, log in via LinkedIn or follow interesting content. You can recognise the plug-ins by the company name or the LinkedIn logo. For the European Economic Area (EEA) and Switzerland, the company responsible is LinkedIn Ireland Unlimited (Wilton Place, Dublin 2, Ireland).

By embedding such plug-ins, data can be sent to LinkedIn, stored and processed there. In this privacy policy, we want to inform you about what data is involved, how the network uses this data and how you can manage or prevent the data storage.

LinkedIn is the largest social network for business contacts. Unlike Facebook, for example, it focuses exclusively on building business contacts. Companies can present services and products on the platform and establish business relationships. Many people also use LinkedIn for the

job search 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 can't follow all the social media channels individually. Even if it would be worth it, as in our case. Because time and again we post interesting news or reports that are worth spreading. That is why we have created the possibility on our website to share interesting content directly on LinkedIn or to link directly to our LinkedIn page. We consider built-in social plug-ins as an extended service on our website. The data that LinkedIn collects also helps us to show possible advertising measures only to people who are interested in our offer.

What data is stored by LinkedIn?

LinkedIn does not store any personal data merely by integrating the social plug-ins. LinkedIn calls this data generated by plug-ins passive impressions. However, when you click on a social plug-in, for example to share our content, the platform stores personal data as so-called "active impressions". And this is regardless of whether you have a LinkedIn account or not. If you are logged in, the collected data is assigned to your account.

Your browser establishes a direct connection to LinkedIn's servers when you interact with our plug-ins. In this way, the company logs various usage data. In addition to your IP address, this may include login data, device information or information about your internet or mobile provider. If you access LinkedIn services via your smartphone, your location (after you have allowed this) can also be determined. LinkedIn may also share this data with third party advertisers in a "hashed" form. Hashing means that a data record is transformed into a string of characters.

This makes it possible to encrypt the data in such a way that people can no longer be identified.

Most data about your user behaviour is stored in cookies. These are small text files that are usually set in your browser. LinkedIn may also use web beacons, pixel tags, display tags and other device identifiers.

Various tests also show which cookies are set when a user interacts with a social plug-in. The data found cannot claim to be complete and only serves as an example. The following cookies were set without being logged in to LinkedIn:

Name: bcookie

Value: =2&34aab2aa-2ae1-4d2a-8baf-c2e2d7235c16331692873346- **Purpose:** The cookie is a so-called "browser ID cookie" and consequently stores your identification number (ID).

Expiry date: After 2 years

Name: lang

Value: v=2&lang=en-en

Purpose: This cookie stores your preset or preferred language.

Expiry date: after end of session

Name: lidc

Wert: 1818367:t=1571904767:s=AQF6KNnJ0G331692873346...

Purpose: This cookie is used for routing. Routing records the ways you came to LinkedIn and how you navigate through the website there.

Expiry date: after 24 hours

Name: rtc

Value: kt0lrv3NF3x3t6xvDgGrZGDKkX

Purpose: No further information could be obtained about this cookie.

Expiry date: after 2 minutes

Name: JSESSIONID

Wert: ajax:3316928733462900777718326218137

Intended use: 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: AQHj7Ii23ZBcqAAAA...

Purpose: No further information could be found on this cookie.

Expiry date: after 7 days

Note: LinkedIn also works with third-party providers. That's why we also detected the two Google Analytics cookies `_ga` and `_gat` during our test.

How long and where is the data stored?

In principle, LinkedIn will retain your personal data for as long as it considers it necessary to provide its services. However, LinkedIn deletes your personal data when you delete your account. In some exceptional cases, LinkedIn may retain some data in aggregate and anonymised form even after you delete your account. Once you delete your account, other people will not be able to see your data within one day. LinkedIn generally deletes data within 30 days. However, LinkedIn retains data if it is necessary for legal reasons. Data that can no longer be assigned to a person remain stored even after the account is closed. The data is stored on various servers in America and presumably also in Europe.

How can I delete my data or prevent data storage?

You have the right to access and also delete your personal data at any time. You can manage, change and delete your data in your LinkedIn account.

In addition, you can also request a copy of your personal data from LinkedIn. This is how you access the account data in your LinkedIn profile:

In LinkedIn, click on your profile icon and select the "Settings and Privacy" section. Now click on "Privacy" and then on "Change" in the section "How LinkedIn uses your data". In just a short time, you can download selected data about your web activity and account history.

You also have the option in your browser to prevent data processing by LinkedIn. As mentioned above, LinkedIn stores most data via cookies that are set in your browser. You can manage, deactivate or delete these cookies. Depending on which browser you have, the management works slightly differently. Under the section "Cookies" you will find the corresponding links to the respective instructions of the most popular browsers.

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

Legal basis

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

LinkedIn also processes data from you in the USA, among other places. We would like to point out that according to the opinion of the European Court of Justice, there is currently no adequate level of protection.

This may be accompanied by various risks to the lawfulness and security of data processing.

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

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

More information on LinkedIn's standard contractual clauses can be found at <https://de.linkedin.com/legal/l/dpa> or <https://www.linkedin.com/legal/l/eu-sccs>.

We have tried to provide you with the most important information about LinkedIn's data processing. You can learn even more about the data processing of the social media network LinkedIn at <https://www.linkedin.com/legal/privacy-policy>.

XING Privacy Policy

Xing Privacy Policy Summary

✓ Parties concerned: Visitors to the website

Purpose: optimisation of our service performance

Processed data: your IP address, browser data, date and time of your page view may be stored.

More details on this can be found below in the privacy policy.

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

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What is Xing?

We use social plugins of the social media network Xing, of the company Xing SE, Dammtorstraße 30, 20354 Hamburg, Germany, on our website. Through these functions, you can, for example, share content on Xing directly via our website, log in via Xing or follow interesting content. You can recognise the plug-ins by the company name or the Xing logo. When you call up a website that uses a Xing plug-in, data may be transmitted to the "Xing servers", stored and analysed. In this data protection declaration, we want to inform you about what data is involved and how you can manage or prevent this data storage.

Xing is a social network with its headquarters in Hamburg. The company specialises in managing professional contacts. This means that unlike other networks, Xing is primarily about professional networking. The platform is often used for job searches or to find employees for one's own company.

Xing also offers interesting content on various professional topics. The global counterpart is the American company LinkedIn.

Why do we use Xing on our website?

There is now a flood of social media channels and we are well aware that your time is very precious. Not every company's social media channel can be closely scrutinised. That's why we want to make your life as easy as possible so that you can share or follow interesting content directly from our website on Xing. With such "social plug-ins" we expand our service on our website.

In addition, the data collected by Xing helps us to carry out targeted advertising measures on the platform. This means that our service is only shown to people who are really interested in it.

What data is stored by Xing?

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

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

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

Name: AMCVS_0894FF2554F733210A4C98C6%40AdobeOrg

Value: 1

Purpose: This cookie is used to create and store website visitor identifiers.

Expiry date: after end of session

Name: c_

Value: 157c609dc9fe7d7ff56064c6de87b019312569961-8

Purpose: We were not able to find out any more information about this cookie.

Expiry date: after one day

Name: prevPage

Value: wbm%2FWelcome%2Flogin

Purpose: This cookie stores the URL of the previous website you visited.

Expiry date: after 30 minutes

Name: s_cc

Value: true

Purpose: This Adobe Site Catalyst cookie determines whether cookies are generally enabled in the browser.

Expiry date: after **end** of session

Name: s_fid

Value: 6897CDCD1013221C-39DDACC982217CD1312569961-2

Purpose: This cookie is used to identify a unique visitor.

Expiry date: after 5 years

Name: visitor_id

Value: fe59fbe5-e9c6-4fca-8776-30d0c1a89c32

Purpose: The visitor cookie contains a unique visitor ID and the unique identifier for your account.

Expiry date: after 2 years

Name: _session_id

Value: 533a0a6641df82b46383da06ea0e84e7312569961-2

Purpose: This cookie creates a temporary session ID that is used as an in-session user ID. The cookie is absolutely necessary to provide the functions of Xing.

Expiry date: after **end** of session

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

How long and where is the data stored?

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

How can I delete my data or prevent data storage?

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

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

Legal basis

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

We have tried to bring you closer to the most important information about data processing by Xing. You can learn even more about the data processing of the social media network Xing at <https://privacy.xing.com/de/datenschutzerklaerung>.

Blogs and publication media Introduction

Blogs and Publication Media Privacy Policy Summary

Data subjects: Visitors to the website

Purpose: Presentation and optimisation of our service performance as well as communication between website visitors, security measures and administration.

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

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

Storage duration: depending on the tools used

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

What are blogs and publication media?

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

Why do we use blogs and publication media?

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

What data is processed?

Exactly what data is processed always depends on the communication functions we use. Very often, IP address, user name and the published content are stored. This is done primarily to ensure security protection, to prevent spam and to be able to take action against illegal content. Cookies can also be used for data storage. These are small text files that are stored with information in your browser. You can find more details about the data collected and stored in our individual sections and in the privacy policy of the respective provider.

Duration of data processing

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

Right of objection

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

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

Legal basis

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

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

That is why we recommend that you read our privacy text about cookies carefully and look at the privacy policy or cookie policy of the respective service provider.

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

Blog posts and comment functions Privacy policy

There are various online communication tools that we can use on our website. For example, we use blog posts and comment functions. This gives you the opportunity to comment on content or write posts. If you use this function, your IP address may be stored for security reasons. This is how we protect ourselves from illegal content such as insults, unauthorised advertising or prohibited political propaganda. In order to identify whether comments are spam, we may also store and process user data on the basis of our legitimate interest. If we launch a poll, we will also store your IP address for the duration of the poll so that we can ensure that all participants really only vote once. Cookies may also be used for storage purposes. All data that we store from you (such as content or information about you) will remain stored until you object.

Online Marketing Introduction

Online Marketing Privacy Policy Summary

¶ Data subjects: Visitors to the website

Purpose: Evaluation of visitor information to optimise the web offer.

Processed data: Access statistics, which include data such as access locations, device data, access duration and time, navigation behaviour, click behaviour and IP addresses. Personal data such as name or e-mail address may also be processed. You can find more details on this in the respective online marketing tool used.

¶ Storage duration: depending on the online marketing tools used.

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What is online marketing?

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

Why do we use online marketing tools?

We want to show our website to everyone who is interested in what we have to offer. We are aware that this is not possible without conscious measures. That is why we do online marketing. There are various tools that make it easier for us to work on our online marketing measures and additionally always provide suggestions for improvement via data. In this way, we can target our campaigns more precisely to our target group. So the purpose of these online marketing tools we use is ultimately to optimise our offer.

What data is processed?

In order for our online marketing to work and the success of the measures to be measured, user profiles are created and data is stored, for example, in cookies (these are small text files). With the help of this data, we can not only place advertisements in the classic sense, but also display our content directly on our website in the way you prefer. For this purpose, there are various third-party tools that offer these functions and accordingly also collect and store data from you. The named cookies store, for example, which web pages you have visited on our website, how long you have looked at these pages, which links or buttons you click or from which website you have come to us. In addition, technical information may also be stored. For example, your IP address, which browser you use, from which end device you visit our website or the time when you accessed our website and when you left it again. If you have consented to us also determining your location, we can also store and process this.

Your IP address is stored in pseudonymised form (i.e. shortened). Unique data that directly identifies you as a person, such as your name, address or email address, is also only stored in pseudonymised form as part of the advertising and online marketing procedures. We are therefore unable to identify you as a person, but only have the pseudonymised information stored in the user profiles.

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

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

With all the advertising tools we use that store data from you on their servers, we only ever receive aggregated information and never data that makes you identifiable as an individual. The data only shows how well the advertising measures worked. For example, we see which measures have persuaded you or other users to come to our website and purchase a service or product there. Based on the analyses, we can improve our advertising offer in the future and adapt it even more precisely to the needs and wishes of interested persons.

Duration of data processing

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

Right of objection

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, deactivating or deleting cookies in your browser. The lawfulness of the processing remains unaffected until the revocation.

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

Legal basis

If you have consented to third-party providers being used, the legal basis for the corresponding data processing is this consent. According to **Art. 6 para. 1 lit. a DSGVO (consent)**, this **consent** constitutes the legal basis for the processing of personal data as it may occur when collected by online marketing tools.

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

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

Affiliate programmes Introduction

Affiliate Programmes Privacy Policy Summary

¶ Data subjects: Visitors to the website

Purpose: economic success and the optimisation of our service performance.

¶ Processed data: Access statistics, the data such as locations of accesses,

device data, access duration and time, navigation behaviour, click behaviour and IP addresses. Personal data such as name or email address can also be processed.

Storage period: personal data is usually stored by partner programmes until it is no longer required

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What are partner programmes?

We use partner programmes of different providers on our website. By using an affiliate programme, data may be transferred from you to the respective affiliate programme provider, stored and processed. In this data protection text, we will give you a general overview of the data processing by affiliate programmes and show you how you can also prevent or revoke a data transfer. Every partner programme (also called affiliate programme) is based on the principle of commission. A link or an advertisement including a link is placed on our website and if you are interested in it and click on it and purchase a product or service in this way, we receive a commission for this (reimbursement of advertising costs).

Why do we use affiliate programmes on our website?

Our goal is to provide you with an enjoyable time with lots of helpful content. For this, we put a lot of work and time into the development of our website. With the help of affiliate programmes, we have the opportunity to also be rewarded a little for our work. Of course, every affiliate link always has to do with our topic and shows offers that might interest you.

What data is processed?

In order to be able to track whether you have clicked on a link used by us, the partner programme provider must know that it was you who followed the link via our website. There must therefore be a correct assignment of the partner programme links used to the subsequent actions (transaction, purchase, conversion, impression, etc.). Only then can the settlement of commissions work.

For this assignment to work, a value can be attached to a link (in the URL) or information can be stored in cookies. This information includes the page from which you came (referrer), when you clicked on the link, an identifier of our website, which offer it is and a user identifier.

This means that as soon as you interact with products and services of a partner programme, this provider also collects data from you. Exactly what data is stored depends on the individual provider. For example, the Amazon affiliate programme distinguishes between active and automatic information. Active information includes name, email address, telephone number, age, payment information or location information. The automatically stored information in this case includes user behaviour, IP address, device information and the URL.

Duration of data processing

We will inform you about the duration of data processing below, provided we have further information on this. In general, personal data is only processed for as long as it is necessary for the provision of the services and products. Data stored in cookies are stored for different lengths of time. Some cookies are already deleted after you leave the website, others may be stored in your browser for several years if they are not actively deleted. The exact duration of data processing depends on the provider used, but you should usually 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 data processing.

Right of objection

You always have the right to information, correction and deletion of your personal data. If you have any questions, you can also contact responsible persons of the partner programme provider used at any time. You can find contact details either in our specific privacy policy or on the website of the relevant provider.

You can delete, deactivate or manage cookies that providers use for their functions in your browser. Depending on which browser you use, this works in different ways.

Legal basis

If you have consented to partner programmes being used, the legal basis for the corresponding data processing is this consent. According to **Art. 6 para. 1 lit. a DSGVO (consent)**, this **consent** constitutes the legal basis for the processing of personal data as it may occur during the collection through a partner programme.

On our part, there is also a legitimate interest in using an affiliate programme to optimise our online service and our marketing measures. The corresponding legal basis for this is **Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)**. Nevertheless, we only use the partner programme if you have given your consent.

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

Content Delivery Networks Introduction

Content Delivery Networks Privacy Policy Summary

¶ Data subjects: Visitors to the website

Purpose: to optimise our service performance (to enable the website to load faster).

] Processed data: Data such as your IP address
More details can be found below and in the individual data protection texts.
Storage period: for the most part, the data is stored until it is no longer required for the fulfilment of the service.
Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What is a Content Delivery Network?

We use a so-called Content Delivery Network on our website. Such a network is usually just called a CDN. A CDN helps us to load our website quickly and smoothly, regardless of your location. In the process, your personal data is also stored, managed and processed on the servers of the CDN provider used. In the following, we will go into more detail about the service and its data processing. You will find detailed information about the handling of your data in the respective privacy policy of the provider.

Every Content Delivery Network (CDN) is a network of regionally distributed servers that are all connected to each other via the internet. Via this network, website content (especially very large files) can be delivered quickly and smoothly even during large load peaks. The CDN creates a copy of our website on your servers for this purpose. Since these servers are distributed worldwide, the website can be delivered quickly. Consequently, the data transfer to your browser is significantly shortened by the CDN.

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

A fast-loading website is part of our service. Of course, we know how annoying it is when a website loads at a snail's pace. Most of the time, people even lose their patience and run away before the website is fully loaded. Of course, we want to avoid that. That's why a fast-loading website is a natural part of our website offering. With a Content Delivery Network, our website loads much faster in your browser. The use of a CDN is particularly helpful if you are abroad, because the website is delivered from a server near you.

What data is processed?

When you request a website or the content of a website and it is cached in a CDN, the CDN routes the request to the server closest to you and it delivers the content. Content Delivery Networks are built so that JavaScript libraries can be downloaded and hosted on npm and Github servers. Alternatively, most CDNs allow WordPress plugins to be loaded if they are hosted on WordPress.org. Your browser may send personal data to the Content Delivery Network we use. This includes data such as IP address, browser type, browser version, which web page is loaded or the time and date of the page visit. This data is collected and stored by the CDN. Whether cookies are used for data storage depends on the network used. Please read the data protection texts of the respective service.

Right of objection

If you want to completely prevent this data transfer, you can install a JavaScript blocker (see for example <https://noscript.net/>) on your PC. Of course, our website will then no longer be able to offer the usual service (such as fast loading speed).

Legal basis

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

We also have a legitimate interest in using a content delivery network to optimise our online service and make it more secure. The corresponding legal basis for this is **Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)**.

Nevertheless, we only use the tool if you have given your consent.

Information on specific content delivery networks, if any, is provided in the following sections.

Cookie Consent Management Platform Introduction

Cookie Consent Management Platform Summary

✓ Concerned: Website visitors

Purpose: to obtain and manage consent to certain cookies and thus the use of certain tools.

] Processed data: Data used to manage the cookie settings set, such as IP address, time of consent, type of consent, individual consents.

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

] Storage period: Depends on the tool used, one must be prepared for periods of several years.

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

What is a Cookie Consent Management Platform?

We use Consent Management Platform (CMP) software on our website to help us and you deal correctly and safely with scripts and cookies in use. The software automatically creates a cookie pop-up, scans and checks all scripts and cookies, provides cookie consent for you as required by data protection law and helps us and you to keep track of all cookies. With most cookie consent management tools, all existing cookies are identified and categorised. You as a website visitor then decide yourself whether and which scripts and cookies you allow or do not allow. The following graphic illustrates 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. In addition, 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 store and process data from you. It is also your right to decide for yourself which cookies you accept and which you do not. In order to grant you this right, we first need to know exactly which cookies have ended up on our website in the first place. Thanks to a cookie management tool that regularly scans the website for all existing cookies, we know about all cookies and can provide you with information about them in compliance with the GDPR.

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

What data is processed?

Within the framework 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 query you each time you visit our website again and so that we can also prove your consent if required by law. This is stored either in an opt-in cookie or on a server. Depending on the provider of the cookie management tool, the storage period of your cookie consent varies. In most cases, this data (e.g. pseudonymous user ID, time of consent, details of cookie categories or tools, browser, device information) is stored for up to two years.

Duration of data processing

We will inform you about the duration of data processing below, provided we have further information on this. In general, we only process personal data for as long as is strictly necessary for the provision of our services and products. Data stored in cookies are stored for different lengths of time. Some cookies are deleted as soon as you leave the website, others may be stored in your browser for several years. The exact duration of data processing depends on the tool used, but 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 data processing.

Right of objection

You also have the right and the possibility 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 through cookies by managing, deactivating or deleting cookies in your browser.

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

Legal basis

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

Security & Anti-Spam

Security & Anti-Spam Privacy Policy Summary

👤 Persons concerned: Visitors to the website

🎯 Purpose: cyber security

📄 Data processed: Data such as your IP address, name or technical data such as browser version.

📖 More details can be found below and in the individual data protection texts.

🕒 Storage period: for the most part, data is stored until it is no longer required for the fulfilment of the service

📜 Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What is Security & Anti-Spam Software?

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

Why do we use security & anti-spam software?

We place particular emphasis on security on our website. After all, it is not only our security that is at stake, but above all yours. Unfortunately, cyber threats have become part of everyday life in the world of IT and the Internet. Hackers often try to steal personal data from an IT system with the help of a cyberattack. And that is why a good defence system is absolutely necessary. A security system monitors all incoming and outgoing connections to our network or computer. In order to achieve even greater security against cyber attacks, we also use other external security services in addition to the standardised security systems on our computer. Unauthorised data traffic is thus better prevented and we protect ourselves from cybercrime.

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

Exactly what data is collected and stored depends, of course, on the service in question. However, we always endeavour to use only programmes that collect data very sparingly or only store data that is necessary for the fulfilment of the service offered. In principle, the service may store data such as name, address, IP address, e-mail address and technical data such as browser type or browser version. Any performance and log data may also be collected in order to detect possible incoming threats in good time. This data is processed within the scope of the services and in compliance with applicable laws. This also includes the GDPR in the case of US providers (via the standard contractual clauses). These security services also work in some cases with third-party providers who may store and/or process data under instruction and in accordance with the data protection policies and further security measures. The data storage is mostly done via cookies.

Duration of data processing

We will inform you about the duration of data processing below, provided we have further information on this. For example, security programmes store data until you or we revoke the data storage. In general, personal data is only stored for as long as is absolutely necessary for the provision of the services. In many cases, we unfortunately lack precise information from the providers about the length of storage.

Right of objection

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

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

Legal basis

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

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

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

ManageWP Privacy Policy

We use ManageWP, a security management tool, for our website. The service provider is the American company GoDaddy.com LLC, 14455 N. Hayden Rd. Hayden Rd, Ste. 219, Scottsdale, AZ 85260, USA.

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

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

The Data Processing Addendum, which corresponds to the standard contractual clauses, can be found at <https://gcd.com/legal/data-addendum/>.

You can find out more about the data processed through the use of ManageWP in the privacy policy at <https://managewp.com/privacy>.

Cloud services

Cloud Services Privacy Policy Summary

Affected parties: We as website operator and you as website visitor

Purpose: security and data storage

Data processed: Data such as your IP address, name or technical data such as browser version. More details can be found below and in the individual data protection texts or in the data protection declarations of the providers.

Storage period: for the most part, data is stored until it is no longer required for the fulfilment of the service.

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What are cloud services?

Cloud services provide us as website operators with storage space and computing power via the internet. Data can be transferred to an external system, processed and stored via the internet. The corresponding cloud provider takes over the management of this data. Depending on the requirements, an individual person or also a company can choose the storage space size or computing power. Cloud storage is accessed via an API or storage protocols. API stands for Application Programming Interface and means a programming interface that connects software with hardware components.

Why do we use cloud services?

We use cloud services for several reasons. A cloud service offers us the possibility to store our data securely. In addition, we have access to the data from different places and devices and thus have more flexibility and facilitate our work processes. Cloud storage also saves us money because we don't have to build and manage our own infrastructure for data storage and security.

By storing our data centrally in the cloud, we can also expand our fields of application and manage our information much better.

So we as website operators or as a company use cloud services primarily for our own purposes. For example, we use the services to manage our calendar, to store documents or other important information in the cloud.

However, your personal data may also be stored in the process. This is the case, for example, if you provide us with your contact details (such as name and email address) and we store our customer data with a cloud provider. Consequently, data that we process from you may also be stored and processed on external servers. If we offer certain forms or content from cloud services on our website, cookies may also be set for web analysis and advertising purposes. Furthermore, such cookies remember your settings (such as the language used) so that you will find your familiar web environment the next time you visit our website.

What data is processed by cloud services?

Much of the data we store in the cloud does not relate to individuals, but some data is considered personal data according to the definition of the GDPR. This is often customer data such as name, address, IP address or telephone number or technical device information. Videos, images and audio files can also be stored in the cloud. Exactly how the data is collected and stored depends on the service. We only try to use services that handle the data in a very trustworthy and professional manner. Basically, the services, such as Amazon Drive, have access to the stored files in order to be able to offer their own service accordingly. For this, however, the services need permission, such as the right to copy files for security reasons. This data is processed and managed within the scope of the services and in compliance with the applicable laws. This also includes the GDPR for US providers (via the standard contractual clauses). These cloud services also work in some cases with third party providers who may process data under instruction and in accordance with the privacy policy and further security measures. We

would like to emphasise once again at this point that all known cloud services (such as Amazon Drive, Google Drive or Microsoft Onedrive) obtain the right to have access to stored content in order to be able to offer and optimise their own service accordingly.

Duration of data processing

We will inform you about the duration of data processing below, provided we have further information on this. In general, cloud services store data until you or we revoke the data storage or delete the data again. In general, personal data is only stored as long as it is absolutely necessary for the provision of the services. However, a final data deletion from the cloud may take a few months. This is the case because the data is usually not only stored on one server, but is distributed on different servers.

Right of objection

You also have the right and the possibility to revoke your consent to data storage in a cloud at any time. If cookies are used, you also have a right of revocation here. This works either via our cookie management tool or via other opt-out functions. For example, you can also prevent data collection through cookies by managing, deactivating or deleting cookies in your browser. We also recommend that you read our general privacy policy on cookies. To find out exactly which of your data is stored and processed, you should read the privacy statements of the respective cloud providers.

Legal basis

We use cloud services mainly on the basis of our legitimate interests (Art. 6 para. 1 lit. f DSGVO) in a good security and storage system.

Certain processing, in particular the use of cookies and the use of storage functions, requires your consent. If you have consented to your data being processed and stored by cloud services, this consent is the legal basis for the data processing (Art. 6 para. 1 lit. a DSGVO). Most of the services we use set cookies in your browser to store data. That is why we recommend that you read our privacy text on cookies carefully and view the privacy policy or cookie policy of the respective service provider.

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

Payment provider introduction

Payment Provider Privacy Policy Summary

¶ Data subjects: Visitors to the website

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

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

Storage period: depending on the payment provider used

Legal basis: Art. 6 para. 1 lit. b DSGVO (fulfilment of a contract)

What is a payment provider?

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

Why do we use payment providers on our website?

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

What data is processed?

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

The data is usually stored and processed on the servers of the payment providers. We as the website operator do not receive this data. We are only informed whether the payment has worked or not. For identity and creditworthiness checks, payment providers may forward data to the appropriate office. The business and data protection principles of the respective provider always apply to all payment transactions. Therefore, please always check the General Terms and Conditions and the privacy policy of the payment provider. You also have the right to have data deleted or corrected at any time. Please contact the respective service provider regarding your rights (right of revocation, right to information and right to be affected).

Duration of data processing

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

Right of objection

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

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

Legal basis

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

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

PayPal Privacy Policy

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

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

As a basis for data processing with recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, i.e. in particular in the USA) or a data transfer there, PayPal uses so-called standard contractual clauses (= Art.

46. para. 2 and 3 DSGVO). Standard Contractual Clauses (SCC) are templates provided by the EU Commission and are intended to ensure that your data comply with European data protection standards even if they are transferred to third countries (such as the USA) and stored there. Through these clauses, PayPal undertakes to comply with the European level of data protection when processing your relevant data, even if the data is stored, processed and managed in the US. These clauses are based on an implementing decision of the EU Commission. You can find the decision and the corresponding standard contractual clauses here, among other places: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=en

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

Visa Privacy Policy

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

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

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

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

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

External online platforms Introduction

External Online Platforms Privacy Policy Summary

Data subjects: Visitors to the website or visitors to the external online platforms.

Purpose: Presentation and optimisation of our service performance, contact with visitors, interested parties

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

You can find more details on this at the respective platform used.

Storage duration: depending on the platforms used

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What are external online platforms?

In order to be able to offer our services or products outside of our website, we also use external platforms. These are mostly online marketplaces such as Amazon or eBay. In addition to our responsibility for data protection, the data protection provisions of the external platforms we use also apply. This is specifically the case when our products are purchased via the platform. So if there is a payment process. Furthermore, most platforms also use your data to optimise their own marketing measures. For example, with the help of collected data, the platform can tailor advertisements precisely to the interests of customers and website visitors.

Why do we use external online platforms?

In addition to our website, we also want to offer our products on other platforms in order to bring our offer closer to more customers. External online marketplaces such as Amazon, Ebay or Digistore24 offer large sales websites that offer our products to people who may not be familiar with our website. It may also happen that built-in elements on our site redirect to an external online platform. Data that is processed and stored by the online platform used serves the company on the one hand to log the payment process and on the other hand to be able to carry out web analyses.

The aim of these analyses is to be able to develop more precise and personalised marketing and advertising strategies. Depending on your behaviour on a platform, appropriate conclusions can be drawn about your interests with the help of the analysed data and so-called user profiles can be created. In this way, it is also possible for the platforms to present you with customised advertisements or products. Cookies are usually set in your browser for this purpose, which store data on your usage behaviour.

Please note that when using the platforms or our built-in elements, data from you may also be processed outside the European Union, as online platforms, for example Amazon or eBay, are American companies.

This may make it less easy for you to claim or enforce your rights in relation to your personal data.

What data is processed?

Exactly what data is stored and processed depends on the external platform. But usually it is data such as telephone numbers, email addresses, data you enter in a contact form, user data such as which buttons you click, when you visited which pages, information about your device and your IP address. Very often, most of this data is stored in cookies. If you have your own profile on an external platform and are also logged in there, data can be linked to the profile. The collected data is stored on the servers of the platforms used and processed there. You can find out exactly how an external platform stores, manages and processes data in the respective privacy policy. If you have questions about data storage and data processing or wish to assert corresponding rights, we recommend that you contact the platform directly.

Duration of data processing

We will inform you about the duration of data processing below, provided we have further information on this. For example, Amazon stores data until it is no longer needed for its own purpose. In general, we only process personal data for as long as is absolutely necessary for the provision of our services and products.

Right of objection

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

Since cookies may be used, we also recommend that you read our general privacy policy on cookies. To find out exactly which of your data is stored and processed, you should read the privacy statements of the respective external platforms.

Legal basis

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

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

Credit Assessment Bodies Introduction

Credit Assessment Bodies Privacy Policy Summary

☑ Affected parties: Clients

Purpose: creditworthiness and credit assessment

Processed data: Inventory data, payment data, contact data, contract data

Storage duration: depending on the test points used.

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What are credit rating agencies?

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

Why do we use credit assessment agencies?

In our business it happens from time to time that we render a service before the contractually stipulated consideration or accept similar economic risks. This is always the case, for example, when an order is placed on account. In order to protect our legitimate interests, we may obtain so-called identity and creditworthiness information.

In this process, the credit risk is assessed with the help of a mathematical-statistical procedure by credit rating agencies (credit agencies).

What data is processed?

The decision to advance or not is made by software that works with the information from the credit rating agency on the basis of an automated decision in the individual case (= Art. 22 DSGVO). The data that is usually processed includes, for example, name, address, bank details, invoices, payment history, contact data such as e-mail address and telephone number, as well as contract data such as term, customer information and the subject matter of the contract. You can find out more information about data processing in the data protection statements of the respective credit rating agencies.

Duration of data processing

The length of time for which the data is processed and stored depends mainly on the credit rating agencies we use. You can find out more about the data processing of the individual providers below. The providers' data protection statements usually state exactly what data is stored and processed and for how long.

In principle, personal data is only processed for as long as is necessary for the provision of our services. When data is stored in cookies, it varies

the storage period strongly. 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(1) lit. a DSGVO) for the credit rating information and also for the transmission of the customer's data to an inspection agency. If this consent does not exist, the legal basis is our legitimate interest (Article 6(1)(f) DSGVO) in default protection. If we obtain consent from you, this is also the legal basis for creditworthiness information and data transmission.

We have no influence on the specific checking process or the profiling of the credit rating agencies we use and thus on the accuracy or appropriateness of the result. In this respect, we are not responsible under data protection law. Responsibility in this respect remains solely with the credit rating agency, to whose data protection information we refer below. We are only responsible for obtaining and using creditworthiness information provided by third parties in individual cases.

SCHUFA Privacy Policy

We use SCHUFA, a credit information agency, for our business. The service provider is the German company SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden, Germany. You can find out more about the data processed through the use of SCHUFA in the data protection declaration at <https://www.schufa.de/global/datenschutz-dsgvo/>.

Audio & Video Introduction

Audio & Video Privacy Policy Summary

👤 Parties concerned: Visitors to the website

Purpose: optimisation of our service performance

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

You will find more details on this below in the relevant data protection texts. 📄

Storage period: Data are generally stored for as long as they are necessary for the purpose of the service.

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What are audio and video elements?

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

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

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

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

Of course we want to provide you with the best offer on our website. And we are aware that content is no longer conveyed merely 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 that are entertaining or informative and ideally even both. This enhances our service and makes it easier for you to access interesting content. Thus, in addition to our texts and images, we also offer video and/or audio content.

What data is stored by audio & video elements?

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

Duration of data processing

You can find out exactly how long the data is stored on the servers of the third-party providers either below in the data protection text of the respective tool or in the privacy policy of the provider. In principle, personal data is only processed for as long as is absolutely necessary for the provision of our services or products. As a rule, this also applies to third-party providers. In most cases, you can assume that certain data will be stored on the servers of third-party providers for several years. Data can be stored for different lengths of time specifically in cookies. Some cookies are deleted as soon as you leave the website, others can be stored in your browser for several years.

Right of objection

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, deactivating or deleting cookies in your browser. The lawfulness of the processing until the revocation remains unaffected.

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

Legal basis

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

Video Conferencing & Streaming Introduction

Video Conferencing & Streaming Privacy Policy Summary

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

Purpose: communication and presentation of content

Data processed: Access statistics containing data such as name, address, contact details, email address, telephone number or your IP address. More details can be found in the respective video conferencing or streaming tool used.

Storage duration: depending on the video conferencing or streaming tool used.

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests), Art. 6 para. 1 lit. b DSGVO (Contract)

What are video conferencing & streaming?

We use software programmes that enable us to hold video conferences, online meetings, webinars, display sharing and/or streaming. Video conferencing or streaming involves the simultaneous transmission of information via sound and moving image. With the help of such video conferencing or streaming tools, we can communicate with customers, business partners, clients and also employees quickly and easily via the Internet. Of course, we pay attention to the specified legal framework conditions when selecting the service provider.

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

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

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

What data is processed?

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

Exactly what data is stored depends on the solutions used. Each provider stores and processes different and varying amounts of data. But as a rule, most providers store your name, your address, contact data such as your email address or your telephone number and your IP address.

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

Duration of data processing

We will inform you about the duration of data processing below in connection with the service used, 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. It may be that the provider stores data from you according to its own specifications, over which we then have no influence.

Right of objection

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

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

Legal basis

If you have consented to your data being processed and stored by the video or streaming solution, this consent is the legal basis for the data processing (**Art. 6 para. 1 lit. a DSGVO**). In addition, we can also use a

offer video conferencing as part of our services if this has been contractually agreed with you in advance (**Art. 6 para. 1 lit. b DSGVO**). In principle, your data will also be stored and processed on the basis of our legitimate interest (**Art. 6 para. 1 lit. f DSGVO**) in fast and good communication with you or other customers and business partners, but only if you have at least consented to this. Most video or streaming solutions also set cookies in your browser to store data. Therefore, we recommend that you read our privacy text about cookies carefully and look at the privacy policy or cookie policy of the respective service provider.

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

Cisco WebEx Privacy Policy

We use Cisco WebEx on our website, a service for online meetings and video conferences. The service provider is the American company Cisco Systems, Inc., Legal Department, 170 West Tasman Dr., San Jose, CA 95134 USA.

Cisco also processes data in the USA, among other places. We would like to point out that according to the opinion of the European Court of Justice, there is currently no adequate level of protection for the transfer of data to the USA. This may be associated with various risks for the legality and security of data processing.

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

You can find out more about the data processed through the use of Cisco WebEx in the Privacy Policy at <https://www.cisco.com/c/en/us/about/legal/privacy-full.html>.

Microsoft Teams Privacy Policy

We use Microsoft Teams, an online meeting and video conferencing service, on our website. The service provider is the American company Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA.

Microsoft also processes data from you in the USA, among other places. We would like to point out that according to the opinion of the European Court of Justice, there is currently no adequate level of protection for the transfer of data to the USA. This may be associated with various risks for the legality and security of data processing.

As the basis of data processing for recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, i.e. in particular the USA) or

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

More information on Microsoft's standard contractual clauses can be found at <https://learn.microsoft.com/en-us/compliance/regulatory/offering-eu-model-clauses>.

You can find out more about the data processed by using Microsoft in the privacy policy at <https://privacy.microsoft.com/de-de/privacystatement>.

Skype Privacy Policy

We use Skype, a service for chat and video conferencing solutions, on our website. The service provider is the American company Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA.

Microsoft also processes data from you in the USA, among other places. We would like to point out that according to the opinion of the European Court of Justice, there is currently no adequate level of protection for the transfer of data to the USA. This may be associated with various risks for the legality and security of data processing.

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

More information on Microsoft's standard contractual clauses can be found at <https://learn.microsoft.com/en-us/compliance/regulatory/offering-eu-model-clauses>.

You can find out more about the data processed by using Microsoft in the privacy policy at <https://privacy.microsoft.com/de-de/privacystatement>.

TeamViewer Privacy Policy

We use TeamViewer, a service for web conferencing and remote maintenance, on our website. The service provider is the German company TeamViewer Germany GmbH, Bahnhofplatz 2, 73033 Göppingen, Germany.

You can find out more about the data processed through the use of TeamViewer in the Privacy Policy at <https://www.teamviewer.com/de/datenschutzinformation/>.

Zoom Privacy Policy

Zoom Privacy Policy Summary

Affected: Users who use Zoom

Purpose: an additional service for our website visitors

Processed data: Access statistics, which include data such as name, address, contact details, email address, telephone number or your IP address. More details can be found below in this privacy policy.

Storage period: Data is stored for as long as Zoom requires it for the purpose of the service.

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests), Art. 6 para. 1 lit. b DSGVO (Contract)

What is Zoom?

We use the Zoom video conferencing tool from the American software company Zoom Video Communications for our website. The company is headquartered in San Jose, California, 55 Almaden Boulevard, 6th Floor, CA 95113. Thanks to "Zoom", we can hold a video conference with customers, business partners, clients and also employees very easily and without installing any software. In this privacy statement, we go into more detail about the service and inform you about the most important aspects relevant to data protection.

Zoom is one of the world's best-known video conferencing solutions. With the "Zoom Meetings" service, we can hold an online video conference with you, for example, but also with employees or other users via a digital conference room. This makes it very easy for us to get in touch digitally, exchange information on various topics, send text messages or even talk on the phone. Furthermore, you can also share the screen, exchange files and use a whiteboard via Zoom.

Why do we use Zoom on our website?

It is important to us that we can communicate with you quickly and easily. And that's exactly what Zoom offers us. The software programme also works directly via a browser. This means we can simply send you a link and start the video conference. Of course, additional functions such as screen sharing or exchanging files are also very practical.

What data is stored by Zoom?

When you use Zoom, data is also collected from you so that Zoom can provide its services. On the one hand, this is data that you consciously provide to the company. This includes, for example, your name, telephone number or e-mail address. However, data is also automatically transmitted to Zoom and stored.

This includes, for example, technical data of your browser or your IP address. In the following, we will go into more detail about the data that Zoom can collect from you and store:

If you provide data such as your name, your user name, your e-mail address or your telephone number, this data will be stored by Zoom. Content that you upload while using Zoom is also stored. This includes, for example, files or chat logs.

The technical data that Zoom automatically saves includes, in addition to the IP address already mentioned above, the MAC address, other device IDs, device type, which operating system you are using, which client you are using, camera type, microphone type and speaker type. Your approximate location is also determined and stored. Zoom also stores information about how you use the service. For example, whether you are "zooming" via desktop or smartphone, whether you are using a phone call or VoIP, whether you are participating with or without video, or whether you are requesting a password. Zoom also records so-called metadata such as the duration of the meeting/call, start and end of meeting participation, meeting name and chat status.

Zoom mentions in its own privacy policy that it does not use advertising cookies or tracking technologies for its services. Only on its own marketing websites, such as <https://explore.zoom.us/docs/de-de/home.html>, are these tracking methods used. Zoom does not resell personal data or use it for advertising purposes.

How long and where is the data stored?

Zoom does not disclose a specific time frame in this regard, but emphasises that the collected data will be stored for as long as it is necessary to provide the services or for its own purposes. The data is only stored longer if this is required for legal reasons.

In principle, Zoom stores the data it collects on American servers, but data can arrive at different data centres around the world.

How can I delete my data or prevent data storage?

If you do not want data to be stored during the Zoom meeting, you must refrain from attending the meeting. However, you always have the right and the possibility to have all your personal data deleted. If you have a Zoom account, you can find instructions on how to delete your account at <https://support.zoom.us/hc/en-us/articles/201363243-How-Do-I-Delete-Terminate-My-Account>.

Please note that when using this tool, data from you 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 may therefore not simply be transferred, 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 given your consent for your data to be processed and stored by the video or streaming solution, this consent is the legal basis for the data processing (**Art. 6 para. 1 lit. a DSGVO**). In addition, we may also offer a video conference as part of our services if this has been contractually agreed with you in advance (**Art. 6 para. 1 lit. b DSGVO**). In principle, your data will also be stored and processed on the basis of our legitimate interest (**Art. 6 para. 1 lit. f DSGVO**) in fast and good communication with you or other customers and business partners, but only if you have at least consented to this.

Zoom also processes data from you in the USA, among other places. We would like to point out that according to the opinion of the European Court of Justice, there is currently no adequate level of protection for the transfer of data to the USA. This may be associated with various risks for the legality and security of the data processing.

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

We hope we have provided you with an overview of Zoom's data processing. Of course, it is always possible that the company's privacy policy may change. Therefore, for more information on the data processed and the standard contractual clauses, we also recommend that you consult Zoom's privacy policy at <https://explore.zoom.us/de/privacy/>.

Order processing contract (AVV) Zoom

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have concluded a Data Processing Agreement (DPA) with Zoom. You can find out exactly what a GCU is and, in particular, what must be included in a GCU, in our general section "Order Processing Agreement (AVV)".

This contract is required by law because Zoom processes personal data on our behalf. It clarifies that Zoom 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 order processing agreement (AVV) at https://explore.zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf.

Recruiting Tools Introduction

Recruiting Tools Privacy Policy Summary

Affected persons: Users who carry out an application procedure online or use a recruiting tool.

Purpose: Handling of an application procedure

Processed data: Data such as name, address, contact details, email address or your telephone number. You can find more details on this in the respective recruiting tool used.

Storage period: if the application is successful, until the end of the employment relationship.

Otherwise, the data will be deleted after the application procedure.

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

What are recruiting tools?

Various companies offer software programmes that can make the application process much easier. Most systems offer filter options to search through databases of potential candidates. This allows us to quickly and efficiently find employees who fit our company. Both online forms and recruiting tools transmit, store and manage your personal data. In this general text, we refer not only to recruiting tools but also to the classic application procedure by e-mail or online form. More detailed information on the recruiting tools can be found in the data protection statements of the respective providers.

Why do we use recruiting tools?

For the search for suitable applicants and for the administration of all application documents, we use software programmes and platforms that specialise in application management, taking into account all legal guidelines. So-called recruiting tools generally facilitate the application process by taking over many administrative tasks and optimising 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 procedures, we refer in detail to the respective job advertisements.

What data is processed?

When you apply to us, you must of course also provide us with data about yourself so that we can also assess the application accordingly. The exact information you provide depends on the job advertisement or the information required in the online form.

This usually involves data such as name, address, date of birth and proof of your qualifications required for the job. During the process of an application

but not only the usual personal data, such as name or address, but also information about your health or ethnic origin may be requested so that we and you can exercise the rights relating to labour law, social security and social protection and at the same time comply with the corresponding obligations. These data are called special category data.

The data of your application will be sent to us in encrypted form via the online form. Alternatively, you can also send us your application by e-mail. If you choose this option, the data will be transmitted in encrypted form, but will not be stored in encrypted form by the server that sends and receives it.

Duration of data processing

In the event of a successful application, we may process the data you have provided for the purpose of employment. If the application does not meet the expectations, we delete the data received. This data will also be deleted if you withdraw your application. If you agree to be included in our applicant pool, we will store your data collected in this context until you leave the applicant pool. The same rules apply to the withdrawal as to the revocation of your consent.

Right of objection

You also always have the right and the possibility to revoke your consent. So that we can still answer possible questions about the application and fulfil our obligations to provide proof, the data will be deleted after 6 months at the latest. We archive invoices for possible travel expense reimbursements 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 DSGVO). We would like to point out that your consent to our application pool is voluntary, has no influence on the application process and you have the option to revoke your consent at any time.

In the case of the protection of vital interests, data processing is carried out in accordance with Art. 9 para. 2 lit. c. DSGVO. For the purposes of health care, occupational medicine, medical diagnosis, health or social care or treatment, or the management of health or social care systems and services, the processing of personal data is carried out in accordance with Art. 9 (2) (h) of the GDPR.

DSGVO. If you voluntarily provide special category data, the processing is based on Art. 9 para. 2 lit. a. DSGVO.

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

LinkedIn Recruiter Privacy Policy

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

LinkedIn also processes data from you in the USA, among other places. We would like to point out that according to the opinion of the European Court of Justice, there is currently no adequate level of protection for the transfer of data to the USA. This may be associated with various risks for the legality and security of the data processing.

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

More information on the standard contractual clauses at LinkedIn can be found at <https://www.linkedin.com/help/linkedin/answer/62538/datenubertagung-aus-der-eu-dem-ewr-and-switzerland?lang=en>.

You can find out more about the data processed through the use of LinkedIn Recruiter in the privacy policy at <https://de.linkedin.com/legal/privacy-policy>.

Order processing agreement (AVV) LinkedIn Recruiter

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have concluded a Data Processing Agreement (DPA) with LinkedIn. You can find out exactly what a GCU is and, above all, what must be included in a GCU in our general section "Order processing agreement (GCU)".

This contract is required by law because LinkedIn processes personal data on our behalf. It clarifies that LinkedIn may only process data they receive from us according to our instructions and must comply with the GDPR. You can find the link to the order processing agreement (AVV) at <https://de.linkedin.com/legal/l/dpa>.

Monster Privacy Policy

We use the recruiting tool Monster. The service provider is the Austrian company Monster Worldwide Austria GmbH, Neubaugasse 43/1/1-2, 1070 Vienna, Austria. You can find out more about the data processed through the use of Monster in the privacy policy at <https://www.monster.at/datenschutz/kurzversion/inside2.aspx>.

Stepstone Privacy Policy

We use StepStone, an applicant management software. The service provider is the Austrian company StepStone Österreich GmbH, Prinz-Eugen-Straße 8-10, A-1040 Vienna, Austria. You can find out more about the data processed through the use of StepStone in the data protection [declaration](https://www.stepstone.at/Ueber-StepStone/legal-notice/data-protection-declaration/) at <https://www.stepstone.at/Ueber-StepStone/legal-notice/data-protection-declaration/>.

Single sign-on logins Introduction

Single sign-on logins Privacy policy summary

¶ Data subjects: Visitors to the website

Purpose: Simplification of the authentication process

¶ Processed data: Depends strongly on the respective provider, usually e-mail address and user name can be stored.

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

¶ Storage duration: depending on the tools used

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

What are single sign-on logins?

On our website, you have the option of quickly and easily registering for our online service via a user account from another provider (e.g. via Facebook). This authentication procedure is called "single sign-on registration", among other things. Of course, this registration procedure only works if you are registered with the other provider or have a user account and enter the corresponding access data in the online form. In many cases you are already registered, the access data is automatically entered into the form and you only have to confirm the single sign-on registration via a button. In the course of this registration, your personal data may also be processed and stored. In this data protection text, we deal in general with data processing through single sign-on logins. You can find more detailed information in the data protection declarations of the respective providers.

Why do we use single sign-on logins?

We want to make your life on our website as easy and pleasant as possible. That's why we also offer single sign-on logins. This saves you valuable time because you only need one authentication. As you only need to remember one password and it is only transmitted once, security is also increased. In many cases, you have also already saved your password automatically with the help of cookies and the login process on our website therefore only takes a few seconds.

What data is stored through single sign-on logins?

Although you log in to our website via this special login procedure, the actual authentication takes place with the corresponding single sign-on provider. As the website operator, we receive a user ID in the course of the authentication. This records that you are registered with the corresponding provider under this ID. This ID cannot be used for any other purpose. Other data may also be transmitted to us, but this depends on the single sign-on provider used. It also depends on what data you voluntarily provide during the authentication process and what data you generally release in your settings with the provider. In most cases, this is data such as your email address and your user name. We do not know your password, which is required for registration, and it is not stored by us. It is also important for you to know that data stored with us can be automatically compared with the data of the respective user account through the registration process.

Duration of data processing

We will inform you about the duration of data processing below, provided we have further information on this. For example, the social media platform Facebook stores data until it is no longer needed for its own purpose. However, customer data that is matched with our own user data is deleted within two days. In general, we only process personal data for as long as is absolutely necessary for the provision of our services and products.

Right of objection

You also have the right and the possibility to revoke your consent to the use of single sign-on logins at any time. This usually works via opt-out functions of the provider. If available, you will also find links to the corresponding opt-out functions in our data protection texts for the individual tools.

Legal basis

If it has been agreed with you and this is done in the context of contract performance (Article 6(1)(b) DSGVO) and consent (Article 6(1)(a) DSGVO), we may use the single sign-on procedure on their legal bases.

In addition to consent, there is a legitimate interest on our part in providing you with a quick and easy registration process. The legal basis for this is Art. 6 para. 1 lit. f DSGVO (legitimate interests). Nevertheless, we only use the single sign-on registration if you have given your consent.

If you no longer wish to have this link to the provider with the single sign-on login, please delete it in your user account with the respective provider. If you also want to delete data from us, it is necessary to cancel your registration.

Survey and polling systems Introduction

Survey and polling systems Privacy policy summary

👤 Persons concerned: Visitors to the website

Purpose: evaluation of surveys on the website

Processed data: Contact data, device data, access duration and time, IP addresses. More details can be found in the respective survey and questionnaire system used.

📅 Storage duration: depending on the tool used

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What are survey and polling systems?

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

Why do we use survey and polling systems?

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

Furthermore, the information also helps us to target our advertising and marketing measures more specifically at those people who are really interested in our offer.

What data is processed?

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

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

How long is data stored?

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

Right of objection

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

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

Legal basis

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

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

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

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

Assessment platforms Introduction

Assessment platforms Summary

✓Data subjects: visitors to the website or a rating platform

Purpose: Feedback on our products and/or services

Processed data: Among other things, IP address, email address, name. More details can be found below or on the respective rating platforms used.

Storage period: depends on the respective platform.

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

What are rating platforms?

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

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

Why do we use rating platforms?

Rating platforms collect feedback and reviews about our offerings. Through your ratings, we quickly receive appropriate feedback and can improve our products and/or services much more efficiently. Consequently, the ratings serve us on the one hand to optimise our offers and on the other hand they give you and all our future customers a good overview of the quality of our products and services.

What data is processed?

With your consent, we transmit information about you and the services you have used to the corresponding rating platform. We do this to ensure that you have actually used one of our services. Only then can you provide real feedback. The transmitted data only serves to identify the user. Exactly what data is stored and processed depends, of course, on the providers used. In most cases, the rating platforms are also provided with personal data such as IP address, email address or your name. Order information such as the order number of a purchased item is also forwarded to the corresponding platform after you have submitted your rating. If your email address is transmitted, this is done so that the rating platform can send you an email after the purchase of an item.

product can send. So that we can also include your rating on our website, we also give the providers the information that you have accessed our page.
The rating platform used is responsible for the personal data collected.

How long and where is the data stored?

You can find out more about the duration of data processing below in the relevant privacy policy of the provider, 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.

Personal data mentioned in an assessment is usually anonymised by employees of the platform used and is thus only visible to administrators of the company. The collected data is stored on the servers of the providers and, in the case of most providers, deleted after the end of the order.

Right of objection

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, deactivating or deleting cookies in your browser.

Legal basis

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

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

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

Web design introduction

Web Design Privacy Policy Summary

Persons concerned: Visitors to the website

Purpose: to improve the user experience

] Processed data: Which data is processed depends strongly on the

services used. In most cases, this includes the IP address, technical data, language settings, browser version, screen resolution and browser name. You can find more details about this in the respective web design tools used.

Storage duration: depending on the tools used

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What is web design?

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

Why do we use web design tools?

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

What data is stored by web design tools?

When you visit our website, web design elements may be embedded in our pages that can also process data. Exactly what data is involved depends, of course, heavily on the tools used. Below you can see exactly which tools we use for our website. We recommend that you also read the respective data protection statement of the tools used for more detailed information on data processing. In most cases, you will find out there which data is processed, whether cookies are used and how long the data is stored. Fonts such as Google Fonts, for example, also automatically transmit information such as language settings, IP address, browser version, browser screen resolution and browser name to the Google servers.

Duration of data processing

How long data is processed is very individual and depends on the web design elements used. For example, if cookies are used, the retention period can be as short as a minute or as long as a few years. Please find out more about this. For this purpose, we recommend on the one hand our general text section on cookies and on the other hand the data protection declarations of the tools used. There you will usually find out exactly which cookies are used and what information is stored in them. Google font files, for example, are stored for one year. This is to improve the loading time of a website. In principle, data is only stored for as long as is necessary for the provision of the service. In the case of legal requirements, data can also be stored for longer.

Right of objection

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. You can also prevent data collection through cookies by managing, deactivating or deleting cookies in your browser. Under web design elements (mostly fonts), however, there is also data that cannot be deleted quite so easily. This is the case if data is automatically collected directly when a page is called up and transmitted to a third-party provider (such as Google). In this case, please contact the support of the relevant provider. In the case of Google, you can reach the support at <https://support.google.com/?hl=de>.

Legal basis

If you have consented to web design tools being used, the legal basis for the corresponding data processing is this consent. According to Art. 6 para. 1 lit. a DSGVO (consent), this consent is the legal basis for the processing of personal data as may occur when collected by web design tools. From our side, there is also a legitimate interest in improving the web design on our website. After all, only then can we provide you with a beautiful and professional web offer. The corresponding legal basis for this is Art. 6 para. 1 lit. f DSGVO (Legitimate Interests). Nevertheless, we only use web design tools if you have given your consent. We would like to emphasise this again here in any case.

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

Online map services Introduction

Online Map Services Privacy Policy Summary

Parties concerned: Visitors to the website

Purpose: to improve the user experience

Processed data: Which data is processed depends strongly on the

services used. This usually involves IP address, location data, search items and/or technical data. You can find more details about this in the respective tools used.

Storage duration: depending on the tools used

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What are online map services?

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

Why do we use online map services on our website?

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

Therefore, we thought an online map system could still be a significant optimisation of our service on the website. Without leaving our website, you can easily view route descriptions, locations or even points of interest with the help of the map system. Of course, it is also super practical that you can see at a glance where we are located so that you can find us quickly and safely. As you can see, there are simply many advantages and we clearly consider online map services on our website as part of our customer service.

What data are stored by online map services?

When you open a page on our website that has an online map function built in, personal data may be transmitted to the respective service and stored there. In most cases, this is your IP address, which can also be used to determine your approximate position. In addition to the IP address, data such as search terms entered and latitude and longitude coordinates are also stored. If you enter an address for route planning, for example, this data is also stored. The data is not stored by us, but on the servers of the integrated tools.

You can think of it something like this: You are on our website, but when you interact with a map service, that interaction actually happens on their website. In order for the service to function properly, at least one cookie is usually set in your browser. Google Maps, for example, also uses cookies to record user behaviour in order to optimise its own service and offer personalised maps.

to be able to place advertisements. You can find out more about cookies in our section "Cookies."

How long and where is the data stored?

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

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

Right of objection

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

Legal basis

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

We also have a legitimate interest in using an online map service to optimise our service on our website. The corresponding legal basis for this is Art. 6 para. 1 lit. f DSGVO (Legitimate Interests). However, we only ever use an online map service if you have given your consent. We definitely want to have this stated again at this point.

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

Google Maps Privacy Policy

Google Maps Privacy Policy Summary

✓ Parties concerned: Visitors to the website

Purpose: optimisation of our service performance

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

More details can be found below in this privacy policy.

Storage duration: depending on the stored data

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What is Google Maps?

We use Google Maps from Google Inc. on our website. Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services in Europe. Google Maps enables us to better show you locations and thus adapt our service to your needs. By using Google Maps, data is transmitted to Google and stored on Google servers. Here we would like to go into more detail about 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 mapping service provided by Google. With Google Maps you can search for exact locations of cities, sights, accommodation or businesses online via a PC, tablet or app. If companies are represented on Google My Business, further information about the company is displayed in addition to the location. To show how to get there, map sections of a location can be integrated into a website using HTML code. Google Maps shows the earth's surface as a street map or as an aerial or satellite image. Thanks to the Street View images and the high-quality satellite images, very accurate representations are possible.

Why do we use Google Maps on our website?

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

What data is stored by Google Maps?

In order for Google Maps to be able to offer its service in full, the company must collect and store data from you. This includes the search terms entered, your IP address and also the latitude and longitude coordinates. If you use the route planner function, the starting address you entered is also stored. This

However, data storage happens on the websites of Google Maps. We can only inform you about this, but cannot influence it. Since we have integrated Google Maps into our website, Google sets at least one cookie (name: NID) in your browser. This cookie stores data about your user behaviour. Google uses this data primarily to optimise its own services and to provide you with individual, personalised advertising.

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

Name: NID

Value: 188=h26c1Ktha7fCQTx8rXgLyATyITJ312569961-5

Purpose: NID is used by Google to tailor ads to your Google search. With the help of the cookie, Google "remembers" your most frequently entered search queries or your previous interaction with ads. This means you will always receive tailored ads. The cookie contains a unique ID that Google uses to collect your personal preferences for advertising purposes.

Expiry date: after 6 months

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

How long and where is the data stored?

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

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

Google distributes the data on different data carriers. This means that the data can be retrieved more quickly and is better protected against any attempts at manipulation. Each data centre also has special emergency programmes. If, for example, there are problems with Google's hardware or a natural disaster brings the servers to a standstill, the data will pretty much remain protected anyway.

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

How can I delete my data or prevent data storage?

With the automatic deletion of location and activity data introduced in 2019, location and web/app activity information will be stored for either 3 or 18 months - depending on your decision - and then deleted. In addition, you can also manually delete this data from your history at any time via your Google Account. If you want to completely prevent your location tracking, you must pause the "Web and App Activity" section in the Google Account. Click "Data and personalisation" and then on the "Activity setting" option. Here you can switch the activities on or off.

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

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

Legal basis

If you have consented to Google Maps being used, the legal basis for the corresponding data processing is this consent. According to **Art. 6 para. 1 lit. a DSGVO (consent)**, this **consent** constitutes the legal basis for the processing of personal data as may occur during the collection 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 DSGVO (legitimate interests)**. Nevertheless, we only use Google Maps if you have given your consent.

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

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

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

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

Content Search Provider Introduction

Content Search Provider Privacy Policy Summary

✓ Parties concerned: Visitors to the website

Purpose: to improve the user experience

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

Storage duration: depending on the tools used

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What is a content search provider?

In the meantime, we have published a lot of content on our website. And of course we don't want it to be forgotten just because it can't be found. That's why we use a content search provider on our website. You are probably familiar with major search engines like Google. Content search providers are basically also search engines, but unlike Google, they do not search the entire web for content, but only the website you are on. You can enter terms that match the content you are looking for in a text field and the search programme will find the desired articles for you. If you use the integrated search function, your personal data may also be processed.

Why do we use a content search provider?

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

What data is processed?

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

You can find out which cookies the individual search tools use - if available - below or in the corresponding privacy statements of the integrated tools.

How long and where is the data stored?

As a general rule, each content search provider processes different data. Therefore, this general section cannot specifically address the data processing of the individual tools. Usually, however, the services only store personal data as long as this is necessary for the smooth functioning of the tools. Some services (such as Giphy) also retain personal data for longer if required by legal obligations. In depersonalised form, data is also kept longer by most providers. Content search providers may also use cookies to store various data. You can read more about this in our general section on cookies. If you want to know about the specific cookies that a search provider uses, we recommend that you read the privacy policy of the providers we use. In most cases, you will find an exemplary list of the cookies used there.

Right of objection

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

Legal basis

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

We also have a legitimate interest in using a content search provider to optimise our service on our website. The corresponding legal basis for this is Art. 6 para. 1 lit. f DSGVO (Legitimate Interests). However, we only ever use a content search provider if you have given your consent. We definitely want to have this stated again at this point.

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

Online booking systems Introduction

Online Booking Systems Privacy Policy Summary

Data subjects: Visitors to the website

Purpose: Improve user experience and organisation

Processed data: Which data is processed depends largely on the services used. In most cases, it is an IP address, contact and payment data and/or technical data. You can find more details about this in the respective tools used.

Storage duration: depending on the tools used

Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What is an online booking system?

To enable you to make bookings via our website, we use one or more booking systems. Appointments, for example, can be easily created online. A booking system is a software application integrated into our website that displays available resources (such as free appointments) and through which you can book directly online and usually also pay. You are probably already familiar with such booking systems from the catering or hotel industry. In the meantime, however, such systems are used in a wide variety of sectors. Depending on the tool and settings, booking systems can be used both internally for us and for clients like you. As a rule, your personal data is also collected and stored in the process.

In most cases, the booking works as follows: You will find the booking system on our website, where you can book an appointment for a service directly with a click of the mouse and enter your details, and usually pay for it straight away. You may be able to enter various details about yourself via a form. Please be aware that all the data you enter may be stored and managed in a database.

Why do we use an online booking system?

In a way, we also see our website as a free service for you. We want you to receive helpful information and feel comfortable on our site. This also includes an online service that makes booking appointments or services as easy as possible for you. Gone are the days when you had to wait days for a booking confirmation by phone or e-mail. With an online booking system, everything is done in just a few clicks and you can get on with other things. The system also makes it easier for us to manage all bookings and appointments. Therefore, we consider such a booking system to be absolutely useful for you as well as for us.

What data is processed?

Of course, we cannot tell you in this general information text about booking systems exactly what data is processed. This always depends on the tool used and the functions and possibilities it contains. In addition to the conventional booking function, many booking systems also offer a number of other functions.

of additional features. For example, many systems also have an external online payment system (e.g. from Stripe, Klarna or Paypal) and a calendar synchronisation function integrated. Accordingly, depending on the functions, different and varying amounts of data can be processed. Usually, data such as IP address, name and contact details, technical information about your device and the time of a booking are processed. If you also make a payment in the system, bank data such as account number, credit card number, passwords, TANs, etc. are also stored and passed on to the respective payment provider. We recommend that you read the respective privacy policy of the tool used carefully so that you know which of your data is specifically processed.

Duration of data processing

Each booking system stores data for different lengths of time. Therefore, we cannot yet give any concrete information about the duration of data processing. In principle, however, personal data is only stored for as long as is absolutely necessary to provide the services. Booking systems usually also use cookies, which store information for different lengths of time. Some cookies are deleted immediately after you leave the site, others can be stored for several years. You can find out more about this in our "Cookies" section. Please also take a look at the respective data protection declarations of the providers. These should explain how long your data will be stored in the specific case.

Right of objection

If you have consented to data processing by a booking system, you always have the possibility and the right to revoke this consent. Please be aware that you have rights with regard to your personal data and that you can exercise these rights at any time. If you do not want personal data to be processed, then no personal data may be processed. It's as simple as that. The easiest way to revoke data processing is to use a cookie consent tool or other opt-out functions offered. You can also manage the data storage by cookies directly in your browser, for example. Until your revocation, the lawfulness of the data management remains unaffected.

Legal basis

If you have consented to the use of booking systems, the legal basis for the corresponding data processing is this consent. According to Art. 6 para. 1 lit. a DSGVO (consent), it constitutes the legal basis for the processing of personal data as it may occur through booking systems.

Furthermore, we also have a legitimate interest in using booking systems because, on the one hand, this enables us to expand our customer service and, on the other hand, optimise our internal booking organisation. The corresponding legal basis for this is Art. 6 para. 1 lit. f DSGVO (legitimate interests). Nevertheless, we only use the tools if you have given your consent. We would like to make this clear once again at this point.

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

Miscellaneous Introduction

Miscellaneous Privacy Policy Summary

📄 Data subjects: Visitors to the website

Purpose: to improve the user experience

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

📄 Storage duration: depending on the tools used

📄 Legal basis: Art. 6 para. 1 lit. a DSGVO (Consent), Art. 6 para. 1 lit. f DSGVO (Legitimate Interests)

What falls under "Other"?

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

Why do we use other third party providers?

With our website, we want to offer you the best web offer in our industry. For a long time now, a website has been more than just a business card for companies. Rather, it is a place to help you find what you are looking for. To make our website even more interesting and helpful for you, we use various third-party services.

What data is processed?

Whenever elements are integrated into our website, your IP address is transmitted to the respective provider, stored and processed there. This is necessary because otherwise the content will not be sent to your browser and consequently will not be displayed accordingly. It may also happen that service providers also use pixel tags or

Use web beacons. These are small graphics on websites that record a log file and can also generate analyses of this file. With the information obtained, providers can improve their own marketing measures. In addition to pixel tags, such information (such as which button you click or when you call up which page) can also be stored in cookies. In addition to analysis data on your web behaviour, technical information such as your browser type or operating system can also be stored in them. Some providers may also link the data obtained with other internal services or with third-party providers. Each provider handles your data differently. We therefore recommend that you carefully read the privacy statements of the respective services. We

are generally endeavouring to use only services that handle the issue of data protection very carefully.

Duration of data processing

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

Legal basis

If we ask you for your consent and you also consent to us using the service, this is considered the legal basis for the processing of your data (Art. 6 para. 1 lit. a DSGVO). In addition to the consent, there is a legitimate interest on our part in analysing the behaviour of website visitors and thus improving our offer technically and economically. The legal basis for this is Art. 6 para. 1 lit. f DSGVO (legitimate interests). Nevertheless, we only use the tools if you have given your consent.

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

Explanation of terms used

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

Supervisory authority

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

***"supervisory authority"** means an independent public body established by a Member State in accordance with Article 51;*

Explanation: "Supervisory authorities" are always governmental, independent institutions which are also authorised to issue instructions in certain cases. They serve to carry out so-called state supervision and are located in ministries, special departments or other authorities. For data protection in Austria there is an Austrian data protection [authority](#), for Germany there is a separate data protection authority for each federal state.

Processor

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

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

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

Supervisory authority concerned

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"supervisory authority concerned" means a supervisory authority which is concerned by the processing of personal data because

a)

the controller or processor is established in the territory of the Member State of that supervisory authority,

b)

that processing has or is likely to have a significant impact on data subjects residing in the Member State of that supervisory authority; or

c)

a complaint has been filed with this supervisory authority;

Explanation: In Germany, each federal state has its own supervisory authority for data protection. So if your company headquarters (main office) is in Germany, the respective supervisory authority of the federal state is generally your contact. In Austria, there is only one supervisory authority for [data protection](#) for the entire country.

Biometric data

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"biometric data" means personal data, obtained by means of specific technical procedures, relating to the physical, physiological or behavioural characteristics of a natural person, which enable or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

Explanation: These are biological characteristics that are described by biometric data and from which personal data can be obtained with the help of technical procedures. These include DNA, fingerprints, the geometry of various body parts, body size, but also handwriting or the sound of a voice.

File system

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"file system" means any structured collection of personal data accessible according to specified criteria, whether such collection is maintained in a centralised, decentralised or functional or geographical manner;

Explanation: Any organised storage of data on a data carrier of a computer is called a "file system". For example, if we store your name and email address on a server for our newsletter, then this data is located in a so-called "file system". The most important tasks of a "file system" include the fast searching and finding of specific data and, of course, the secure storage of the data.

Information Society Service

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"information society service" means a service as defined in Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council (19);

Explanation: Basically, the term "information society" refers to a society based on information and communication technologies. Especially as a website visitor, you are familiar with all kinds of online services and most online services belong to "information society services". A classic example is an online transaction, such as buying goods over the internet.

Third

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"third party" means any natural or legal person, public authority, agency or other body other than the data subject, the controller, the processor and the persons authorised to process the personal data under the direct responsibility of the controller or the processor;

Explanation: The GDPR basically only explains here what a "third party" is not. In practice, a "third party" is anyone who also has an interest in the personal data but is not one of the persons, authorities or entities mentioned above. For example, a parent company may act as a "third party". In this case, the subsidiary group is the controller and the parent group is the "third party". However, this does not mean that the parent company is automatically allowed to view, collect or store the personal data of the subsidiary company.

Restriction of processing

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"restriction of processing" means the marking of stored personal data with the aim of limiting their future processing;

Explanation: One of your rights is that you can ask processors to restrict your personal data for further processing at any time. This is done by marking specific personal data, such as your name, date of birth or address, so that it can no longer be processed in full. For example, you could restrict the processing so that your data can no longer be used for personalised advertising.

Consent

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"consent" means any freely given specific, informed and unambiguous indication of the data subject's wishes, in the form of a statement or other unambiguous affirmative act, by which the data subject signifies his or her agreement to personal data relating to him or her being processed;

Explanation: As a rule, such consent is given on websites via a cookie consent tool. You are probably familiar with this. Whenever you visit a website for the first time, you are usually asked via a banner whether you agree or consent to data processing. In most cases, you can also make individual settings and thus decide for yourself which data processing you allow and which you do not. If you do not consent, no personal data of yours may be processed.

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

Receiver

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

***"recipient" means** a natural or legal person, public authority, agency or other body to whom personal data are disclosed, whether or not a third party. However, public authorities that may receive personal data in the context of a specific investigative task under Union or Member State law shall not be considered as recipients and the processing of such data by those authorities shall be carried out in accordance with the applicable data protection rules, in accordance with the purposes of the processing;*

Explanation: Every person and every company that receives personal data is considered a recipient. Thus, we and our processors are also so-called recipients. Only authorities that have a mandate to investigate are not considered recipients.

Genetic data

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

***'genetic data' means** personal data relating to the inherited or acquired genetic characteristics of a natural person which provide unique information about the physiology or health of that natural person and which have been obtained, in particular, from the analysis of a biological sample from the natural person concerned;*

Explanation: With a certain amount of effort, people can be identified via genetic data. That is why genetic data also belong to the category of personal data. Genetic data are obtained, for example, via blood or saliva samples.

Health data

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

***"health data" means** personal data relating to the physical or mental health of a natural person, including the provision of health services, revealing information about that person's state of health;*

Explanation: Health data therefore includes all stored information concerning your own health. It is often data that is also recorded in a patient file. This includes, for example, which medicines you use, X-ray images, the entire medical history or, as a rule, the vaccination status.

Cross-border processing

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"cross-border processing" either a)

a processing of personal data carried out in the context of the activities of establishments of a controller or a processor in the Union in more than one Member State, where the controller or processor is established in more than one Member State, or

b)

a processing of personal data which is carried out in the course of the activities of a single establishment of a controller or processor in the Union but which has or is likely to have a significant impact on data subjects in more than one Member State;

Explanation: If, for example, a company or other organisation has branches in Spain and in Croatia and personal data are processed in connection with the activities of the branches, this is "cross-border processing" of personal data. Even if the data is only processed in one country (as in this example in Spain), but the effects for the data subject are also apparent in another country, this is also referred to as "cross-border processing".

Head office

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"Headquarters"

a)

in the case of a controller with establishments in more than one Member State, the place of its main administration in the Union, unless the decisions regarding the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and that establishment has the power to have those decisions implemented, in which case the establishment taking such decisions shall be considered to be the main establishment;

b)

in the case of a processor with establishments in more than one Member State, the place of its head office in the Union or, where the processor does not have a head office in the Union, the establishment of the processor in the Union where the processing activities in the context of the activities of an establishment of a processor mainly take place, to the extent that the processor is subject to specific obligations under this Regulation;

Explanation: Google, for example, is an American company that also processes data in the USA, but its European headquarters are in Ireland (Google Ireland Limited, Gordon House, Barrow Street Dublin 4, Ireland). Thus, Google Ireland Limited is legally a separate company and responsible for all Google products offered in the European Economic Area. In contrast to a main branch office, there are also branch offices, but these do not function as legally independent branches and are therefore also to be distinguished from subsidiaries. A principal place of business is therefore always the place where a company (trading company) has its centre of operations.

International organisation

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"international organisation" means an organisation governed by international law and its subsidiary bodies or any other body established by or pursuant to an agreement concluded between two or more countries.

Explanation: The best-known examples of international organisations are probably the European Union or the United Nations. In the GDPR, a distinction is made between third countries and international organisations in connection with the transfer of data. Within the EU, the transfer of personal data is not a problem because all EU countries are bound by the provisions of the GDPR. However, the transfer of data with third countries or international organisations is subject to certain conditions.

Relevant and reasoned objection

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"(c) 'relevant and reasoned objection' means an objection to a draft decision as to whether there is a breach of this Regulation or whether intended measures against the controller or processor are in compliance with this Regulation, clearly indicating the scope of the risks posed by the draft decision in relation to the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

Explanation: If certain measures taken by us as data controllers or by our processors are not in compliance with the GDPR, you can raise a so-called "relevant and reasoned objection". You must explain the extent of the risks to your fundamental rights and freedoms and possibly to the free flow of your personal data in the EU.

Personal data

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

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

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

- Name
- Address
- E-mail address
- Postal address
- Telephone number
- Date of birth
- Identification numbers such as national insurance number, tax identification number, identity card number or matriculation number
- Bank data such as account number, credit information, account balances, etc.

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

- racial and ethnic origin
- political opinions
- Religious or ideological convictions
- the trade union affiliation
- Genetic data such as data taken from blood or saliva samples
- biometric data (this is information on mental, physical or behavioural characteristics that can identify a person). Health data
- Data on sexual orientation or sexual life

Profiling

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"profiling" means any automated processing of personal data which consists in using such personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects relating to that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or change of location;

Explanation: Profiling involves gathering various pieces of information about a person in order to learn more about that person. In the web sector, profiling is often used for advertising purposes or also for credit checks. Web or advertising analysis programmes, for example, collect data about your behaviour and interests on a website. This results in a special user profile that can be used to target advertising to a specific group.

Pseudonymisation

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"pseudonymisation" means the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures which ensure that the personal data are not attributed to an identified or identifiable natural person;

Explanation: Our data protection statement often refers to pseudonymised data. Pseudonymised data means that you can no longer be identified as a person unless other information is added. However, you should not confuse pseudonymisation with anonymisation. Anonymisation removes any reference to a person, so that this can really only be reconstructed with a disproportionately large technical effort.

Company

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"undertaking" means a natural and legal person engaged in an economic activity, regardless of its legal form, including partnerships or associations regularly engaged in an economic activity;

Explanation: For example, we are a company and also carry out an economic activity via our website by offering and selling services and/or products. For every company, there is the formal characteristic of a legal entity, such as a GmbH (limited liability company) or AG (public limited company).

Group of companies

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"group of undertakings" means a group consisting of a controlling undertaking and the undertakings dependent on that controlling undertaking;

Explanation: One thus speaks of a "group of companies" when several companies unite and are legally and financially connected to each other, but there is nevertheless a central, overarching company. For example, Instagram, WhatsApp, Oculus VR or Facebook are largely independent companies, but they are all subject to the parent company Meta Platforms, Inc.

Responsible

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

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

Explanation: In our case, we are responsible for the processing of your personal data and consequently the "controller". If we pass on collected data to other service providers for processing, they are "processors". This requires the signing of a "Contractual Processing Agreement (CPA)".

Processing

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

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

Note: When we talk about processing in our privacy statement, we mean any kind of data processing. This includes, as mentioned above in the original GDPR declaration, not only the collection but also the storage and processing of data.

Binding internal data protection regulations

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

***"binding internal data protection rules" means** measures for the protection of personal data with which a controller or processor established in the territory of a Member State undertakes to comply in respect of data transfers or a set of data transfers of personal data to a controller or processor of the same group of undertakings or the same group of undertakings engaged in a joint economic activity in one or more third countries;*

Explanation: You may have heard or read the term "Binding Corporate Rules" more than once. Because this is the term that mostly appears when it comes to binding internal data protection rules. Especially for companies (such as Google) that process data in third countries, it is advisable to have such an internal regulation, by which a company commits itself, so to speak, to comply with data protection regulations. This regulation governs the handling of personal data that is transferred to and processed in third countries.

Violation of the protection of personal data

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

***"personal data breach" means** a breach of security leading, whether accidentally or unlawfully, to the destruction, loss, alteration of, or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;*

Explanation: For example, a "personal data breach" can occur in the event of a data leak, i.e. a technical problem or a cyber attack.

If the breach leads to a risk to the rights and freedoms of natural persons, the controller must immediately report the incident to the competent supervisory authority.

In addition, data subjects must also be informed if the breach poses a high risk to the rights and freedoms of natural persons.

Representative

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term:

"(c) 'representative' means a natural or legal person established in the Union appointed in writing by the controller or processor in accordance with Article 27 to represent the controller or processor in relation to their respective obligations under this Regulation;

Explanation: A "representative" can therefore be any person appointed in writing by us (controller) or one of our service providers (processor). Companies outside the EU that process data of EU citizens must specify a representative within the EU. For example, if a web analytics provider has its main office in the US, it must appoint a "representative" within the European Union to represent the data processing obligations.

Closing words

Congratulations! If you are reading these lines, you have really "fought" your way through our entire data protection statement, or at least scrolled this far. As you can see from the scope of our privacy policy, we take the protection of your personal data anything but lightly. It is important to us to inform you to the best of our knowledge and belief about the processing of personal data. However, we do not only want to tell you what data is processed, but also explain the reasons for using various software programmes. As a rule, data protection statements sound very technical and legalistic. However, since most of you are not web developers or lawyers, we also wanted to take a different linguistic approach and explain the facts in simple and clear language. Of course, this is not always possible due to the subject matter. Therefore, the most important terms are explained in more detail at the end of the privacy policy.

If you have any questions about data protection on our website, please do not hesitate to contact us or the responsible office. We wish you a good time and hope to see you on our website again soon.

All texts are protected by copyright.

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