



privacy policy

last edit: 30.01.2024

table of contents

1. [Privacy Policy Introduction and Overview](#)
2. [Scope](#)
3. [Legal bases](#)
4. [Contact details of the data protection controller](#)
5. [Storage Period](#)
6. [Rights in accordance with the General Data Protection Regulation](#)
7. [Data transfer to third countries](#)
8. [Security of data processing operations](#)
9. [Communications](#)
10. [Data Processing Agreement \(DPA\)](#)
11. [Cookies](#)
12. [Customer Data](#)
13. [Registration](#)
14. [Website Builders](#)
15. [Web Analytics](#)
16. [Email-Marketing](#)
17. [Online Marketing](#)
18. [External Online Platforms](#)
19. [Explanation of the terminology used](#)

1. Privacy Policy Introduction and Overview

We have written this privacy policy 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](#).

2. 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.

3. 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 DSGVO.
- 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.

4. 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:

Maximilian Krieger
Eschersheimer Landstr. 42
60322 Frankfurt am Main
Germany

E-Mail: info@yaur-gold.com

Imprint: <https://www.yaur-gold.com/imprint/>

5. 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.

6. 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:

Hessen Data protection authority
State Commissioner for Data Protection: Prof. Dr. Alexander Roßnagel
Address: Postfach 31 63, 65021 Wiesbaden
Phone number: 06 11/140 80
E-mail address: poststelle@datenschutz.hessen.de
Website: <https://datenschutz.hessen.de/>

7. Data transfer to third countries

We only transfer or process data to countries outside the scope of the GDPR (third countries) if you consent to this processing or if there is another legal permission. This is particularly true when processing is legally required or necessary for the performance of a contractual relationship, and in any case, only to the extent permitted by law. Your consent is in most cases the primary reason for us to process data in third countries. Processing of personal data in third countries such as the USA, where many software providers offer services and have their server locations, may mean that personal data is processed and stored in unexpected ways. We explicitly point out that, according to the opinion of the European Court of Justice, there is currently only an adequate level of protection for data transfers to the USA if a US company processing personal data of EU citizens in the USA is an active participant in the EU-US Data Privacy Framework. More information can be found at: https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en. Data processing by US services that are not active participants in the EU-US Data Privacy Framework may result in data not being anonymized and processed, if applicable. Additionally, US government authorities may potentially have access to individual data. Furthermore, it may occur that collected data is linked with data from other services of the same provider, if you have a corresponding user account. Where possible, we try to use server locations within the EU, if offered. We will inform you in the appropriate sections of this privacy policy in more detail about data transfers to third countries, if applicable.

8. 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, 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.

9. 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.

- 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.
- 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.
- 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.

10. 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.

11. 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 [graphic under this link](#) 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: GA1.2.1326744211.152312451506-9
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 165 (3) of the Telecommunications Act (2021). 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.

12. 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.

13. 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 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.

14. Website Builders

Website Builders Privacy Policy Overview

- Affected parties: website visitors
- Purpose: service optimisation
- Data processed: The data that is being processed includes but is not limited to technical usage information, browser activity, clickstream activity, session heat maps, contact details, IP addresses or geographic locations. You can find more details in the Privacy Policy below as well as in the providers' Privacy Policies.
- Storage duration: depends on the provider
- Legal bases: Art. 6 (1) lit. f GDPR (legitimate interests), Art. 6 (1) lit. a GDPR (consent)

What are website builders?

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

Why do we use website builders for our website?

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

Which data are stored by website builders?

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

How long and where are the data stored?

Provided that we have any further information on this, we will inform you below about the duration of the data processing associated with the website builder we use. You can find detailed information on this in the provider's Privacy Policy. Generally, we only process personal data for as long as is absolutely necessary to provide our services and products. The provider may store your data according to their own specifications, over which we have no influence.

Right to object

You always retain the right to information, rectification and erasure of your personal data. If you have any questions, you can also contact the responsible parties at the respective website builder system at any time. You can find the corresponding contact details either in our Privacy Policy or on the website of the respective provider. What is more, in your browser you can clear, disable or manage cookies that providers use for their functions. Depending on the browser you use, this can be done in different ways. Please note, that this

may lead to not all functions working as usual anymore.

Legal Bases

We have a legitimate interest in using a website builder system to optimise our online service and present it in an efficient and user-friendly way. The corresponding legal basis for this is Article 6 (1) (f) GDPR (legitimate interests). However, we only use the website builder system if you have consented to it. If the processing of data is not absolutely necessary for the operation of the website, your data will only be processed on the basis of your consent. This particularly applies to tracking activities. The legal basis for this is Article 6 (1) (a) GDPR. With this Privacy Policy, we have made you more familiar with the most important general information on data processing. If you want to find out more about this, you will find further information – if available – in the following section or in the Privacy Policy of the provider.

Wix Privacy Policy

Wix Privacy Policy Overview

- Affected parties: website visitors
- Purpose: service optimisation
- Processed data: data such as technical usage information like browser activity, clickstream activities, session heat maps and contact details, IP addresses or geographic locations. You can find more details on this in the Privacy Policy below.
- Storage period: no precise information is known
- Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is Wix?

For our website we use the website construction-kit Wix by the Israeli company Wix.com Ltd., 40 Hanamal Tel Aviv St., Tel Aviv 6350671, Israel. In addition to the headquarters in Tel Aviv, the company also has other headquarters such as in Berlin, Dublin, Vancouver, or New York. Due to the use of Wix, your personal data may be collected, stored and processed. In this privacy policy we want to explain why we use Wix, what data is stored, where your data is stored and how you can prevent data retention. Wix is a website construction-kit that makes it very easy to create HTML5 websites as well as mobile websites. The online platform is based on the cloud principle and allows easy integration of various Wix or third-party provider functions into your own website.

Why do we use Wix on our website?

For working on our website, we need an easy-to-use system, that allows us to present you a beautiful design and interesting content quickly and easily. We have found Wix to be the right system for this. Thanks to both, Wix's easy operation and its extensive functions, we can design our website as we wish, while ensuring its user-friendliness.

What data is stored by Wix?

Non-personal data include for example technical usage information such as browser activity, clickstream activity, session heat maps, as well as data about your computer, operating system, browser, screen resolution, language and keyboard settings, internet provider and date of the page visit. Personal data are also recorded. These are primarily contact details (email address or telephone number, if you have provided them), IP address or your geographical location. Tracking systems such as cookies are used to collect data about your behaviour on our website. For example, it records which sub-pages you take a particular interest in, how much time you spend on individual pages, when you leave a page (bounce rate) or which pre-sets (e.g. language settings) you have made. Based on this data, [Wix.com](https://www.wix.com) can adjust their marketing measures better to your interests and your user behaviour. Therefore, the next time you visit our website, you will get to view it with the settings you have chosen priorly. [Wix.com](https://www.wix.com) may also forward personal data to third parties (such as service providers). Below we will show you a list of exemplary cookies that are placed due to the use of Wix:

Name: XSRF-TOKEN

Value: 1591628008|P01ovn-JtsrK

Purpose: This cookie is a security cookie and prevents the so-called cross-site request forgery, which is an attack on a computer system.

Expiry date: after end of session

Name: _wixCIDX

Value: b2474394-b64f-4c7a-a598-16b9043a8938312451506-9

Purpose: This cookie appropriately stores data when you to log in to our website, to shorten the logon process the following time.

Expiry date: after 3 months

Name: AWSELB

Value: EB626B5A40C80CEFD0EB26286F9684716FECD023880992D31DEC38312451506-1

Purpose: This cookie is used to distribute the website's load across multiple servers. Therefore, the page loading speed gets increased.

Expiry date: after one hour

Name: AWSELBCORS

Value: 85FDC7C91873988D19D2D53305AA8CAB73AF02FCEAEB626B5A40C

Purpose: We have not yet been able to find out more information on this cookie. We will inform you as soon as we know more.

Expiry date: after one hour

Note: Please note that the cookies shown above are examples and that this list does not claim to be exhaustive.

How long and where is the data stored?

Your data can be stored on various servers that are distributed across the globe. For example, the data can be stored in the USA, Ireland, South Korea, Taiwan, or Israel. Wix always stores data until it is no longer required for their provided service. We have not yet been able to find out more about the period the data is stored for.

How can I delete my data or prevent data retention?

You have the option to update, correct or delete your personal data at any time. You can also contact Wix's data protection department directly at privacy@wix.com. To deactivate, delete, or manage cookies you have to select the appropriate settings in your browser. Depending on which browser you use, the cookie settings work a little differently. Under the "Cookies" section you will find the relevant instructions for the most popular browsers. Wix.com Ltd. is headquartered in Israel. The European Commission declared Israel to be a country that provides adequate protection for personal data of EU citizens.

Legal basis

If you have consented to the use of Wix, your consent is the legal basis for the corresponding data processing. According to Art. 6 Paragraph 1 lit. (Consent) your consent is the legal basis for the processing of personal data as may occur when collected by Wix. We also have a legitimate interest in using Wix to optimise our online service and to present our services nicely for you. The corresponding legal basis for this is Art. 6 para. 1 lit. f GDPR (legitimate interests). Nevertheless, we only use Wix if you have given your consent to it. Wix 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 Wix 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://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=en. With this Privacy Policy we have made you familiar with the most important information on data processing by Wix.com. If you want to find out more about it, we recommend you to read the company's Privacy guidelines at <https://www.wix.com/about/privacy>.

Data Processing Agreement (DPA) Wix

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have entered into a Data Processing Agreement (DPA) with Wix. 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 Wix processes personal data on our behalf. It clarifies that Wix 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 at <https://www.wix.com/about/privacy-dpa-users>.

15. 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 graphic under this link](#) 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.

Google Analytics Privacy Policy

Google Analytics Privacy Policy Overview

- Affected parties: website visitors
- Purpose: Evaluation of visitor information to optimise the website.
- Processed data: Access statistics that contain data such as the location of access, device data, access duration and time, navigation behaviour, click behaviour and IP addresses. You can find more details on this in the privacy policy below.
- Storage period: Customizable, GA4 stores data for 14 months by default.
- Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is Google Analytics?

On our website, we use the analytics tracking tool Google Analytics in the Google Analytics 4 (GA4) version provided by the American company Google Inc. For the European region, Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services. Google Analytics collects data about your actions on our website. By combining various technologies such as cookies, device IDs, and login information, you can be identified as a user across different devices. This allows your actions to be analyzed across platforms as well. For example, when you click on a link, this event is stored in a cookie and sent to Google Analytics. With the reports we receive from Google Analytics, we can better tailor our website and service to your needs. In the following, we will provide more information about the tracking tool and specifically inform you about the data processed and how you can prevent it. Google Analytics is a tracking tool used for website traffic analysis. The basis for these measurements and analyses is a pseudonymous user identification number. This number does not include personally identifiable information such as name or address but is used to assign events to a device. GA4 utilizes an event-based model that captures detailed information about user interactions such as page views, clicks, scrolling, and conversion events. Additionally, GA4 incorporates various machine learning features to better understand user behavior and certain trends. GA4 employs modeling through machine learning capabilities, meaning that based on the collected data, missing data can be extrapolated to optimize the analysis and provide forecasts. In order for Google Analytics to function properly, a tracking code is embedded in the code of our website. When you visit our website, this code records various events that you perform on our website. With GA4's event-based data model, we, as website operators, can define and track specific events to obtain analyses of user interactions. This allows us to track not only general information such as clicks or page views but also specific events that are important for our business, such as submitting a contact form or making a purchase. Once you leave our website, this data is sent to and stored on Google Analytics servers. Google processes the data, and we receive reports on your user behavior. These reports can include, among others, the following:

- Audience reports: Audience reports help us get to know our users better and gain a more precise understanding of who is interested in our service.
- Advertising reports: Advertising reports make it easier for us to analyze and improve our online advertising.
- Acquisition reports: Acquisition reports provide helpful information on how we can attract more people to our service.
- Behavior reports: Here, we learn about how you interact with our website. We can track the path you take on our site and which links you click on.
- Conversion reports: Conversion refers to an action you take as a result of a marketing message, such as going from being a website visitor to becoming a buyer or newsletter

subscriber. Through these reports, we gain insights into how our marketing efforts resonate with you, with the aim of improving our conversion rate.

- Real-time reports: With real-time reports, we can see what is currently happening on our website. For example, we can see how many users are currently reading this text.

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

- Event-based data model: This model captures specific events that can occur on our website, such as playing a video, making a purchase, or subscribing to our newsletter.
- Advanced analytics features: With these features, we can gain a better understanding of your behavior on our website or certain general trends. For example, we can segment user groups, conduct comparative analyses of target audiences, or track your path on our website.
- Predictive modeling: Based on the collected data, missing data can be extrapolated through machine learning to predict future events and trends. This can help us develop better marketing strategies.
- Cross-platform analysis: Data collection and analysis are possible from both websites and apps. This enables us to analyze user behavior across platforms, provided you have consented to data processing.

Why do we use Google Analytics on our website?

Our goal with this website is clear: we want to provide you with the best possible service. The statistics and data from Google Analytics help us achieve this goal. The statistically evaluated data gives us a clear picture of the strengths and weaknesses of our website. On one hand, we can optimize our site to make it more easily found by interested people on Google. On the other hand, the data helps us better understand you as a visitor. We know exactly what we need to improve on our website in order to provide you with the best possible service. The data also helps us conduct our advertising and marketing activities in a more personalized and cost-effective manner. After all, it only makes sense to show our products and services to people who are interested in them.

What data is stored by Google Analytics?

With the help of a tracking code, Google Analytics creates a random, unique ID associated with your browser cookie. This way, Google Analytics recognizes you as a new user, and a user ID is assigned to you. When you visit our site again, you are recognized as a "returning" user. All collected data is stored together with this user ID, making it possible to evaluate pseudonymous user profiles. To analyze our website with Google Analytics, a property ID must be inserted into the tracking code. The data is then stored in the corresponding property. For each newly created property, the default is Google Analytics 4 Property. The data storage duration varies depending on the property used. Through identifiers such as cookies, app instance IDs, user IDs, or custom event parameters, your interactions, if you have consented, are measured across platforms. Interactions encompass all types of actions you perform on our website. If you also use other Google systems (such as a Google account), data generated through Google Analytics can be linked to third-party cookies. Google does not disclose Google Analytics data unless we, as website operators, authorize it, except when required by law. According to Google, IP addresses are not logged or stored in Google Analytics 4. However, IP address data is used by Google for deriving location data and is immediately deleted thereafter. All IP addresses collected from users in the EU are deleted before the data is stored in a data center or on a server. Since GA4 focuses on event-based data, the tool uses significantly fewer cookies compared to previous versions such as Google Universal Analytics. However, there are still some specific cookies used by GA4. These can include:

Name: `_ga`

Value: 2.1326744211.152312451506-5

Purpose: By default, analytics.js uses the `_ga` cookie to store the user ID. It is used to distinguish website visitors.

Expiration: After 2 years

Name: `_gid`

Value: 2.1687193234.152312451506-1

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

Expiration: After 24 hours

Name: `gat_gtag_UA`

Value: 1

Purpose: Used to reduce the request rate. If Google Analytics is deployed via Google Tag Manager, this cookie will be named `dc_gtm`.

Expiration: After 1 minute

Note: This list cannot claim to be exhaustive, as Google may change their choice of cookies from time to time. GA4 aims to improve data privacy and offers several options for controlling data collection. For example, we can determine the storage duration ourselves and control data. Here we provide an overview of the main types of data collected by Google Analytics:

- Heatmaps: Google creates heatmaps to show the exact areas you click on. This provides us with information about your interactions on our site.
- Session duration: Google refers to session duration as the time you spend on our site without leaving. If you are inactive for 20 minutes, the session automatically ends.
- Bounce rate: Bounce rate refers to when you view only one page on our website and then leave.
- Account creation: If you create an account or place an order on our website, Google Analytics collects this data.
- Location: IP addresses are not logged or stored in Google Analytics. However, location data is derived shortly before the IP address is deleted.
- Technical information: Technical information includes your browser type, internet service

provider, and screen resolution, among others.

- Source of Origin: Google Analytics is interested in the website or advertisement that brought you to our site.

Additional data may include contact information, reviews, media playback (e.g., if you play a video on our site), sharing of content via social media, or adding to favorites. This list is not exhaustive and serves only as a general guide to the data storage by Google Analytics.

Where and how long are the data stored?

Google has servers distributed worldwide. You can find precise information about the locations of Google data centers at: <https://www.google.com/about/datacenters/locations/?hl=en>. Your data is distributed across multiple physical storage devices. This ensures faster access to data and better protection against manipulation. Each Google data center has emergency programs in place for your data. In the event of hardware failure or natural disasters, the risk of service interruption at Google remains low. The retention period of data depends on the properties used. The storage duration is always set separately for each individual property. Google Analytics offers us four options for controlling the storage duration:

- 2 months: This is the shortest storage period.
- 14 months: By default, data is stored in GA4 for 14 months.
- 26 months: Data can also be stored for 26 months.
- Data is only deleted manually.

In addition, there is also the option for data to be deleted only if you do not visit our website within the selected time period. In this case, the retention period is reset every time you revisit our website within the defined time frame. Once the defined period has expired, the data is deleted once a month. This retention period applies to data linked to cookies, user identification, and advertising IDs (e.g., cookies from the DoubleClick domain). Report results are based on aggregated data and are stored independently of user data. Aggregated data is a combination of individual data into larger units.

How can I delete my data or prevent data storage?

Under the data protection laws of the European Union, you have the right to access, update, delete, or restrict your data. By using the browser add-on to deactivate Google Analytics JavaScript (analytics.js, gtag.js), you can prevent Google Analytics 4 from using your data. You can download and install the browser add-on at: <https://tools.google.com/dlpage/gaoptout?hl=en>. Please note that this add-on only disables data collection by Google Analytics. If you want to disable, delete, or manage cookies in general, you can find the respective instructions for the most common browsers in the "Cookies" section.

Legal basis

The use of Google Analytics requires your consent, which we obtained through our cookie popup. According to Art. 6 (1) (a) of the GDPR, this consent constitutes the legal basis for the processing of personal data that may occur during the collection by web analytics tools. In addition to consent, we also have a legitimate interest in analyzing the behavior of website visitors to improve our offering technically and economically. By using Google Analytics, we can identify website errors, detect attacks, and improve efficiency. The legal basis for this is Art. 6 (1) (f) of the GDPR (legitimate interests). However, we only use Google Analytics if you have given your consent. Google processes data from you, among other things, in the USA. Google is an active participant in the EU-US Data Privacy Framework, which regulates the correct and secure transfer of personal data from EU citizens to the USA. More information can be found at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en. Additionally, Google uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Google commits to maintaining the European data protection level when processing your relevant data, even if the data is stored, processed, and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the decision and the corresponding Standard Contractual Clauses here: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847. You can find the Google Ads Data Processing Terms, which refer to the Standard Contractual Clauses, at: <https://business.safety.google/intl/en/adsprocessorterms/>. We hope we have provided you with the most important information regarding the data processing by Google Analytics. If you want to learn more about the tracking service, we recommend the following links: <https://marketingplatform.google.com/about/analytics/terms/en/> and <https://support.google.com/analytics/answer/6004245?hl=en>. If you want to learn more about data processing, you can refer to the Google Privacy Policy at: <https://policies.google.com/privacy?hl=en>.

Data Processing Agreement (DPA) Google Analytics

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have entered into a Data Processing Agreement (DPA) with Google Analytics. 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 Google Analytics processes personal data on our behalf. It clarifies that Google Analytics 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 Terms under <https://business.safety.google/intl/en/adsprocessorterms/>.

Google Analytics Reports on demographic characteristics and interests

We have turned on Google Analytics' functions for advertising reports. These reports on demographic characteristics and interests contain details about age, gender and interests. Through them we can get a better picture of our users – without being able to allocate any data to individual persons. You can learn more about advertising functions at auf

https://support.google.com/analytics/answer/3450482?hl=en&utm_id=ad. You can terminate the use of your Google Account's activities and information in "Ads Settings" at <https://adssettings.google.com/authenticated> via a checkbox.

Google Analytics Google Signals Privacy Policy

We have activated Google signals in Google Analytics. Through this, any existing Google Analytics functions (advertising reports, remarketing, cross-device reports and reports on interests and demographic characteristics) are updated, to result in the summary and anonymisation of your data, should you have permitted personalised ads in your Google Account. The special aspect of this is that it involves cross-device tracking. That means your data can be analysed across multiple devices. Through the activation of Google signals, data is collected and linked to the Google account. For example, it enables Google to recognise when you look at a product on a smartphone and later buy the product on a laptop. Due to activating Google signals, we can start cross-device remarketing campaigns, which would otherwise not be possible to this extent. Remarketing means, that we can show you our products and services across other websites as well. Moreover, further visitor data such as location, search history, YouTube history and data about your actions on our website are collected in Google Analytics. As a result, we receive improved advertising reports and more useful information on your interests and demographic characteristics. These include your age, the language you speak, where you live or what your gender is. Certain social criteria such as your job, your marital status or your income are also included. All these characteristics help Google Analytics to define groups of persons or target audiences. Those reports also help us to better assess your behaviour, as well as your wishes and interests. As a result, we can optimise and customise our products and services for you. By default, this data expires after 26 months. Please consider, that this data is only collected if you have agreed to personalised advertisement in your Google Account. The retained information is always exclusively summarised and anonymous data, and never any data on individual persons. You can manage or delete this data in your Google Account.

Google Analytics IP Anonymisation

We implemented Google Analytics' IP address anonymisation to this website. Google developed this function, so this website can comply with the applicable privacy laws and the local data protection authorities' recommendations, should they prohibit the retention of any full IP addresses. The anonymisation or masking of IP addresses takes place, as soon as they reach Google Analytics' data collection network, but before the data would be saved or processed. You can find more information on IP anonymisation at <https://support.google.com/analytics/answer/2763052?hl=en>.

16. 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.

Ascend by Wix Privacy Policy

We use Ascend by Wix on our website, which is a service for our email marketing. The service provider is the Israeli company Wix.com Ltd., 40 Namal Tel Aviv Street, Tel Aviv, 6350671 Israel. Ascend by Wix 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 Ascend by Wix 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 Ascend by Wix in the privacy policy at <https://www.wix.com/about/privacy>.

Data Processing Agreement (DPA) Ascend by Wix

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have entered into a Data Processing Agreement (DPA) with Wix. 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 Wix processes personal data on our behalf. It clarifies that Wix 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.wix.com/about/privacy-dpa-users>.

17. Online Marketing

Online Marketing Privacy Policy Overview

- Affected parties: visitors to the website
- Purpose: Evaluation of visitor information for website optimisation
- Processed data: Access statistics containing data such as access location, device data, access duration and time, navigation behaviour, click behaviour and IP addresses. Personal data such as name or email address may also be processed. You can find more details on this from the respective Online Marketing tool.
- Storage period: depending on the Online Marketing tools used
- Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is Online Marketing?

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

Why do we use Online Marketing tools?

We want to show our website to everyone who is interested in our offer. We are aware that

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

Which data are processed?

For our Online Marketing to work and to measure its success, user profiles are created and data are e.g. stored in cookies (small text files). With the help of this data, we can not only advertise in the traditional way, but also present our content directly on our website in the way you prefer. There are various third-party tools that offer these functions and thus collect and store your data accordingly. The aforementioned cookies e.g. store the pages you visit on our website, how long you view these pages, which links or buttons you click or which website you came from. What is more, technical information may also be stored. This may include e.g. your IP address, the browser and device you use to visit our website or the time you accessed our website as well as the time you left. If you have agreed for us to determine your location, we can also store and process it. Your IP address is stored in pseudonymised form (i.e. shortened). What is more, distinct data that directly identify you as a person, such as your name, address or email address, are only stored in pseudonymised for advertising and Online Marketing purposes. With this data we cannot identify you as a person and only retain the pseudonymised information that is stored in your user profile. Under certain circumstances, cookies may also be utilised, analysed and used for advertising purposes on other websites that use the same advertising tools. Thus, your data may then also be stored on the servers of the respective provider of the advertising tool. In rare exceptions, unique data (name, email address, etc.) may also be stored in the user profiles. This can happen, if you are for example a member of a social media channel that we use for our Online Marketing measures and if the network connects previously received data with the user profile. We only ever receive summarised information from the advertising tools we use that do store data on their servers. We never receive data that can be used to identify you as an individual. What is more, the data only shows how well-placed advertising measures have worked. For example, we can see what measures have caused you or other users to visit our website and purchase a service or product. Based on these analyses we can improve our advertising offer in the future and adapt it more precisely to the needs and wishes of people who are interested.

Duration of data processing

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

Right of withdrawal

You also retain the right and the option to revoke your consent to the use of cookies or third-party providers at any time. This can be done either via our cookie management tool or via other opt-out functions. You can for example also prevent data collection by cookies if you manage, deactivate or erase cookies in your browser. The legality of the processing remains unaffected to the point of revocation. Since Online Marketing tools usually use cookies, we also recommend you to read our privacy policy on cookies. If you want to find out which of your data is stored and processed, you should read the privacy policies of the respective tools.

Legal basis

If you have consented to the use of third-party providers, then this consent is the legal basis for the corresponding data processing. According to Art. 6 para. 1 lit. a GDPR (consent), this consent is the legal basis for personal data processing, as may be done when data is collected by online marketing tools. Moreover, we have a legitimate interest in measuring our online marketing activities in anonymised form, in order to use this data for optimising our offer and our Marketing. The corresponding legal basis for this is Art. 6 para. 1 lit. f GDPR (legitimate interests). Nevertheless, we only use these tools if you have given your consent. Information on special online marketing tools can be found in the following sections, provided this information is available.

Google Ads (Google AdWords) Conversion Tracking Privacy Policy

Google Ads (Google AdWords) Conversion Tracking Privacy Policy Overview

- Affected parties: visitors to the website
- Purpose: economic success and service optimisation.
- Processed data: Access statistics that contain data such as access location, device data, access duration and time, navigation behaviour, click behaviour and IP addresses. Personal data such as name or email address may also be processed.
- Storage period: Conversion cookies usually expire after 30 days and do not transmit any personal data
- Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit.f GDPR (legitimate interests)

What is Google Ads conversion tracking?

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

will explain, why we use conversion tracking, what data gets saved and how you can prevent this data retention. Google Ads (previously Google AdWords) is the internal online advertising system of the company Google LLC. We are convinced of our offer's quality and would like as many people as possible to discover our website. For this, Google Ads offers the best platform within the online environment. Of course, we also want to get an overview of the cost-benefit factor of our advertising campaigns. Thence, we use Google Ads' conversion tracking tool. But what is a conversion actually? A conversion occurs, when you turn from an interested visitor into an acting website visitor. This happens every time you click on our ad and then make another action, such as paying a visit to our website. With Google's conversion tracking tool, we can understand what happens after a user clicks our Google ad. It shows us for instance if products get bought, services are used or whether users have subscribed to our newsletter.

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

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

What data is stored with Google Ads conversion tracking?

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

Name: Conversion

Value: EhML_aySuoyv4gIVled3Ch0llweVGAEgt-mr6aXd7dYISAGQ312451506-3

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

Expiry date: after 3 months

Name: _gac

Value:

1.1558695989.EAlalQobChMliOmEgYO04glVj5AYCh2CBAPrEAAAYASAAEglYQfD_BwE

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

Expiry date: after 3 months

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

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

How long and where is the data stored?

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

How can I erase my data or prevent data retention?

You have the possibility to opt out of Google Ads' conversion tracking. The conversion tracking can be blocked by deactivating the conversion tracking cookie via your browser. If you do this, you will not be considered for the statistic of the tracking tool. You can change the cookie settings in your browser anytime. Doing so, works a little different in every browser. Under the "Cookies" section you will find the relevant instructions for the most popular browsers. If you generally do not want to allow any cookies at all, you can set up your browser to notify you whenever a potential cookie is about to be set. This lets you decide upon permitting or denying the cookie's placement. By downloading and installing the browser plugin at <https://support.google.com/ads/answer/7395996> you can also deactivate all "advertising cookies". Please consider that by deactivating these cookies, you cannot prevent all advertisements, only personalised ads.

Legal basis

If you have consented to the use of Google Ads Conversion Tracking, your consent is the

legal basis for the corresponding data processing. According to Art. 6 para. 1 lit. a GDPR (consent), this consent is the legal basis for personal data processing, as may be done when collected by Google Ads Conversion Tracking. We also have legitimate interest in using Google Ads Conversion Tracking to optimise our online service and marketing measures. The corresponding legal basis for this is Art. 6 para. 1 lit. f GDPR (legitimate interests). Nevertheless, we only use Google Ads Conversion Tracking if you have consented to it. Google processes data from you, among other things, in the USA. Google is an active participant in the EU-US Data Privacy Framework, which regulates the correct and secure transfer of personal data from EU citizens to the USA. More information can be found at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en. Additionally, Google uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Google commits to maintaining the European data protection level when processing your relevant data, even if the data is stored, processed, and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the decision and the corresponding Standard Contractual Clauses here: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847 You can find the Google Ads Data Processing Terms, which refer to the Standard Contractual Clauses, at: <https://business.safety.google/intl/en/adsprocessor/terms/> If you would like to find out more about data protection at Google, we recommend Google's privacy policy at: <https://policies.google.com/privacy?hl=en-GB>.

18. External Online Platforms

External Online Platforms Privacy Policy Overview

- Affected parties: website visitors or visitors to the external online platforms
- Purpose: Presentation and optimisation of our service, as well as establishing contact with visitors & interested parties
- Data processed: data such as phone numbers, email addresses, contact details, user behaviour data, information about your device and your IP address. More details can be found directly with the respective platform used.
- Storage duration: depends on the platforms used
- Legal bases: Article 6 paragraph 1 lit. a GDPR (consent), Article 6 paragraph 1 lit. f GDPR (legitimate interests)

What are external online platforms?

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

Why do we use external online platforms?

In addition to our website, we also want to display our offer on other platforms in order to reach more customers. External online marketplaces such as Amazon, eBay or Digistore24 offer large sales websites that show our products to people who may not know our website. Moreover, built-in elements on our site may also lead to an external online platform. Any data that is processed and stored by the respective online platform is used by the business to log the payment process and also to conduct web analyses. The aim of these analyses is to enable the development of more precise and personal marketing and advertising strategies. Depending on your interaction with a platform, the evaluated data may be used to draw appropriate conclusions about your interests and to create a so-called user profile on you. This also allows the platforms to show customised advertisements or products to you. For this purpose, cookies are usually set in your browser in order to store data on your usage behaviour. Please note that when using the platforms or our built-in elements, your data may also be processed outside the European Union, since online platforms such as Amazon or eBay 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 stored and processed depends on the respective external platform. But usually, it is data such as phone numbers, email addresses, data you enter in a contact form, along with user data (e. g. which buttons you click and which pages you view during your visit), as well as information about your device and IP address. In most cases, the majority of this data is stored in cookies. If you have a profile on an external platform and are logged in there, your data can be linked to any such profile. The collected data is stored on the servers of the platforms used, where it is processed. You can find out exactly how an external platform stores, manages and processes data in the respective privacy policy. If you have any questions about data storage and data processing, or if you want to assert corresponding rights, we recommend that you contact the platform directly.

Duration of data processing

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

Right to object

You also have the right and the opportunity to revoke your consent to the use of cookies at

any time. This can be done either via our cookie management tool or via opt-out functions on the respective external platform. You can also prevent data collection through cookies by managing, deactivating or erasing the cookies in your browser. As cookies may be used, we also recommend our general privacy policy on cookies. To find out exactly which of your data is stored and processed, you should read the privacy policies of the respective external platforms.

Legal Basis

If you have consented to your data being processed and stored by external platforms, this consent is the legal basis for data processing (Art. 6 Para. 1 lit. a GDPR). In general, if you have consented, your data will also be stored and processed on the basis of our legitimate interest (Art. 6 Para. 1 lit. f GDPR) in fast and good communication with you as well as other customers and business partners. If there are integrated elements of external platforms on our website, we only use them if you have given your consent. Information on specific external platforms – if available – can be found in the following sections.

Ecwid Privacy Policy

We use Ecwid on our website, which is a cloud commerce platform. The provider of this service is the American company Ecwid, Inc., 687 South Coast Highway 101, Suite 239, Encinitas, California 92024 USA. Ecwid 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. Ecwid 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, Ecwid 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 Standard Contractual Clauses at Ecwid, as well as the data that is processed through the use of the service in their Privacy Policy at <https://www.lightspeedhq.com/legal/privacy-policy/>.

19. 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.

Supervisory authority

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

"supervisory authority" means an independent public authority which is established by a Member State pursuant to Article 51;

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

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.

Supervisory authority concerned

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

- a) the controller or processor is established on the territory of the Member State of that supervisory authority;
 - b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
 - c) a complaint has been lodged with that supervisory authority;
- Explanation: In Germany, each federal state has its own supervisory authority for data

protection. If your company headquarters (head office) is in Germany, your point of contact is the respective supervisory authority of the respective federal state. In Austria there is only one Data Protection Authority for the whole country.

Biometric data

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

- Explanation: They are biological markers that are classified by biometric data and thus hold personal data which can be obtained with the help of technical processes. These include DNA, fingerprints, the geometry of different body parts, body size, but also handwriting or the sound of a voice.

Filing system

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“filing system” means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

- Explanation: Any organised storage of data on a computer's disk is referred to as a “filing system”. For example, if we store your name and email address on a server for our newsletter, this data would be located in a so-called “filing system”. One of the most important tasks of a “filing system” is to quickly be able to search and find specific data and, of course, to store the data securely.

Information society service

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

- Explanation: Basically, the term “information society” refers to a society based on information and communication technologies. As a website visitor, in particular, you are familiar with all kinds of online services. Most online services are classified as “information society services”. A classic example of this is an online transaction, such as buying goods over the Internet.

Third party

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“third party” means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

- Explanation: The GDPR basically only explains what a “third party” is not. In practice, any “third party” who also has an interest in personal data, but not the persons mentioned above, are authorities or institutions. For example, a parent company can act as a “third party”. In this case, the subsidiary company is the controller and the parent company is the “third party”. However, this does not mean that the parent company may automatically view, collect or store personal data of the subsidiary.

Restriction of processing

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“restriction of processing” means the marking of stored personal data with the aim of limiting their processing in the future;

- Explanation: It is part of your rights that you can ask processors at any time to restrict your personal data for further processing operations. For this purpose, certain personal data such as your name, your date of birth or your address are marked in a way to limit further processing. For example, you could restrict processing to prevent your data from being used for personalised advertising.

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.

Recipient

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“recipient” means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the

applicable data protection rules according to the purposes of the processing;

- Explanation: Any person or establishment that receives personal data is considered a recipient. We and our processors are therefore also so-called recipients. Only authorities that have an investigation mandate are not considered recipients.

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.

Data concerning health

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“Data concerning health” means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

- Explanation: Health data includes all stored information relating to your own health. It is often data that is also noted in patient files. This includes, for example, which medication you are using, X-rays, your entire medical history or your vaccination statuses.

Cross-border processing

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means: “Cross-border processing” either

- a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
- b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

- Explanation: If a company or other organisation e. g. has branches in Spain and Croatia where personal data is processed in connection with the branches’ activities, this constitutes “cross-border processing” of personal data. Even if the data is only processed in one country (as in this example in Spain) but the effects for the data subject are also recognisable in another country, it is also considered “cross-border processing”.

Main Establishment

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means: “main establishment”

- a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
- b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

- Explanation: For example, Google is an American establishment that also processes data in the USA, but its European headquarters are in Ireland (Google Ireland Limited, Gordon House, Barrow Street Dublin 4, Ireland) . From a legal point of view, Google Ireland Limited is therefore an independent establishment and is responsible for all Google products offered in the European Economic Area. In contrast to one head office, there are also branches, but these do not function as legally independent branches and must therefore be distinguished from subsidiaries. A head office is always the place where an entity (company) has its centre of operations.

International Organisation

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“international organisation” means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

- Explanation: The best-known examples of international organisations are probably the European Union and the United Nations. In the GDPR, there is a distinction between third countries and international organisations in relation to data transfer. Within the EU, data traffic of personal data does not pose a problem as all EU countries are bound by the provisions of the GDPR. On the other hand, data transfer to third countries or international organisations is subject to certain requirements.

Relevant and reasoned Objection

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“Relevant and reasoned objection” means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

- Explanation: If certain measures we as controllers or our processors take are not in line with the GDPR, you can raise a so-called “relevant and reasoned objection”. In doing so, you must explain the scope of the risks in relation to your fundamental rights and freedoms and, where applicable, the free flow of your personal data in the EU.

Personal Data

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term 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:
 - 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.

Pseudonymisation

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“Pseudonymisation” means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

- Explanation: Our Privacy Policy often refers to pseudonymised data. Pseudonymised data means that this data can no longer be used to identify you as a person unless additional information is added. However, you should not confuse pseudonymisation with anonymisation. With anonymisation, there is no personal reference whatsoever, and the only way to reconstruct it would require a disproportionate amount of technical effort.

Enterprise

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“Enterprise” means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

- Explanation: For example, we are an enterprise and also carry out an economic activity through our website by offering and selling services and/or products. As a formal characteristic, every enterprise has a legal entity such as a GmbH or an AG.

Group of undertakings

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“group of undertakings” means a controlling undertaking and its controlled undertakings;

- Explanation: A “group of companies” is when several companies unite and are legally and financially connected to each other but under a central, superordinate company. For example, while Instagram, WhatsApp, Oculus VR or Facebook are mostly independent companies, they are all controlled by the parent company Meta Platforms, Inc.

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.

Binding corporate rules

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“binding corporate rules” means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

- Explanation: You may have heard or read the term “binding corporate rules” before. This is a term that usually appears when it comes to binding internal data protection regulations. For companies that process data in third countries (e.g. Google), it is sensible to have such an internal regulation, through which a company commits itself to comply with data protection regulations. This regulation regulates the handling of personal data that is transferred to and processed in third countries.

Personal data breach

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

- Explanation: For example, a personal data breach can occur in the event of a data leak, i.e. a technical problem or a cyber attack. If the breach results in a risk to the rights and freedoms of individuals, the data controller must immediately report the incident to the supervisory authority, and the data subjects must be informed if the violation poses a high risk to the rights and freedoms of natural persons.

Representative

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“representative” means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

- Explanation: A “representative” can therefore be any person who has been appointed in writing by us (controller) or one of our service providers (processors). Non-EU companies that process EU citizens’ data must designate a representative within the EU. For example, if a web analytics provider has its headquarters in the United States, it must appoint a “representative” within the European Union to represent its data processing obligations.