

Legal Notice

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

NESTEC Scharf IT-Solutions OG
Pummerinplatz 5,
4490 St. Florian,
Österreich

Object of the company: IT Dienstleistungen

VAT-Number: ATU56088708

GLN: 9110016442839

GISA: 16348257

Corporate register number: Fn 224911b

Corporate register court: Landesgericht Steyr

Company location: A-4490 St. Florian

Phone: +43 (7223) 80703

Email: office@nestec.at

Member of: WKO

Laws re. professions: Gewerbeordnung: www.ris.bka.gv.at

Supervisory/Trade authority: Bezirkshauptmannschaft Linz-Land

Job title: Dienstleistung in der automatischen Datenverarbeitung und Informationstechnik

Awarding country: Österreich

Authorized representatives

Alexander Scharf, Harald Scharf

Contact details of the data protection controller

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

NESTEC OG

Hr. Alexander Scharf

Pummerinplatz 5, 4470 Enns

E-Mail: office@nestec.at

Phone: +43 (7223) 80703

Company details: <https://nestec.at/impressum/>

EU Dispute Resolution

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

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

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

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

Liability for the Contents of this Website

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

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

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

Liability for Links on this Website

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

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

Copyright Notice

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

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

All texts are copyrighted.

Privacy Policy

Table of contents

- [Privacy Policy Introduction and Overview](#)
- [Scope](#)
- [Legal bases](#)
- [Contact details of the data protection controller](#)
- [Storage Period](#)
- [Rights in accordance with the General Data Protection Regulation](#)
- [Security of data processing operations](#)
- [Communications](#)
- [Data Processing Agreement \(DPA\)](#)
- [Cookies](#)
- [Customer Data](#)
- [Registration](#)
- [Web hosting](#)
- [Web Analytics](#)
- [Email-Marketing](#)
- [Messenger & Communication Introduction](#)
- [Online Marketing](#)
- [Payment providers](#)
- [Credit Checking Agency Introduction](#)
- [Audio & Video](#)
- [Video Conferencing & Streaming](#)
- [Web Design Introduction](#)
- [Online Booking Systems Introduction](#)
- [Explanation of the terminology used](#)
- [Closing Remarks](#)

Privacy Policy Introduction and Overview

We have written this privacy policy (version 03.02.2023-122400850) in order to explain to you, in accordance with the provisions of the [General Data Protection Regulation \(EU\) 2016/679](#) and applicable national laws, which personal data (data for short) we as the controller – and the processors commissioned by us (e.g. providers) – process, will process in the future and what legal options you have. The terms used are to be considered gender-neutral.

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

Privacy policies usually sound very technical and use legal terminology. However, this privacy policy is intended to describe the most important things to you as simply and transparently as possible. So long as it aids transparency, technical **terms are explained in a reader-friendly manner, links** to further information are provided and **graphics** are used. We are thus informing in clear and

simple language that we only process personal data in the context of our business activities if there is a legal basis for it. This is certainly not possible with brief, unclear and legal-technical statements, as is often standard on the internet when it comes to data protection. I hope you find the following explanations interesting and informative. Maybe you will also find some information that you have not been familiar with.

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

Scope

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

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

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

Legal bases

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

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

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

1. **Consent** (Article 6 Paragraph 1 lit. a GDPR): You have given us your consent to process data for a specific purpose. An example would be the storage of data you entered into a contact form.
2. **Contract** (Article 6 Paragraph 1 lit. b GDPR): We process your data in order to fulfill a contract or pre-contractual obligations with you. For example, if we conclude a sales contract with you, we need personal information in advance.
3. **Legal obligation** (Article 6 Paragraph 1 lit. c GDPR): If we are subject to a legal obligation, we will process your data. For example, we are legally required to keep invoices for our bookkeeping. These usually contain personal data.

4. **Legitimate interests** (Article 6 Paragraph 1 lit. f GDPR): In the case of legitimate interests that do not restrict your basic rights, we reserve the right to process personal data. For example, we have to process certain data in order to be able to operate our website securely and economically. Therefore, the processing is a legitimate interest.

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

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

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

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

Contact details of the data protection controller

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

NESTEC OG

Hr. Alexander Scharf

Pummerinplatz 5, 4470 Enns

E-Mail: office@nestec.at

Phone: [+43 \(7223\) 80703](tel:+43722380703)

Company details: <https://nestec.at/impressum/>

Storage Period

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

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

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

Rights in accordance with the General Data Protection Regulation

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

- According to Article 15 DSGVO, you have the right to information about whether we are processing data about you. If this is the case, you have the right to receive a copy of the data and to know the following information:
 - for what purpose we are processing;
 - the categories, i.e. the types of data that are processed;
 - who receives this data and if the data is transferred to third countries, how security can be guaranteed;
 - how long the data will be stored;
 - the existence of the right to rectification, erasure or restriction of processing and the right to object to processing;
 - that you can lodge a complaint with a supervisory authority (links to these authorities can be found below);
 - the origin of the data if we have not collected it from you;
 - Whether profiling is carried out, i.e. whether data is automatically evaluated to arrive at a personal profile of you.
- You have a right to rectification of data according to Article 16 GDPR, which means that we must correct data if you find errors.
- You have the right to erasure (“right to be forgotten”) according to Article 17 GDPR, which specifically means that you may request the deletion of your data.
- According to Article 18 of the GDPR, you have the right to restriction of processing, which means that we may only store the data but not use it further.
- According to Article 20 of the GDPR, you have the right to data portability, which means that we will provide you with your data in a standard format upon request.
- According to Article 21 DSGVO, you have the right to object, which entails a change in processing after enforcement.
 - If the processing of your data is based on Article 6(1)(e) (public interest, exercise of official authority) or Article 6(1)(f) (legitimate interest), you may object to the processing. We will then check as soon as possible whether we can legally comply with this objection.
 - If data is used to conduct direct advertising, you may object to this type of data processing at any time. We may then no longer use your data for direct marketing.
 - If data is used to conduct profiling, you may object to this type of data processing at any time. We may no longer use your data for profiling thereafter.
- According to Article 22 of the GDPR, you may have the right not to be subject to a decision based solely on automated processing (for example, profiling).
- You have the right to lodge a complaint under Article 77 of the GDPR. This means that you can complain to the data protection authority at any time if you believe that the data processing of personal data violates the GDPR.

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

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

Austria Data protection authority

Manager: Mag. Dr. Andrea Jelinek

Address: Barichgasse 40-42, 1030 Wien

Phone number.: +43 1 52 152-0

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

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

Security of data processing operations

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


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

TLS encryption with https

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

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

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

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

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

Communications

Communications Overview

Affected parties: Anyone who communicates with us via phone, email or online form

Processed data: e. g. telephone number, name, email address or data entered in forms. You can find more details on this under the respective form of contact

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

Storage duration: for the duration of the business case and the legal requirements

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

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

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

Affected persons

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

Telephone

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

Email

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

Online forms

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

Legal bases

Data processing is based on the following legal bases:

- Art. 6 para. 1 lit. a GDPR (consent): You give us your consent to store your data and to

continue to use it for the purposes of the business case;

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

Data Processing Agreement (DPA)

In this section, we would like to explain what a Data Processing Agreement is and why it is needed. As the term "Data Processing Agreement" is quite lengthy, we will often only use the acronym DPA here in this text. Like most companies, we do not work alone, but also use the services of other companies or individuals. By involving different companies or service providers, we may pass on personal data for processing. These partners then act as processors with whom we conclude a contract, the so-called Data Processing Agreement (DPA). Most importantly for you to know is that any processing of your personal data takes place exclusively according to our instructions and must be regulated by the DPA.

Who are the processors?

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

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

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

Contents of a Data Processing Agreement

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

- indication to us as the controller
- obligations and rights of the controller
- categories of data subjects

- type of personal data
- type and purpose of data processing
- subject and duration of data processing
- location of data processing

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

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

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

Cookies

Cookies Overview

Affected parties: visitors to the website

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

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

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

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

What are cookies?

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

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

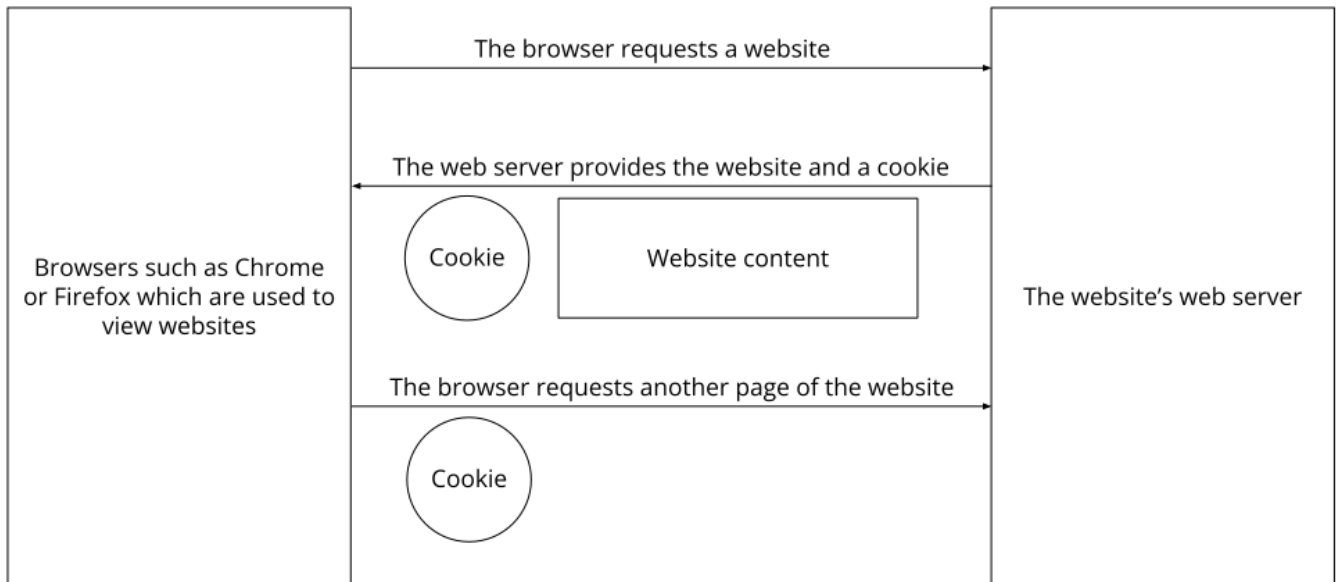
Whenever you surf the Internet, you are using a browser. Common browsers are for example, Chrome, Safari, Firefox, Internet Explorer and Microsoft Edge. Most websites store small text-files in your browser. These files are called cookies.

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

Cookies store certain user data about you, such as language or personal page settings. When you re-open our website to visit again, your browser submits these "user-related" information back to

our site. Thanks to cookies, our website knows who you are and offers you the settings you are familiar to. In some browsers, each cookie has its own file, while in others, such as Firefox, all cookies are stored in one single file.

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



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

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

Name: `_ga`

Value: `GA1.2.1326744211.152122400850-9`

Purpose: Differentiation between website visitors

Expiry date: after 2 years

A browser should support these minimum sizes:

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

Which types of cookies are there?

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

There are 4 different types of cookies:

Essential cookies

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

Purposive cookies

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

Target-orientated cookies

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

Advertising cookies

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

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

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

Purpose of processing via cookies

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

Which data are processed?

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

Storage period of cookies

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

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

remain unaffected until then.

Right of objection – how can I erase cookies?

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

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

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

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

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

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

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

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

Legal basis

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

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

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

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

Customer Data

Customer Data Overview

Affected parties: Customers or business and contractual partners

Purpose: Performance of a contract for the provision of agreed services or prior to entering into such a contract, including associated communications.

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

Storage period: the data will be erased as soon as they are no longer required for our business purposes and there is no legal obligation to process them.

Legal bases: Legitimate interests (Art. 6 Para. 1 lit. f GDPR), Contract (Art. 6 Para. 1 lit. b GDPR)

What is customer data?

In order to be able to offer our services and contractual services, we also process data from our customers and business partners. This data always includes personal data. Customer data is all information that is processed on the basis of contractual or pre-contractual agreements so that the offered services can be provided. Customer data is therefore all the information we collect and process about our customers.

Why do we process customer data?

There are many reasons why we collect and process customer data. The main reason is that we simply need specific data to provide our services. Sometimes for example your email address may be enough. But if you purchase a product or service, we may e. g. also need data such as your name, address, bank details or other contract data. This data will subsequently be used for marketing and sales optimisation so that we can improve our overall service for our customers and clients. Another important reason for data processing is our customer service, which is very important to us. We want you to have the opportunity to contact us at any time with questions about our offers. Thus, we may need certain data such as your email address at the very least.

What data is processed?

Exactly which data is stored can only be shown by putting them in categories. All in all, it always depends on which of our services you receive. In some cases, you may only give us your email address so that we can e. g. contact you or answer your questions. In other instances, you may purchase one of our products or services. Then we may need significantly more information, such as your contact details, payment details and contract details.

Here is a list of potential data we may receive and process:

- Name
- Contact address
- Email address
- Phone number

- Your birthday
- Payment data (invoices, bank details, payment history, etc.)
- Contract data (duration, contents)
- Usage data (websites visited, access data, etc.)
- Metadata (IP address, device information)

How long is the data stored?

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

Legal Basis

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

In the case of protecting vital interests, data processing is carried out in accordance with Article 9 Paragraph 2 Letter c. GDPR. For the purposes of health care, occupational medicine, medical diagnostics, care or treatment in the health or social sectors or for the administration of systems and services in health or social sectors, the processing of personal data takes place in accordance with Art. 9 Para. 2 lit. h. GDPR. If you voluntarily provide data of these special categories, the processing takes place on the basis of Article 9 Paragraph 2 lit. a GDPR.

Registration

Registration Overview

Affected parties: Anyone who registers to create an account with us, and logs in to use the account.

Processed data: Personal data such as email address, name, password and other data that is collected during registration, login and account use.

Purpose: For the provision of our services, as well as to communicate with clients or customers in the scope of our services.

Storage period: As long as the company account associated with the texts exists, plus a period of usually 3 years.

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

If you register with us and provide any personal data, this data may be processed, possibly along with your IP address. Below you can explore what we mean by the rather broad term "personal data".

Please only enter the data we need for the registration. In case you are registering on behalf of a third party, please only enter data for which you have the approval of the party you are registering for. If possible, use a secure password that you don't use anywhere else and an email address that you check regularly.

In the following, we will inform you about the exact type of data processing we do. After all, we want you to feel at ease with the services we provide!

What is a registration?

When you register, we retain certain of your data in order to make it easy for you to log in with us online and use your account. An account with us has the advantage that you don't have to re-enter everything every time. It saves time and effort and ultimately prevents any issues with the provision of our services.

Why do we process personal data?

In short, we process personal data to make account registration and usage possible for you. If we didn't do this, you would have to enter all your data each time, wait for our approval and then enter everything again. This strenuous process would probably not only irritate us a little, but also many of our dear clients and customers.

Which data is processed?

Any data that you provided during registration or login and any data that you may enter as part of managing your account data.

During registration, we process the following types of data:

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

During your registration, we process any data you enter, such as your username and password, along with data that is collected in the background such as your device information and IP addresses.

When using your account, we process any data you enter while using the account, as well as any data that is created while you use our services.

Storage time

We store the entered data for at least as long as the account associated with the data exists with us and is in use – and as long as there are contractual obligations between you and us. In case the contract ends, we retain the data until the respective claims get time-barred. Moreover, we store your data as long as we are subject to legal storage obligations, if applicable. Following that, we keep any accounting records (invoices, contract documents, account statements, etc.) of the contract for 10 years (§ 147 AO) and other relevant business documents for 6 years (§ 247 HGB) after accrual.

Right to object

You have registered, entered data and want to revoke the data processing? Not a problem. As you can see above, you retain this right under the General Data Protection Regulation also at and after registration, login or account creation with us. Contact the Data Protection Officer above to exercise your rights. If you already have an account with us, you can easily view and manage your data and texts in your account.

Legal Basis

By completing the registration process, you enter into a pre-contractual agreement with us, with the intention to conclude a contract of use for our platform (although there is no automatic payment obligation). You invest time to enter data and register and in return, we offer you our services after you log on to our system and view your customer account. We also meet our contractual obligations. Finally, we need to be able to email registered users about important changes. Article 6(1)(b) GDPR (implementation of pre-contractual measures, fulfilment of a contract) applies.

Where applicable, we will ask for your consent, e.g. in case you voluntarily provide more data than is absolutely necessary, or in case we may ask you if we may send you advertising. Article 6 paragraph 1 lit. a GDPR (consent) applies in this matter.

We also have a legitimate interest in knowing who who our clients or customers are, in order to get in touch if required. We also need to know who is using our services and whether they are being used in accordance with our terms of use, i.e. Article 6(1)(f) GDPR (legitimate interests) applies in this matter.

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

Registration with real names

Since business operations require us to know who our clients or customers are, registration is only possible with your real name (full name) and not with a pseudonym.

Registration with pseudonyms

You can use a pseudonym for the registration, which means you don't have to register with your

real name. This ensures that your real name cannot be processed by us.

Storage of the IP address

During registration, login and account use, we store your IP address for security reasons in order to be able to determine legitimate use.

Public Profile

User profiles are publicly visible, i.e. parts of the profiles can also be viewed on the Internet without the need to enter a username and password.

Two Factor Authentication (2FA)

Two Factor Authentication (2FA) offers additional security when logging in, as it prevents you from logging in without a smartphone, for example. This technical measure to secure your account protects you against the loss of data or unauthorised access, even if your username and password were leaked. During your registration process, login or within the account itself you can find out which 2FA is used.

Web hosting

Web hosting Overview

Affected parties: visitors to the website

Purpose: professional hosting of the website and security of operations

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

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

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

What is web hosting?

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

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

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

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

Illustration:



Why do we process personal data?

The purposes of data processing are:

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

Which data are processed?

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

- the full address (URL) of the accessed website (e. g. <https://www.examplepage.uk/examplesubpage.html?tid=122400850>)
- browser and browser version (e.g. Chrome 87)
- the operating system used (e.g. Windows 10)
- the address (URL) of the previously visited page (referrer URL) (e. g. <https://www.examplepage.uk/icamefromhere.html/>)
- the host name and the IP address of the device from the website is being accessed from (e.g. COMPUTERNAME and 194.23.43.121)
- date and time
- in so-called web server log files

How long is the data stored?

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

In short: Your visit is logged by our provider (company that runs our website on special computers

(servers)), but we do not pass on your data without your consent!

Legal basis

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

Hetzner Privacy Policy

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

Data Processing Agreement (DPA) Hetzner

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

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

Web Analytics

Web Analytics Privacy Policy Overview

Affected parties: visitors to the website

Purpose: Evaluation of visitor information to optimise the website.

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

Storage period: depending on the respective web analytics tool used

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

What is Web Analytics?

We use software on our website, which is known as web analytics, in order to evaluate website visitor behaviour. Thus, data is collected, which the analytic tool provider (also called tracking tool) stores, manages and processes. Analyses of user behaviour on our website are created with this data, which we as the website operator receive. Most tools also offer various testing options. These enable us, to for example test which offers or content our visitors prefer. For this, we may show you two different offers for a limited period of time. After the test (a so-called A/B test) we know which

product or content our website visitors find more interesting. For such testing as well as for various other analyses, user profiles are created and the respective data is stored in cookies.

Why do we run Web Analytics?

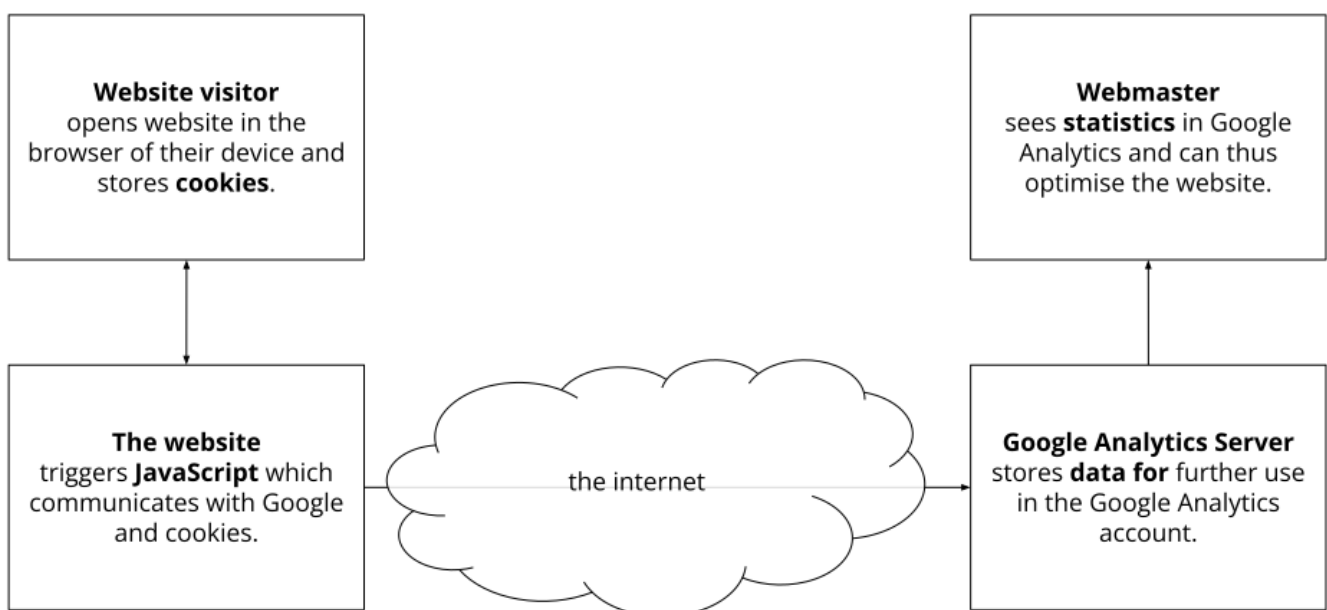
We have a clear goal in mind when it comes to our website: we want to offer our industry's best website on the market. Therefore, we want to give you both, the best and most interesting offer as well as comfort when you visit our website. With web analysis tools, we can observe the behaviour of our website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

Which data are processed?

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

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

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



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

Duration of data processing

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

Right to object

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

Legal basis

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

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

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

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

YouTube Analytics and Reporting API Privacy Policy

We use the web analysis tool YouTube Analytics and Reporting API on our website. The service provider is the American company YouTube, LLC, 901 Cherry Ave., San Bruno, CA 94066, USA.

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

YouTube uses standard contractual clauses approved by the EU Commission (= Art. 46. Para. 2 and

3 GDPR). These clauses oblige YouTube to comply with EU data protection standards when processing relevant data outside the EU. These clauses are based on an implementation order of the EU Commission. You can find the decision and the clauses here:

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

You can find more information about the standard contractual clauses at Google at

<https://business.safety.google/intl/en/adsprocessor/terms/>.

Since YouTube is a subsidiary of Google, they share the same privacy policy. If you want to find out more about how your data is handled, we recommend you read the privacy policy at

<https://policies.google.com/privacy?hl=en>.

Email-Marketing

Email Marketing Overview

Affected parties: newsletter subscribers

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

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

Storage duration: for the duration of the subscription

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

What is Email-Marketing?

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

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

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

Why do we use Email-Marketing?

Of course, we want to stay in contact with you and keep you in the loop of the most important news about our company. For this, we use email marketing – often just referred to as “newsletters”

– as an essential part of our online marketing. If you agree to this or if it is permitted by law, we will send you newsletters, system emails or other notifications via email. Whenever the term “newsletter” is used in the following text, it mainly refers to emails that are sent regularly. We of course don't want to bother you with our newsletter in any way. Thus, we genuinely strive to offer only relevant and interesting content. In our emails you can e.g. find out more about our company and our services or products. Since we are continuously improving our offer, our newsletter will always give you the latest news, or special, lucrative promotions. Should we commission a service provider for our email marketing, who offers a professional mailing tool, we do this in order to offer you fast and secure newsletters. The purpose of our email marketing is to inform you about new offers and also to get closer to our business goals.

Which data are processed?

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

Duration of data processing

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

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

Withdrawal – how can I cancel my subscription?

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

Legal basis

Our newsletter is sent on the basis of your **consent** (Article 6 (1) (a) GDPR). This means that we are only allowed to send you a newsletter if you have actively registered for it beforehand. Moreover,

we may also send you advertising messages on the basis of Section 7 (3) UWG (Unfair Competition Act), provided you have become our customer and have not objected to the use of your email address for direct mail.

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

Messenger & Communication Introduction

Messenger & Communication Privacy Statement Overview

Affected parties: website visitors

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

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

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

Storage duration: depends on the messenger & communication functions

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

What are Messenger & Communication functions?

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

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

Why do we use Messenger & Communication functions?

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

We generally assume our responsibility under data protection law, even if we use the services of any social media platform. However, the European Court of Justice has decided that in certain cases

the operator of the social media platform be jointly responsible alongside us in the scope of Art. 26 GDPR. Should this be the case, we will point it out separately and work on the basis of a relevant agreement. You will find the essence of the agreement for the respective platforms below.

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

Which data is processed?

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

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

How long is data stored?

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

Right to object

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

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

Legal Basis

If you have consented to the data processing and storage by integrated messenger &

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

Zoho Desk Privacy Policy

We also use the customer service software Zoho Desk. The provider of this service is the American company Zoho Corporation, 4141 Hacienda Drive, Pleasanton, CA 94588, USA.

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

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

For more information on Zoho's standard contractual clauses, visit https://www.zoho.com/privacy/dpa/DPA_zoho_com.pdf.

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

Online Marketing

Online Marketing Privacy Policy Overview

Affected parties: visitors to the website

Purpose: Evaluation of visitor information for website optimisation

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

Storage period: depending on the Online Marketing tools used

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

What is Online Marketing?

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

Why do we use Online Marketing tools?

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

Which data are processed?

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

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

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

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

We only ever receive summarised information from the advertising tools we use that do store data on their servers. We never receive data that can be used to identify you as an individual. What is

more, the data only shows how well-placed advertising measures have worked. For example, we can see what measures have caused you or other users to visit our website and purchase a service or product. Based on these analyses we can improve our advertising offer in the future and adapt it more precisely to the needs and wishes of people who are interested.

Duration of data processing

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

Right of withdrawal

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

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

Legal basis

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

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

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

Payment providers

Payment Providers Privacy Policy Overview

Affected parties: visitors to the website

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

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

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

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

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

What is a payment provider?

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

Why do we use payment providers on our website?

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

Which data are processed?

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

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

Duration of data processing

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

Right to object

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

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

Legal basis

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

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

PayPal Privacy Policy

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

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

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

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

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

You can find out more about the data processed by using PayPal in the Privacy Policy at

<https://www.paypal.com/webapps/mpp/ua/privacy-full>.

UniCredit Privacy Policy

We use the payment provider UniCredit on our website. The service provider is the Italian company UniCredit S.p.A., Piazza Gae Aulenti 3, Tower A, 20154 Milan, Italy.

You can find out more about the data processed through the use of UniCredit in their Privacy Policy at <https://www.unicredit.it/it/info/privacy.html>

Visa Privacy Policy

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

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

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

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

You can find out more about the data processed through the use of Visa in the Privacy Policy at

<https://www.visa.co.uk/legal/privacy-policy.html>.

Credit Checking Agency Introduction

Credit Checkers Privacy Policy Overview

Affected parties: Customers and clients

Purpose: Credit score checks and credit rating checks

Processed data: credit data, payment data, contact data, contract data

Storage duration: depends on the credit checking agency used

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

What are credit checking agencies?

In some cases, we use credit checking agencies for our online transactions so we can obtain information about your creditworthiness if we provide our services or products in advance of payment receipt. Credit checking agencies calculate a statistic probability of non-payment. This means we receive information about how likely it is that you will be able to pay your bill, for example. This information enables us to better decide whether or not to provide our products or services in advance of receiving your payment. We can therefore also refuse requests for payments after delivery (e.g. payment after you receive our products/services) if the result of your credit check is negative.

Why do we use credit checking agencies?

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

Which data is processed?

The decision on whether you will be able to pay after delivery is made on the basis of an automated decision on a case-by-case basis by software that uses the information of the respective credit checking agency (= Art. 22 GDPR). The data that is usually processed includes your name, address, bank details, invoices, payment history, contact details such as your email address and telephone number, as well as contract data such as the term, customer information and the subject of the contract. You can find more information about data processing in the privacy policies of the respective credit rating agencies.

Duration of data processing

How long your data is processed and stored depends mainly on the credit checking agencies we use. Below you can find out more about the data processing of individual providers. The providers' privacy policies usually state exactly which data is stored and processed and for how long. Generally, personal data is only processed for as long as is necessary to provide our services. However, when data is stored in cookies, the storage period varies greatly. Usually, you will be able to find helpful information about individual cookies in the privacy policies of the individual providers.

Legal Basis

If we obtain consent through our contractual partners, this consent serves as the legal basis (Article 6 Paragraph 1 lit. a GDPR) for credit checks, as well as for customer data transmission to credit checking agencies. If this consent does not exist, the legal basis is our legitimate interest (Article 6 Paragraph 1 lit. f GDPR) in payment failsafety. If you have given your consent, this also serves as the legal basis for creditworthiness checks and data transmission.

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

KSV1870 Privacy Policy

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

Audio & Video

Audio & Video Privacy Policy Overview

Affected parties: website visitors

Purpose: service optimisation

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

You can find more details in the Privacy Policy below.

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

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

What are audio and video elements?

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

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

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

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

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

Which data are retained by audio & video elements?

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

Duration of data processing

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

Right to object

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

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

Legal basis

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

YouTube Privacy Policy

YouTube Privacy Policy Overview

Affected parties: website visitors

Purpose: optimising our service

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

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

Storage period: data are generally stored for as long as is necessary for the purpose of the service

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

What is YouTube?

We have integrated YouTube videos to our website. Therefore, we can show you interesting videos directly on our site. YouTube is a video portal, which has been a subsidiary company of Google LLC since 2006. The video portal is operated by YouTube, LLC, 901 Cherry Ave., San Bruno, CA 94066, USA. When you visit a page on our website that contains an embedded YouTube video, your browser automatically connects to the servers of YouTube or Google. Thereby, certain data are transferred (depending on the settings). Google is responsible for YouTube's data processing and therefore Google's data protection applies.

In the following we will explain in more detail which data is processed, why we have integrated YouTube videos and how you can manage or clear your data.

On YouTube, users can watch, rate, comment or upload videos for free. Over the past few years, YouTube has become one of the most important social media channels worldwide. For us to be able to display videos on our website, YouTube provides a code snippet that we have integrated to our website.

Why do we use YouTube videos on our website?

YouTube is the video platform with the most visitors and best content. We strive to offer you the best possible user experience on our website, which of course includes interesting videos. With the help of our embedded videos, we can provide you other helpful content in addition to our texts and images. Additionally, embedded videos make it easier for our website to be found on the Google search engine. Moreover, if we place ads via Google Ads, Google only shows these ads to people who are interested in our offers, thanks to the collected data.

What data is stored by YouTube?

As soon as you visit one of our pages with an integrated YouTube, YouTube places at least one cookie that stores your IP address and our URL. If you are logged into your YouTube account, by using cookies YouTube can usually associate your interactions on our website with your profile. This includes data such as session duration, bounce rate, approximate location, technical information such as browser type, screen resolution or your Internet provider. Additional data can

include contact details, potential ratings, shared content via social media or YouTube videos you added to your favourites.

If you are not logged in to a Google or YouTube account, Google stores data with a unique identifier linked to your device, browser or app. Thereby, e.g. your preferred language setting is maintained. However, many interaction data cannot be saved since less cookies are set.

In the following list we show you cookies that were placed in the browser during a test. On the one hand, we show cookies that were set without being logged into a YouTube account. On the other hand, we show you what cookies were placed while being logged in. We do not claim for this list to be exhaustive, as user data always depend on how you interact with YouTube.

Name: YSC

Value: b9-CV6ojl5Y122400850-1

Purpose: This cookie registers a unique ID to store statistics of the video that was viewed.

Expiry date: after end of session

Name: PREF

Value: f1=50000000

Purpose: This cookie also registers your unique ID. Google receives statistics via PREF on how you use YouTube videos on our website.

Expiry date: after 8 months

Name: GPS

Value: 1

Purpose: This cookie registers your unique ID on mobile devices to track GPS locations.

Expiry date: after 30 minutes

Name: VISITOR_INFO1_LIVE

Value: 95Chz8bagyU

Purpose: This cookie tries to estimate the user's internet bandwidth on our sites (that have built-in YouTube videos).

Expiry date: after 8 months

Further cookies that are placed when you are logged into your YouTube account:

Name: APISID

Value: zILlvClZSkqGsSwI/AU1aZl6HY7122400850-

Purpose: This cookie is used to create a profile on your interests. This data is then used for personalised advertisements.

Expiry date: after 2 years

Name: CONSENT

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

Purpose: The cookie stores the status of a user's consent to the use of various Google services. CONSENT also provides safety measures to protect users from unauthorised attacks.

Expiry date: after 19 years

Name: HSID

Value: AcRwpgUik9Dveht0I

Purpose: This cookie is used to create a profile on your interests. This data helps to display customised ads.

Expiry date: after 2 years

Name: LOGIN_INFO

Value: AFmmF2swRQIhALl6aL...

Purpose: This cookie stores information on your login data.

Expiry date: after 2 years

Name: SAPISID

Value: 7oaPxoG-pZsjuuF5/AnUdDUlsj9ijz2vdM

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

Expiry date: after 2 years

Name: SID

Value: oQfNKjAsI122400850-

Purpose: This cookie stores your Google Account ID and your last login time, in a digitally signed and encrypted form.

Expiry date: after 2 years

Name: SIDCC

Value: AN0-TYuqub2JOcDTyL

Purpose: This cookie stores information on how you use the website and on what advertisements you may have seen before visiting our website.

Expiry date: after 3 months

How long and where is the data stored?

The data YouTube receive and process on you are stored on Google's servers. Most of these servers are in America. At <https://www.google.com/about/datacenters/locations/?hl=en> you can see where Google's data centres are located. Your data is distributed across the servers. Therefore, the data can be retrieved quicker and is better protected against manipulation.

Google stores collected data for different periods of time. You can delete some data anytime, while other data are automatically deleted after a certain time, and still other data are stored by Google for a long time. Some data (such as elements on "My activity", photos, documents or products) that are saved in your Google account are stored until you delete them. Moreover, you can delete some data associated with your device, browser, or app, even if you are not signed into a Google Account.

How can I erase my data or prevent data retention?

Generally, you can delete data manually in your Google account. Furthermore, in 2019 an automatic deletion of location and activity data was introduced. Depending on what you decide on, it deletes stored information either after 3 or 18 months.

Regardless of whether you have a Google account or not, you can set your browser to delete or deactivate cookies placed by Google. These settings vary depending on the browser you use. The following instructions will show how to manage cookies in your browser:

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

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

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

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

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

If you generally do not want to allow any cookies, you can set your browser to always notify you when a cookie is about to be set. This will enable you to decide to either allow or permit each individual cookie.

Legal basis

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

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

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

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

Since YouTube is a subsidiary company of Google, Google's privacy statement applies to both. If you want to learn more about how your data is handled, we recommend the privacy policy at <https://policies.google.com/privacy?hl=en>.

YouTube Subscribe Button Privacy Policy

We have integrated the YouTube subscribe button to our website, which you can recognise by the classic YouTube logo. The logo shows the words "Subscribe" or "YouTube" in white letters against a red background, with a white "Play" symbol on the left. The button may also be displayed in a different design.

Our YouTube channel consistently offers you funny, interesting or exciting videos. With the built-in "Subscribe" button you can subscribe to our channel directly via our website and do not need to go to YouTube's website for it. With this feature, we want to make it as easy as possible for you to access our comprehensive content. Please note that YouTube may save and process your data.

If you see a built-in subscription button on our page, YouTube sets at least one cookie, according to Google. This cookie stores your IP address and our URL. It also allows YouTube to receive information about your browser, your approximate location and your default language. In our test the following four cookies were placed, without us being logged into YouTube:

Name: YSC

Value: b9-CV6ojl5122400850Y

Purpose: This cookie registers a unique ID, which stores statistics of the viewed video.

Expiry date: after end of session

Name: PREF

Value: f1=50000000

Purpose: This cookie also registers your unique ID. Google uses PREF to get statistics on how you interact with YouTube videos on our website.

Expiry date: after 8 months

Name: GPS

Value: 1

Purpose: This cookie registers your unique ID on mobile devices to track your GPS location.

Expiry date: after 30 minutes

Name: VISITOR_INFO1_LIVE

Value: 12240085095Chz8bagyU

Purpose: This cookie tries to estimate the user's internet bandwidth on our website (that contain built-in YouTube video).

Expiry date: after 8 months

Note: These cookies were set after a test, thus we do not claim for the list to be exhaustive.

If you are logged into your YouTube account, YouTube may store many of the actions and

interactions you make on our website via cookies, to then assign them to your YouTube account. This gives YouTube information on e.g. how long you have been browsing our website, which browser type you use, which screen resolution you prefer or what actions you take.

On the one hand, YouTube uses this data to improve its own services and offers, and on the other hand to provide analyses and statistics for advertisers (who use Google Ads).

Video Conferencing & Streaming

Video Conferencing & Streaming Privacy Policy Overview

Affected parties: users of our video conferencing or streaming tools

Purpose: communication and presentation of content

Processed data: Access statistics such as your name, address, contact details, email address, telephone number or IP address. You can find more details on this directly at the video conference or streaming tool that is being used.

Storage duration: depending on the video conferencing or streaming tool

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

What are video conferences & streamings?

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

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

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

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

Which data are processed?

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

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

Duration of data processing

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

Right to object

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

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

Legal basis

If you have consented to the processing and storage of your data by the respective video or streaming solution, this consent is the legal basis for data processing (**Art. 6 para. 1 lit. a GDPR**). We may also offer a video conference as part of our services, if there has been a contractual agreement with you in advance (**Art. 6 para. 1 lit. b GDPR**). Generally, your data is also stored and processed on the basis of our legitimate interest (**Art. 6 para. 1 lit. f GDPR**) to maintain fast and good communication with you or other customers and business partners, provided you have priorly given consent. Most video or streaming solutions also place cookies in your browser to store data. We therefore recommend you to read our privacy policy about cookies carefully and to take a look at the privacy policy or the cookie policy of the respective service provider.

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

GoToMeeting Privacy Policy

We use GoToMeeting on our website, which is a video meeting service. The provider of this service is the American company LogMeIn with its Irish headquarters at Ireland Limited, Bloodstone Building Block C 70, Sir John Rogerson's Quay Dublin 2, Ireland.

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

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

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

You can find out more about the data that is processed through the use of GoToMeeting in their Privacy Policy at <https://www.logmein.com/legal/privacy>.

Data Processing Agreement (DPA) GoToMeeting

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

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

Web Design Introduction

Web Design Privacy Policy Overview

Affected parties: website visitors

Purpose: improvement of user experience

Processed data: depends heavily on the services used. Usually, data such as IP address, technical data, language settings, browser version, screen resolution and browser name are processed. You can find more details directly with the respective web design tools.

Storage duration: depends on the tools used

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

What is web design?

We use various tools on our website for the purpose of our web design. Contrary to common belief, web design is not just about making our website look nice, but rather also about functionality and performance. But of course, a good-looking website is also a major goal of professional web design. Web design is a part of media design and deals with the visual as well as the structural and

functional design of a website. Our aim with our web design is to improve your experience on our site. In web design jargon, this is called User Experience (UX) and usability. User Experience entails all impressions and experiences that website visitors come across on a website. What is more, usability is part of the User Experience, as it determines how user-friendly a website is. This includes the clear structuring of content, subpages or products, along with how quickly and easily the website enables you to find what you are looking for. In order to offer you the best possible experience on our website, we also use so-called third-party web design tools. Therefore, all tools and services that help improve our website's design are classified under the category "web design". This may, for example, include fonts, various plugins or other integrated web design functions.

Why do we use web design tools?

The way you absorb information on a website depends very much on its structure, functionality and visual perception. Therefore, good and professional web design has become increasingly important for us. We are constantly working on improving our site as a way of further extending our services for you as a website visitor. Furthermore, a beautiful and functioning website also has economic advantages for us. Needless to say, you will only visit it and take advantage of our offers if you feel completely at ease.

What data is stored by web design tools?

When you visit our website, any web design elements integrated into our pages may process your data. The exact data that is processed depends on the tools used. Below you can see exactly which tools we use for our website. For more information about data processing, we recommend you also read the respective privacy policy of the respective tools. There you can usually find out which data is processed, whether cookies are used and how long the data is stored. Moreover, fonts such as Google Fonts, for example, also automatically transmit information such as your language settings, IP address, browser version, browser screen resolution and browser name to Google's servers.

Duration of data processing

Data processing times are very individual and depend on the web design elements used. For example, when cookies are used, the retention period can be as little as a minute, but it may also be a few years. Please make yourself familiar with this topic. You may for example read our general section on cookies as well as the Privacy Policies of the tools used. There you can likely find out exactly which cookies are used and what information is stored there. For example, Google Font files are stored for one year, in order to improve the loading speed of a website. In principle, data is only kept for as long as is necessary to provide the service. But legal requirements may require data to be stored for longer.

Right to object

You also retain the right and the option to revoke your consent to the use of cookies or third-party providers at any time. You can do this either via our cookie management tool or via other opt-out functions. You can also prevent cookies from collecting your data by managing, deactivating or

deleting the cookies in your browser. However, among web design elements (typically fonts) there is also data that cannot be erased easily. This is the case whenever data is automatically collected as soon as a page is accessed and then directly transmitted to a third party (e.g. Google). In these cases, please contact the support of the respective provider. In the case of Google, you can reach support at <https://support.google.com/?hl=de>.

Legal Basis

If you have consented to the use of web design tools, this consent serves as the legal basis for the relevant data processing. According to Article 6 (1) (a) GDPR (consent), your consent represents the legal basis for the processing of personal data, as it may occur when it is collected by web design tools. We also have a legitimate interest in web design to improve on our website. After all, only then can we provide you with a beautiful and professional web offer. The corresponding legal basis for this is Article 6 (1) (f) GDPR (legitimate interests). However, we strongly want to emphasise once more that we only use web design tools if you have given your consent.

You can find information on different web design tools – if available – in the following sections.

Google Fonts Local Privacy Policy

On our website we use Google Fonts, by the company Google Inc. The responsible entity for the European area is Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland). We have integrated Google fonts locally, i.e. on our web server and not on Google's servers. This means that no connection to Google's servers and therefore no data transfer or retention take place.

What are Google Fonts?

Google Fonts was previously called Google Web Fonts. It is an interactive list with over 800 fonts which [Google](#) offer for free use. With the use of Google Fonts, it is possible to utilise fonts without uploading them to your own server. In order to prevent any transfer of information to Google's servers, we downloaded the fonts to our own server. This way we can comply with data privacy and do not transmit any data to Google Fonts.

Online Booking Systems Introduction

Online Booking Systems Privacy Policy Overview

Affected parties: website visitors

Purpose: improvement of user experience and organisation

Processed data: depends heavily on the services used. Usually, data such as IP address, contact and payment details and/or technical data is processed. You can get more details on this directly from the respective tools used.

Storage duration: depends on the tools used

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

What is an online booking system?

We use one or more booking systems which enable you to make bookings via our website. That way e.g. appointments can easily be created online. A booking system is a software application integrated into our website that displays available resources (such as available appointments) and allows you to book – and usually, also pay – directly online. You've probably already come across many such booking systems from the restaurant or hotel industry. However, such systems are actually used in a wide variety of industries. Depending on the tool and settings, booking systems can be used both by us internally, as well as by customers like yourself. In most cases, your personal data is also collected and stored.

Bookings usually work as follows: You will find a booking system on our website, through which you can book an appointment directly with one click. Then you will enter your data and usually also be able to pay immediately. You may also have the option to enter various information about yourself into a form. Please be aware that any information you enter may be stored and managed in a database.

Why do we use an online booking system?

In a way, we also consider our website a free service for you. We want you to receive helpful information on our site and feel comfortable on there. This also includes an online service that makes it as easy as possible for you to book appointments or services. Gone are the days when you had to wait days for booking confirmations via phone or email. With an online booking system, you can get everything done after just a few clicks and get on with your day. The system also makes it easier for us to manage all bookings and appointments. Therefore, we consider a booking system absolutely sensible for both you and ourselves.

Which data is processed?

In this general introduction about booking systems, we naturally cannot tell you exactly what data is processed for which system. It always depends on the tool used, as well as the functions and possibilities it contains. What is more, in addition to the conventional booking function, many booking systems also offer a range of other features. For example, many systems also have an external online payment system (e.g. Stripe, Klarna or Paypal) and an integrated calendar synchronisation function. Accordingly, different data and different amounts of data can be processed, depending on the included functions. Usually, data such as your IP address, name and contact details, technical device information and the time of your booking are processed. If you also make a payment via the system, your bank details such as your account number, credit card number, passwords, TANs etc. will also be stored and passed on to the respective payment provider. We recommend you carefully read the respective privacy policy of the tool used, so that you know which of your data is processed specifically.

Duration of data processing

Each booking system stores data for different lengths of time. Therefore, we cannot yet give any specific information about the duration of data processing in this instance. In general, however,

personal data is only stored for as long as is absolutely necessary to provide the services. Booking systems usually also use cookies, which store information for different lengths of time. While some cookies are erased immediately after leaving the site, others can be stored for a number of years. You can find out more about this in our “Cookies” section. Please also take a look at the respective privacy policies of the providers. There you should find answers on how long your data will be stored specifically.

Right to object

If you have consented to data processing by a booking system, you always retain the option and the right to revoke this consent. So please, always be aware that you have rights in relation to your personal data and that you can exercise these rights at any time. Thus, if you do not agree to the processing of your personal data, then none of your personal data may be processed. It is that simple. The easiest way to revoke data processing is via a cookie consent tool or via other available opt-out functions. You can, for example, manage data retention by cookies directly in your browser. Until you withdraw your consent, the lawfulness of data processing remains unaffected.

Legal Basis

If you have agreed that booking systems may be used, this consent is the legal basis for the corresponding data processing. According to Article 6 (1) (a) GDPR (consent), your consent represents the legal basis for the processing of personal data, as it may occur through the use of booking systems.

Furthermore, we also have a legitimate interest in using booking systems because we use them to extend our customer service and to optimise our internal booking organisation. The corresponding legal basis for this is Article 6 (1) (f) GDPR (legitimate interests). However, we strongly want to emphasise once more that we only use these tools if you have given your consent.

You can find information on different booking systems – if available – in the following sections.

Calendly Privacy Policy

We use Calendly, a planning and organization tool, for our website. The service provider is the American company Calendly LCC, 271 17th St NW, Ste 1000, Atlanta, Georgia, 30363, USA.

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

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

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

You can find out more about the data that is processed through the use of Calendly in their Privacy Policy at <https://calendly.com/privacy>.

Data Processing Agreement (DPA) Calendly

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

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

Explanation of the terminology used

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

Processor

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

newsletter providers or large companies such as Google or Microsoft.

Consent

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Genetic data

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“genetic data” means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

Explanation: With a certain amount of effort, persons can be identified using genetic data. That is why genetic data also belongs to the category of personal data. Genetic data is obtained from blood or saliva samples, for example.

Personal Data

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or

indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

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

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

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

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

Profiling

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Controller

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Processing

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Closing Remarks

Congratulations! If you are reading these lines, you have most likely familiarised yourself with our entire Privacy Policy – or at least scrolled down here. As you can see from the scope of our Privacy Policy, we do not take the protection of your personal data lightly.

We find it important to inform you about the processing of your personal data to the best of our abilities. In doing so, we not only want to tell you which data is processed but also explain to you why we use various software programs. In general, Privacy Policies have very technical and legal jargon. However, since most of you are not web developers or solicitors, we wanted to take a different approach and explain the facts in simple and clear language. Of course, this is not always possible due to the subject matter. Therefore, you can also find a more detailed explanation of the most important terms 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 body. We wish you all the best and hope to soon welcome you to our website again.

All texts are copyrighted.