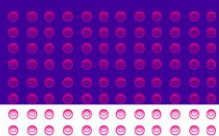


## Table of Content

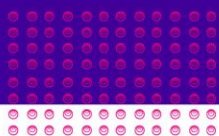
Privacy Policy .....	1
1. General.....	1
2. Legal bases .....	1
2.1 Contact details of the data protection controller .....	2
3. Storage Period.....	2
4. Rights in accordance with the General Data Protection Regulation .....	2
4.1 Austria Data Protection Authority.....	4
5. Security of data processing operations.....	4
5.1 TLS encryption with https .....	4
6. Communications .....	4
6.1 Affected persons.....	5
6.2 Telephone .....	5
6.3 Email.....	5
6.4 Online forms .....	5
6.5 Legal bases.....	6
7. Data Processing Agreement (DPA).....	7
7.1 Who are the processors? .....	7
7.2 Contents of a Data Processing Agreement .....	7
8. Cookies.....	8
8.1 What are cookies? .....	8
8.2 Which types of cookies are there? .....	9
8.3 Purpose of processing via cookies.....	10
8.4 Which data are processed? .....	10
8.5 Storage period of cookies .....	10
8.6 Right of objection - how can I erase cookies?.....	10
8.7 Legal basis .....	11
9. Customer Data .....	11
9.1 What is customer data? .....	11
9.2 Why do we process customer data?.....	12
9.3 What data is processed?.....	12
9.4 How long is the data stored? .....	12
9.5 Legal Basis.....	13
9.6. Withdrawl of consent .....	13



10.	Web hosting .....	13
10.1	What is web hosting?.....	13
10.2	Why do we process personal data?.....	14
10.3	Which data are processed? .....	14
10.4	How long is the data stored?.....	14
10.5	Legal basis .....	14
10.6	Webhosting Other .....	15
11.	Web Analytics.....	15
11.1	What is web analytics?.....	15
11.2	Why do we run web analytics?.....	15
11.3	Which data are processed? .....	16
11.4	Duration of data processing.....	16
11.5	Right to object.....	16
11.6	Legal basis .....	16
11.7	Google Analytics Privacy Policy.....	17
11.7.1	What is Google Analytics?.....	17
11.7.2	Why do we use Google Analytics on our website?.....	19
11.7.3	What data is stored by Google Analytics?.....	19
11.7.4	How long and where is the data stored?.....	20
11.7.5	How can I delete my data or prevent data retention?.....	21
11.7.6	Legal basis.....	21
11.7.7	Data Processing Agreement (DPA) Google Analytics .....	22
11.7.8	Google Analytics in Consent Mode.....	22
11.7.9	Google Analytics IP Anonymisation .....	22
11.8	Google Tag Manager Privacy Policy.....	23
11.8.1	What is Google Tag Manager?.....	23
11.8.2	Why do we use Google Tag Manager for our website?.....	23
11.8.3	What data is stored by Google Tag Manager?.....	24
11.8.4	How long and where is the data stored?.....	24
11.8.5	How can I delete my data or prevent data retention?.....	24
11.8.6	Legal basis.....	24
11.9	Hotjar Privacy Policy.....	25
11.9.1	What is Hotjar?.....	25
11.9.2	Why do we use Hotjar on our website?.....	26



11.9.3	What data is stored by Hotjar?.....	26
11.9.4	How long and where is the data stored?.....	28
11.9.5	How can I erase my data or prevent data retention? .....	28
11.9.6	Legal basis.....	29
12.	Email-Marketing.....	29
12.1	What is Email-Marketing?.....	29
12.2	Why do we use Email-Marketing? .....	30
12.3	Which data are processed? .....	30
12.4	Duration of data processing.....	30
12.5	Withdrawal – how can I cancel my subscription? .....	31
12.6	Legal basis .....	31
12.7	Newsletter – Tool Hubspot.....	31
13.	Social Media Platforms.....	32
13.1	What is Social Media? .....	32
13.2	Why do we use Social Media? .....	32
13.3	Which data are processed? .....	33
13.4	Legal basis .....	33
13.5	Facebook.....	33
13.6	Instagram.....	34
13.7	LinkedIn.....	35
13.8	X (formerly Twitter) .....	35
14.	Online Marketing .....	37
14.1	What is Online Marketing? .....	37
14.2	Why do we use Online Marketing tools? .....	37
14.3	Which data are processed? .....	37
14.4	Duration of data processing.....	38
14.5	Right of withdrawal.....	38
14.6	Legal basis .....	39
14.7	HubSpot privacy policy.....	39
14.8	Facebook Pixel Privacy Policy.....	42
14.9	LinkedIn Insight-Tag Privacy Policy.....	44
15.	Audio & Video.....	45
15.1	What are audio and video elements?.....	45
15.2	Why do we use audio & video elements on our website? .....	46



15.3	Which data are retained by audio & video elements?.....	46
15.4	Duration of data processing.....	46
15.5	Right to object.....	46
15.6	Legal basis.....	47
15.7	Vimeo Privacy Policy.....	47
15.7.1	What is Vimeo?.....	47
15.7.2	Why do we use Vimeo on our website?.....	47
15.7.3	What data is stored on Vimeo?.....	48
15.7.4	How long and where is the data stored?.....	49
15.7.5	How can I erase my data or prevent data retention?.....	49
15.7.6	Legal basis.....	50
15.8	YouTube Privacy Policy.....	50
15.8.1	What is YouTube?.....	51
15.8.2	Why do we use YouTube videos on our website?.....	51
15.8.3	What data is stored by YouTube?.....	51
15.8.4	How long and where is the data stored?.....	53
15.8.5	How can I erase my data or prevent data retention?.....	53
15.8.6	Legal basis.....	54
16.	Security & Anti-spam.....	54
16.1	Google reCAPTCHA.....	54
16.1.1	What is reCAPTCHA?.....	55
16.1.2	Why do we use reCAPTCHA on our website?.....	55
16.1.3	What data is stored by reCAPTCHA?.....	55
16.1.4	How long and where are the data stored?.....	57
16.1.5	How can I erase my data or prevent data retention?.....	57
16.1.6	Legal basis.....	58
17.	Data processing within the context of the internal whistleblowing system.....	59
17.1	Whistleblowing & Ethics Reporting Channel.....	59
17.1.1	What is the Whistleblowing & Ethics Reporting Channel and what data is stored?.....	59
17.1.2	How long and where are the data stored?.....	60
17.1.3	Legal notice:.....	60

# Privacy Policy

## 1. General

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 as gender-neutral. **In short:** We provide you with comprehensive information about any personal data we process about you.

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

## 2. 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:

- **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.
- **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.
- **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.

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

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

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

In **Austria** this is the Austrian Data Protection Act (**Datenschutzgesetz**), in short **DSG**.

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

## 2.1 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

enspired GmbH  
Wagenseilgasse 3  
1120 Vienna

E-Mail: [privacy@enspired-trading.com](mailto:privacy@enspired-trading.com)

## 3. 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.

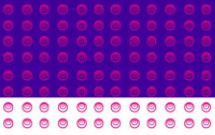
## 4. Rights in accordance with the General Data Protection Regulation

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 GDPR, 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 GDPR, 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.

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/>. The following local data protection authority is responsible for our company:





## 4.1 Austria Data Protection Authority

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

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

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

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

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

## 5. Security of data processing operations

In order to protect personal data, we have implemented both technical and organisational measures. 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.

### 5.1 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.

## 6. 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.

## 6.1 Affected persons

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

## 6.2 Telephone

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

## 6.3 Email

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

## 6.4 Online forms

We use HubSpot, a digital marketing tool, to manage the online forms. Therefore, the data you provide in the online forms is stored by Hubspot. The data will be erased as soon as the business case has ended and the legal requirements allow for its erasure.

Hubspot is a service by the American company HubSpot Inc., 25 First Street, 2nd Floor Cambridge, MA, USA. The responsible entity for the European region is the Irish company HubSpot (1 Sir John Rogerson's Quay, Dublin 2, Ireland).

HubSpot processes data from you, among other things, in the USA. HubSpot 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](https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en).

Additionally, HubSpot 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, HubSpot 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](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847). You can find out more about HubSpot's data processing in their privacy policy at <https://legal.hubspot.com/de/privacy-policy>.

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have entered into a Data Processing Agreement (DPA) with HubSpot. This contract is required by law because HubSpot processes personal data on our behalf. It clarifies that HubSpot may only process data they receive from us according to our instructions and must comply with the GDPR. You can find the link to the Data Processing Agreement (DPA) under <https://legal.hubspot.com/dpa>.

You can also find further information on Hubspot in the [Online Marketing section](#).

## 6.5 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 email programs, Exchange servers and mobile network operators are necessary to efficiently operate our communications.

## 7. 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.

### 7.1 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 interested party or website visitor) → **Controller** (we as a company and contracting entity) → **Processors** (service providers such as web hosts or cloud providers)

### 7.2 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.

## 8. Cookies

### Cookies Overview

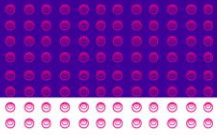
-  Affected parties: visitors to the website
-  Purpose: depending on the respective cookie. You can find out more details below or from the software manufacturer that sets the cookie.
-  Processed data: Depending on the cookie used. More details can be found below or from the manufacturer of the software 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)

### 8.1 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.

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:** GA1.2.1326744211.152112024533-9

**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

## 8.2 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 customized advertisements to the user.

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.

## 8.3 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.

## 8.4 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.

## 8.5 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.

## 8.6 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.

## 8.7 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 of the Telecommunications Act (TKG).






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.

If cookies are used that are not absolutely necessary, this only happens in the case of your consent. 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 service does use cookies.

## 9. 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)

### 9.1 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.

## 9.2 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.

## 9.3 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
- Payment data (invoices, bank details, payment history, etc.)
- Contract data (duration, contents)
- Usage data (websites visited, access data, etc.)
- Metadata (IP address, device information)

## 9.4 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.



## 9.5 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).

## 9.6. Withdrawal of consent

In the case you have given us consent to process your data you can withdraw this consent at any time under [privacy@enspired-trading.com](mailto:privacy@enspired-trading.com).

## 10. Web hosting

### Web hosting Overview

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

### 10.1 What is web hosting?

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

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

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

Whenever the browser on your computer establishes a connection (desktop, laptop, smartphone) and whenever data is being transferred to and from the web server, personal

data may be processed. After all, your computer stores data, and the web server also has to retain the data for a period of time in order to ensure it can operate properly.

## 10.2 Why do we process personal data?

The purposes of data processing are:

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

## 10.3 Which data are processed?

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

- the full address (URL) of the accessed website (e. g. <https://www.examplepage.uk/examplesubpage.html?tid=112024533>)
- browser and browser version (e.g. Chrome 87)
- the operating system used (e.g. Windows 10)
- the address (URL) of the previously visited page (referrer URL) (e. g. <https://www.examplepage.uk/icamefromhere.html/>)
- the host name and the pseudonymised IP address of the device from the website is being accessed from (e.g. COMPUTERNAME and 194.23.43.121)
- the system the visitor uses
- date and time

in so-called web server log files.

## 10.4 How long is the data stored?

Generally, the data mentioned above are stored for 14 days and are then automatically deleted. We do not pass these data on to others, but we cannot rule out the possibility that this data may be viewed by the authorities in the event of illegal conduct.

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

## 10.5 Legal basis

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

## 10.6 Webhosting Other






Contact data for our Webhosting:

EOR Digital GmbH  
Herminengasse 8/2B  
1020 Wien

You can learn more about the data processing at this provider in their [Privacy Policy](#).

## 11. 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)

### 11.1 What is web analytics?

We use web analytics software on our website, in order to evaluate website visitor behavior. Thus, data is collected, which the analytic tool provider (also called tracking tool) stores, manages and processes. Analyses of user behavior on our website are created with this data, which we as the website operator receive. For such analyses, user profiles are created and the respective data is stored in cookies.

### 11.2 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 behavior of our website visitors, and then improve our website accordingly for you and for us. For example, we can see, where visitors 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.



### 11.3 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 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.

### 11.4 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.

### 11.5 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.

### 11.6 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.

## 11.7 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 and click behaviour. You can find more details on this in the privacy policy below
-  Storage period: 14 months
-  Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

#### 11.7.1 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.

Once you leave our website, this data is sent to and stored on Google Analytics servers.

Google processes this data and we then receive reports on your user behaviour. These reports can be one of 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.



### 11.7.2 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.

### 11.7.3 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.

The following cookies are used by Google Analytics:

**Name:** \_ga

**Value:**2.1326744211.152112024533-5

**Purpose:** By default, analytics.js uses the cookie \_ga, to save the user ID. It generally serves the purpose of differentiating between website visitors.

**Expiration date:** After 2 years

**Name:** \_gid

**Value:**2.1687193234.152112024533-1

**Purpose:** This cookie also serves the purpose of differentiating between website users

**Expiration date:** After 24 hours





**Name:** \_gat\_gtag\_UA\_<property-id>

**Value:** 1

**Purpose:** It is used for decreasing the demand rate. If Google Analytics is provided via Google Tag Manager, this cookie gets the name \_dc\_gtm\_ <property-id>.

**Expiration date:** After 1 minute

**Note:** This list is by no means exhaustive, since Google are repeatedly changing the use of their cookies.

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:** Google Analytics is interested in the website or advertisement that brought you to our site.

Further possibly stored data include contact data, potential reviews, playing media (e.g. when you play a video on our site), sharing of contents via social media or adding our site to your favourites. This list is not exhaustive and only serves as general guidance on Google Analytics' data retention. To see the full list visit:

<https://support.google.com/analytics/answer/11593727?hl=en>

#### 11.7.4 How long and where is 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/inside/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.
- 

We chose a deletion after **14 months**.

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.

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

Under the provisions of the European Union's data protection law, you have the right to obtain information on your data and to update, delete or restrict it. With the help of a browser add on that can deactivate Google Analytics' JavaScript (ga.js, analytics.js, dc.js), you can prevent Google Analytics 4 from using your data. You can download this add on at <https://tools.google.com/dlpage/gaoptout?hl=en-GB>. Please consider that this add on can only deactivate any 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.

#### 11.7.6 Legal basis

The use of Google Analytics requires your consent, which we obtained via our cookie popup. According to **Art. 6 para. 1 lit. a of the GDPR (consent)**, this is the legal basis for the processing of personal data when collected via 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](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](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>.

### 11.7.7 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 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 Agreement (DPA) under <https://business.safety.google/intl/en/adsprocessorterms/>.

### 11.7.8 Google Analytics in Consent Mode

Depending on your consent, Google Analytics will process your personal data in the so-called “consent mode”. You can choose whether or not you want to accept Google Analytics cookies, and thus which of your data Google Analytics may process. The retained data is mainly used to measure user behaviour on the website, to serve targeted advertising and to provide us with web analysis reports. Usually, you would consent to Google’s data processing via a cookie consent tool. If you do not consent to data processing, only aggregated data will be collected and processed. This means that data cannot be assigned to individual users and therefore no user profile will be created for you. You also have the option to only agree to statistical measurement, meaning that none of your personal data will be processed and used for advertising or advertising measurement sequences.






### 11.7.9 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>.

## 11.8 Google Tag Manager Privacy Policy

### Google Tag Manager Privacy Policy Overview

-  Affected parties: website visitors
-  Purpose: Organization of individual tracking tools
-  Processed data: Google Tag Manager itself does not store any data. The data record tags of the web analytics tools used.
-  Storage period: depending on the web analytics tool used
-  Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

### 11.8.1 What is Google Tag Manager?

We use Google Tag Manager by the company Google Inc. (1600 Amphitheatre Parkway Mountain View, CA 94043, USA) for our website. This Tag Manager is one of Google's many helpful marketing products. With it, we can centrally integrate and manage code sections of various tracking tools, that we use on our website.

In this privacy statement we will explain in more detail, what Google Tag Manager does, why we use it and to what extent your data is processed.

Google Tag Manager is an organising tool with which we can integrate and manage website tags centrally and via a user interface. Tags are little code sections which e.g. track your activities on our website. For this, segments of JavaScript code are integrated to our site's source text. The tags often come from Google's intern products, such as Google Ads or Google Analytics, but tags from other companies can also be integrated and managed via the manager. Since the tags have different tasks, they can collect browser data, feed marketing tools with data, embed buttons, set cookies and track users across several websites.

### 11.8.2 Why do we use Google Tag Manager for our website?

Everybody knows: Being organised is important! Of course, this also applies to maintenance of our website. In order to organise and design our website as well as possible for you and anyone who is interested in our products and services, we rely on various tracking tools, such as Google Analytics. The collected data shows us what interests you most, which of our services we should improve, and which other persons we should also display our services to. Furthermore, for this tracking to work, we must implement relevant JavaScript Codes to our website. While we could theoretically integrate every code section of every tracking tool separately into our source text, this would take too much time and we would lose overview. This is the

reason why we use Google Tag Manager. We can easily integrate the necessary scripts and manage them from one place. Additionally, Google Tag Manager's user interface is easy to operate, and requires no programming skills. Therefore, we can easily keep order in our jungle of tags.

### 11.8.3 What data is stored by Google Tag Manager?

Tag Manager itself is a domain that neither uses cookies nor stores data. It merely functions as an "administrator" of implemented tags. Data is collected by the individual tags of the different web analysis tools. Therefore, in Google Tag Manager the data is sent to the individual tracking tools and does not get saved.

However, with the integrated tags of different web analysis tools such as Google Analytics, this is quite different. Depending on the analysis tool used, various data on your internet behaviour is collected, stored and processed with the help of cookies. Please read our texts on data protection for more information on the articular analysis and tracking tools we use on our website.

We allowed Google via the account settings for the Tag Manager to receive anonymised data from us. However, this exclusively refers to the use of our Tag Manager and not to your data, which are saved via code sections. We allow Google and others, to receive selected data in anonymous form. Therefore, we agree to the anonymised transfer of our website data. However, even after extensive research it can't be said what summarised and anonymous data it is exactly that gets transmitted. What we do know is that Google deleted any info that could identify our website. Google combines the data with hundreds of other anonymous website data and creates user trends as part of benchmarking measures. Benchmarking is a process of comparing a company's results with the ones of competitors. As a result, processes can be optimised based on the collected information.

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

When Google stores data, this is done on Google's own servers. These servers are located all over the world, with most of them being in America. At <https://www.google.com/about/datacenters/inside/locations/?hl=en> you can read in detail where Google's servers are.

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

Google Tag Manager itself does not set any cookies but manages different tracking websites' tags. In our "Cookies" section you can find detailed information on how you can delete or manage your data.

### 11.8.6 Legal basis

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





In addition to consent, we have a legitimate interest in analysing the behaviour of website visitors and thus technically and economically improving our offer. With the help of Google Tag Managers we can also improve profitability. The legal basis for this is **Art. 6 para. 1 lit. f GDPR (legitimate interests)**. We only use Google Tag Manager if you have given us 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](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](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847).

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

If you want to learn more about Google Tag Manager, we recommend their FAQs at <https://support.google.com/tagmanager/?hl=en#topic=3441530>.

## 11.9 Hotjar Privacy Policy

### Hotjar Privacy Policy Overview

-  Affected parties: website visitors
-  Purpose: To evaluate visitor information for optimising user experience.
-  Processed data: Access statistics that contain data such as access location, device data, access duration and time, navigation behaviour, click behaviour and IP addresses.
-  Storage period: the data will be deleted after one year
-  Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

#### 11.9.1 What is Hotjar?

We use Hotjar of the company Hotjar Limited (Level 2, St Julian's Business Centre, 3, Elia Zammit Street, St Julian's STJ 1000, Malta) on our website, to statistically evaluate visitor data. Hotjar is a service which analyses the behaviour and feedback of you as a user of our website by combining analysis and feedback tools. We receive reports as well as visual displays from Hotjar, which show us how you move on our site. Personal data is anonymised automatically and never reaches Hotjar's servers. This means you as the

website user are not personally identified, while we can still learn much about your user behaviour.

As mentioned in the above paragraph, Hotjar helps us analyse the behaviour of our site visitors. Some of the tools Hotjar offers are e.g. heatmaps, conversion funnels, visitor recording, incoming feedback, feedback polls and surveys (you can find more information about it at <https://www.hotjar.com/>). Therewith, Hotjar helps us to provide you a better user experience as well as an improved service. On the one hand it offers good analysis of online behaviour and on the other hand it gives us good feedback on our website's quality. Besides the analytical aspects we of course also want to know your opinion about our website. This is possible thanks to the feedback tool.

### 11.9.2 Why do we use Hotjar on our website?

Within the last years the importance of websites' user experience has gained in importance. And justifiably so – a website should be structured in a way that makes the user feel comfortable and is easy to navigate. Thanks to Hotjar's analysis and the feedback tools, we can make our website and our offer more attractive. To us, Hotjar's Heatmaps has proven particularly valuable, as it helps with presenting and visualising data. In that sense, Hotjar's Heatmaps e.g. helps us to see on which section of the page you click, and where you scroll to.

### 11.9.3 What data is stored by Hotjar?

Hotjar automatically collects information on your user behaviour while you surf our website. In order to be able to collect this information, we implemented a tracking code. We integrated a tracking code, to be able to collect this information. The following data can be gathered via your computer or your browser:

- Your computer's IP address (is collected and saved in an anonymous format)
- Screen size
- Browser information (which browser and version etc.)
- Your location (but only the country)
- Your language preference
- Visited websites (subpages)
- Date and time of access to one of our subpages (websites)

Moreover, cookies also save data that have been placed on your computer (mostly your browser), although no personal data is collected. Generally, Hotjar does not pass collected data to third parties. However, Hotjar explicitly emphasises that it is sometimes necessary to share data with Amazon Web Services. \_ parts of your information is saved on its servers. Nonetheless, Amazon is bound to a confidentiality obligation and cannot disclose these data.

Only a limited number of people (employees of Hotjar) have access to the stored information. Furthermore, Hotjar's servers are protected by firewalls and IP restrictions (only authorised IP addresses have access). Firewalls are security systems which protect

computers from unwanted network accesses. They serve as barriers between Hotjar's secure internal network and the internet. Moreover, Hotjar also uses third-party companies for their services, such as Google Analytics or Optimizely. These firms can also save information that your browser sends to our website.

The following cookies are used by Hotjar. Since we refer to the cookie list in Hotjar's privacy statement at <https://www.hotjar.com/legal/policies/cookie-information>, not every cookie has a sample value. The list shows examples of utilised Hotjar cookies and does not claim to be exhaustive.

**Name:** ajs\_anonymous\_id

**Value:** %2258832463-7cee-48ee-b346-a195f18b06c3%22112024533-5

**Purpose:** This cookie is generally used for analysis purposes and helps with counting our website's visitors by tracking whether they have been to the website before.

**Expiry date:** after one year

**Name:** ajs\_group\_id

**Value:** 0

**Purpose:** This cookie collects data on user behaviour. Based on the similarities between website visitors, the data can then be assigned to a specific visitor group.

**Expiry date:** after one year

**Name:** \_hjid

**Value:** 699ffb1c-4bfb-483f-bde1-22cfa0b59c6c1

**Purpose:** This cookie is used to maintain a Hotjar user ID, which is unique for the website in the browser. That way, upon the next website visits, the user behaviour can be assigned to the same user ID.

**Expiry date:** after one year

**Name:** \_hjMinimizedPolls

**Value:** 462568112024533-8 1

**Purpose:** Every time you minimise a feedback poll widget, Hotjar sets this cookie. It ensures that the widget stays minimised when you surf our sites.

**Expiry date:** after one year

**Name:** \_hjIncludedInSample

**Value:** 1

**Purpose:** This session cookie is used to inform Hotjar if you are part of the selected individuals (sample), who are used for the creation of funnels.

**Expiry date:** after one year

**Name:** \_hjClosedSurveyInvites

**Purpose:** This cookie is set when you see an invitation to a feedback poll in a popup window. It is used to ensure that this invitation appears to you only once.

**Expiry date:** after one year





**Name:** \_hjDonePolls

**Purpose:** This cookie is set in your browser whenever you finish a round of questions for feedback in a poll widget. Therewith, Hotjar prevents you from receiving the same polls in the future.

**Expiry date:** after one year

**Name:** \_hjDoneTestersWidgets

**Purpose:** This cookie is used when you enter your data in the “recruit user tester” widget. With this widget we want to engage you as a tester. The cookie is used to prevent the form from reappearing repeatedly.

**Expiry date:** after one year

**Name:** \_hjMinimizedTestersWidgets

**Purpose:** This cookie is set to keep the “recruit user tester“ widget minimised accross all our pages. The cookie is set upon you minimising this widget once.

**Expiry date:** after one year

**Name:** \_hjShownFeedbackMessage

**Purpose:** This cookie is set if you minimise or amend the given feedback. This is done so the feedback is instantly loaded as minimised when you navigate to another page, on which it is displayed.

**Expiry date:** after one year

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

We integrated a tracking code to our website, which is transmitted to Hotjar’s servers in Ireland (EU). This tracking code contacts Hotjar’s servers and sends a script to your computer or any terminal device with which you are accessing our website. The script collects certain data concerning your interaction with our website. Then, the data is sent to Hotjar’s servers for processing. Moreover, Hotjar imposed a limit of retaining data for up to 365 days on itself. This means that all data collected by Hotjar which is over one year old are deleted automatically.

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

Hotjar saves none of your personal data for its analysis. The company even advertises with the slogan “We track behaviour, not individuals“. In addition, it is always possible for you to prevent the collection of your data. For this you simply need to visit Hotjar’s [“Opt-out page”](#) and click on “deactivate Hotjar”. Please note that deleting cookies, using your browser’s private mode or utilising a different browser will result in the collection of data again. Furthermore, you can activate the “Do Not Track” button in your browser. To do this in Chrome for example, you must click on the three bars and select “Settings”. In the section “Data Protection“ you will find the option “Send a ‘Do Not Track’ request with your browsing traffic”. Finally, you must click on this button and no data will be collected by Hotjar.



### 11.9.6 Legal basis






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

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

You can find more details on the privacy policy and on what data Hotjar uses and how it is utilised at <https://www.hotjar.com/legal/policies/privacy?tid=112024533>.

## 12. 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)

### 12.1 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 (e.g. 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.

## 12.2 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. 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.

## 12.3 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 Web-Hosting 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.

## 12.4 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 by e-mailing us at [privacy@enspired-trading.com](mailto:privacy@enspired-trading.com). 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.

## 12.5 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.

## 12.6 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 174 of the Telecommunications Act 2021 (TKG) provided you have become our customer and have not objected to the use of your email address for direct mail.

## 12.7 Newsletter – Tool Hubspot

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

HubSpot processes data from you, among other things, in the USA. HubSpot 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](https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en).






Additionally, HubSpot 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, HubSpot 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](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847). You can find out more about HubSpot's data processing in their privacy policy at <https://legal.hubspot.com/de/privacy-policy>.

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have entered into a Data Processing Agreement (DPA) with HubSpot. This contract is required by law because HubSpot processes personal data on our behalf. It clarifies that HubSpot may only process data they receive from us according to our instructions and must comply with the GDPR. You can find the link to the Data Processing Agreement (DPA) under <https://legal.hubspot.com/dpa>.

You can also find further information on Hubspot in the [Online Marketing section](#).

## 13. Social Media Platforms

### Social Media Privacy Policy Overview

-  Affected parties: platform website visitors
-  Purpose: Service presentation and optimisation, staying in contact with visitors, interested parties, etc. as well as advertising
-  Processed data: data such as telephone numbers, email addresses, contact data, data on user behaviour, information about your device and your IP address.  
You can find more details on this directly at the respective social media tool used.
-  Storage period: depending on the social media platforms used
-  Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

### 13.1 What is Social Media?

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

### 13.2 Why do we use Social Media?

For years, social media platforms have been the place where people communicate and get into contact online. The social media elements shown on our website help you switch to our social media content quickly and hassle free.

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

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

Please note that when you use social media platforms your data may also be processed outside the European Union, as many social media platforms, such as Facebook or Instagram or X (formerly Twitter) are American companies. As a result, you may no longer be able to easily claim or enforce your rights regarding your personal data.

### 13.3 Which data are processed?

Exactly which data are stored and processed depends on the respective provider of the social media platform. But usually it is data such as telephone numbers, email addresses, data you enter in contact forms, user data such as which buttons you click, what you like or who you follow, when you visited which pages, as well as information about your device and IP address. Most of this data is stored in cookies. Should you have a profile on the social media channel you are visiting and are logged in, data may be linked to your profile. All data that are collected via social media platforms are also stored on the providers' servers. This means that only the providers have access to the data and can provide you with appropriate information or make changes for you.

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

### 13.4 Legal basis

Your data is stored and processed on the basis of our legitimate interest (Art. 6 para. 1 lit. f GDPR) in fast and good communication with you and other customers and business partners via social media platforms.

Any processing operations beyond this, such as the analysis of behavior on the social media portals with or without a personal login, are the responsibility of the providers of the social media portals themselves. Please inform yourself about the types of data being processed, the legal basis for these processes, and their purposes from the providers themselves. Most social media platforms also set cookies on your browser to store data. We therefore recommend you to read our privacy policy on cookies carefully and to take a look at the privacy policy or cookie policy of the respective service provider.

### 13.5 Facebook

We use the social media platform Facebook (Facebook fan page). The provider of this service is the American company Meta Platforms Inc. The responsible entity for the European area is the company Meta Platforms Ireland Limited (4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland).

Facebook processes data from you, among other things, in the USA. Facebook respectively Meta Platforms 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](https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en).

Additionally, Facebook 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, Facebook 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](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847).

Our joint commitments were also set out in a publicly available agreement at [https://www.facebook.com/legal/controller\\_addendum](https://www.facebook.com/legal/controller_addendum)

Facebook's data processing terms, which correspond to the Standard Contractual Clauses, can be found at <https://www.facebook.com/legal/terms/dataprocessing>.

You can find out more about the data that is processed by using Facebook in their Privacy Policy at <https://www.facebook.com/about/privacy> and their cookie guidelines at <https://www.facebook.com/policy/cookies/>.

## 13.6 Instagram

We use the social media platform Instagram. Instagram is a social media platform of the company Instagram LLC, 1601 Willow Rd, Menlo Park CA 94025, USA. Since 2012, Instagram is a subsidiary company of Facebook Inc. and is a part of Facebook's products.

Instagram processes data from you, among other things, in the USA. Instagram respectively Meta Platforms 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](https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en).

Additionally, Instagram 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, Instagram 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](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847).

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

The cookie guideline is the same as for Facebook, visit <https://www.facebook.com/policy/cookies/> for further information.

### 13.7 LinkedIn

We use the social media platform LinkedIn, of the LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA. Moreover, LinkedIn Ireland Unlimited Company Wilton Place in Dublin is responsible for data processing in the European Economic Area and Switzerland.

LinkedIn also processes data in the United States, among other countries. Currently LinkedIn is not a participant of the [Data Privacy Framework Program](#). We would like to note, that US companies that do not participate in the Data Privacy Framework Program are not certified by the European Commission as having an adequate level of data protection. This can be associated with various risks to the legality and security of data processing. More information can be found at [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_23\\_3752](https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752) as well at [https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf\\_en](https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en).

LinkedIn uses standard contractual clauses approved by the EU Commission as the basis for data processing by recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, and especially in the USA) or data transfer there (= Art. 46, paragraph 2 and 3 of the GDPR). These clauses oblige LinkedIn to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses here: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

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

We have entered a Data Processing Agreement (DPA) with LinkedIn in accordance with Article 28 of the General Data Protection Regulation (GDPR). In our general section "Data Processing Agreement (DPA)" you can find out what a DPA is exactly and what it must contain.

This agreement is a legal requirement as LinkedIn processes personal data on our behalf. It clarifies that LinkedIn may only process any data they receive from us according to our instructions and in compliance with the GDPR. You can find the link to the Data Processing Agreement (DPA) at <https://www.linkedin.com/legal/l/dpa?>.

### 13.8 X (formerly Twitter)

We use X, a short message service and social media platform from the firm Twitter International Unlimited Company., One Cumberland Place, Fenian Street, Dublin 2 D02 AX07, Ireland.

In their Privacy Policy, X repeatedly emphasizes that they do not save data from external website visits, provided you or your browser are in the European Economic Area or



Switzerland. However, if you interact directly with X, the company will of course store your data.






X also processes data in the United States, among other countries. Currently X is not a participant of the [Data Privacy Framework Program](#). We would like to note, that US companies that do not participate in the Data Privacy Framework Program are not certified by the European Commission as having an adequate level of data protection. This can be associated with various risks to the legality and security of data processing. More information can be found at [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_23\\_3752](https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752) as well at [https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf\\_en](https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en).

X uses standard contractual clauses, which are approved by the EU Commission, as the basis for data processing by recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway and especially in the USA) or data transfers there (= Art. 46, paragraphs 2 and 3 of the GDPR). These clauses oblige X to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses here: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

We hope we could give you a basic overview of X's data processing. We do not receive any data from X and are not responsible for what X does with your data. If you have any further questions on this topic, we recommend you to read X's privacy statement at <https://twitter.com/en/privacy>.

## 14. 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)

### 14.1 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.

### 14.2 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.

### 14.3 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.

#### 14.4 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.

#### 14.5 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.



## 14.6 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.

## 14.7 HubSpot privacy policy

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

We use HubSpot to understand the behavior of our website visitors better. Therefore Hubspot sets a number of tracking cookies when a visitor lands on our website. In the following we will show you the cookies, which are set by Hubspot.

**Necessary cookies** - These are essential cookies that do not require consent.

**Name:** `_hs_opt_out`

**Value:** "yes" or "no"

**Purpose:** This cookie is used by the opt-in privacy policy to remember not to ask the visitor to accept cookies again.

**Expiration date:** It expires in 6 months.

**Name:** `__hs_do_not_track`

**Value:** "yes"

**Purpose:** This cookie can be set to prevent the tracking code from sending any information to HubSpot.

**Expiration date:** It expires in 6 months.

**Name:** `__hs_initial_opt_in`

**Value:** "yes" or "no"

**Purpose:** This cookie is used to prevent the banner from always displaying when visitors are browsing in strict mode.

**Expiration date:** It expires in seven days.

**Name:** `__hs_cookie_cat_pref`

**Value:** It contains data on the consented categories.



**Purpose:** This cookie is used to record the categories a visitor consented to.

**Expiration date:** It expires in 6 months.

**Name:** `hs_ab_test`

**Value:** It contains the id of the A/B test page and the id of the variation that was chosen for the visitor.

**Purpose:** This cookie is used to consistently serve visitors the same version of an A/B test page they've seen before.

**Expiration date:** It expires at the end of the session.

**Name:** `<id>_key`

**Value:** The cookie name is unique for each password-protected page. It contains an encrypted version of the password so future visits to the page will not require the password again.

**Purpose:** When visiting a password-protected page, this cookie is set so future visits to the page from the same browser do not require login again

**Expiration date:** It expires in 14 days.

**Name:** `hs-messages-is-open`

**Value:** It contains a boolean value of True if present

**Purpose:** This cookie is used to determine and save whether the chat widget is open for future visits. It is set in your visitor's browser when they start a new chat, and resets to re-close the widget after 30 minutes of inactivity. If your visitor manually closes the chat widget, it will prevent the widget from re-opening on subsequent page loads in that browser session for 30 minutes.

**Expiration date:** It expires in 30 minutes

**Name:** `hs-messages-hide-welcome-message`

**Value:** It contains a boolean value of True or False.

**Purpose:** This cookie is used to prevent the chat widget welcome message from appearing again for one day after it is dismissed.

**Expiration date:** It expires in one day.

**Name:** `__hsmem`

**Value:** It contains encrypted data that identifies the membership user when they are currently logged in.

**Purpose:** This cookie is set when visitors log in to a HubSpot-hosted site.

**Expiration date:** It expires in one year.

**Name:** `hs-membership-csrf`

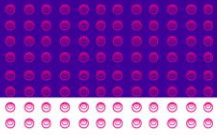
**Value:** It contains a random string of letters and numbers used to verify that a membership login is authentic.

**Purpose:** This cookie is used to ensure that content membership logins cannot be forged.

**Expiration date:** It expires at the end of the session.

**Name:** `hs_langswitcher_choice`

**Value:** It contains a colon delimited string with the ISO639 language code choice on the



left and the top level private domain it applies to on the right. An example will be "EN-US:hubspot.com".

**Purpose:** This cookie is used to save a visitor's selected language choice when viewing pages in multiple languages. It is set when a visitor selects a language from the language switcher and is used as a language preference to redirect them to sites in their chosen language in the future if they are available.

**Expiration date:** It expires in two years.

**Name:** `__cfuid`

**Purpose:** This cookie is set by HubSpot's Content Delivery Network provider because of their rate limiting policies. Learn more about [Cloudflare cookies](#).

**Expiration date:** It expires at the end of the session.

**Name:** `__cf_bm`

**Purpose:** This cookie is set by HubSpot's CDN provider and is a necessary cookie for bot protection. Learn more about [Cloudflare cookies](#).

**Expiration date:** It expires in 30 minutes.

**Analytics cookies** - These are non-essential cookies controlled by the cookie banner. If you're a visitor to a site supported by HubSpot, you can opt out of these cookies by not giving consent.

**Name:** `__hstc`

**Value:** It contains the domain, utk, initial timestamp (first visit), last timestamp (last visit), current timestamp (this visit), and session number (increments for each subsequent session).

**Purpose:** The main cookie for tracking visitors.

**Expiration date:** It expires in 6 months:

**Name:** `hubspotutk`

**Value:** It contains an opaque GUID to represent the current visitor.

**Purpose:** This cookie keeps track of a visitor's identity. It is passed to HubSpot on form submission and used when deduplicating contacts.

**Expiration date:** It expires in 6 months.

**Name:** `__hssc`

**Value:** It contains the domain, viewCount (increments each pageView in a session), and session start timestamp.

**Purpose:** This cookie keeps track of sessions. This is used to determine if HubSpot should increment the session number and timestamps in the `_hstc` cookie

**Expiration date:** It expires in 30 minutes.

**Name:** `__hssrc`

**Value:** It contains the value "1" when present.

**Purpose:** Whenever HubSpot changes the session cookie, this cookie is also set to determine if the visitor has restarted their browser. If this cookie does not exist when



HubSpot manages cookies, it is considered a new session.

**Expiration date:** It expires at the end of the session.

**Note:** We do not claim for this list to be extensive, as Hubspot may change the choice of their cookies.

HubSpot processes data from you, among other things, in the USA. HubSpot 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](https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en).

Additionally, HubSpot 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, HubSpot 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](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847). You can find out more about HubSpot's data processing in their privacy policy at <https://legal.hubspot.com/de/privacy-policy>.

In accordance with Article 28 of the General Data Protection Regulation (GDPR), we have entered into a Data Processing Agreement (DPA) with HubSpot. This contract is required by law because HubSpot processes personal data on our behalf. It clarifies that HubSpot may only process data they receive from us according to our instructions and must comply with the GDPR. You can find the link to the Data Processing Agreement (DPA) under <https://legal.hubspot.com/dpa>.

## 14.8 Facebook Pixel Privacy Policy

We use Meta's Facebook pixel on our website. The provider of this service is the American company Meta Platforms Inc. The responsible entity for the European area is the company Meta Platforms Ireland Limited (4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland).

For that, we have implemented a code on our website. The Facebook pixel is a segment of a JavaScript code, which, in case you came to our website via Facebook ads, loads an array or functions that enable Facebook to track your user actions in one or more cookies. These cookies enable Facebook to match your user data (customer data such as IP address, user ID) with the data of your Facebook account. After that, Facebook deletes your data again. The collected data is anonymous as well as inaccessible and can only be used for ad placement purposes. If you are a Facebook user and you are logged in, your visit to our website is automatically assigned to your Facebook user account.

We exclusively want to show our products or services to persons, who are interested in them. With the aid of the Facebook pixel, our advertising measures can get better adjusted





to your wishes and interests. Therefore, Facebook users get to see suitable advertisement (if they allowed personalised advertisement). Moreover, Facebook uses the collected data for analytical purposes and for its own advertisements.

In the following we will show you the cookies, which were set on a test page with the Facebook pixel integrated to it. Please consider that these cookies are only examples. Depending on the interaction that is made on our website, different cookies are set.

**Name:** \_fbp

**Value:** fb.1.1568287647279.257405483-6112024533-7

**Purpose:** Facebook uses this cookie to display advertising products.

**Expiration date:** after 3 months

**Name:** fr

**Value:** 0aPf312HOS5Pboo2r..Bdeiuf...1.0.Bdeiuf.

**Purpose:** This cookie is used for Facebook pixels to function properly.

**Expiration date:** after 3 months

**Name:** comment\_author\_50ae8267e2bdf1253ec1a5769f48e062112024533-3

**Value:** Name of the author

**Purpose:** This cookie saves the text and name of a user who e.g. leaves a comment.

**Expiration date:** after 12 months

**Name:** comment\_author\_url\_50ae8267e2bdf1253ec1a5769f48e062

**Value:** https%3A%2F%2Fwww.testseite...%2F (URL of the author)

**Purpose:** This cookie saved the URL of the website that the user types into a text box on our website.

**Expiration date:** after 12 months

**Name:** comment\_author\_email\_50ae8267e2bdf1253ec1a5769f48e062

**Value:** email address of the author

**Purpose:** This cookie saves the email address of the user, if they provided it on the website.

**Expiration date:** after 12 months

**Note:** The above-mentioned cookies relate to an individual user behaviour. Moreover, especially concerning the usage of cookies, changes at Facebook can never be ruled out.

If you are registered on Facebook, you can change the settings for advertisements yourself at <https://www.facebook.com/privacy/center>.

If you are not a Facebook user, you can manage your user based online advertising at <https://www.youronlinechoices.com/uk/your-ad-choices>. You have the option to activate or deactivate any providers there.

Facebook processes data from you, among other things, in the USA. Facebook respectively Meta Platforms 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](https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en).

Additionally, Facebook 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, Facebook 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](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847).

The Facebook Data Processing Term, which references the Standard Contractual Clauses, can be found at <https://www.facebook.com/legal/terms/dataprocessing>.

If you want to learn more about Facebook's data protection, we recommend you view the company's in-house data policies at <https://www.facebook.com/policy.php>.

## 14.9 LinkedIn Insight-Tag Privacy Policy

On our website, we use the LinkedIn Insight Tag conversion tracking tool. The provider of this service is the American company LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA. The responsible entity for the European Economic Area (EEA), the EU and Switzerland is LinkedIn Ireland Unlimited (Wilton Place, Dublin 2, Ireland) when it comes to any data protection and privacy relevant aspects.

The LinkedIn Insight Tag collects the following data of the website visitor:

**URL, referrer, IP address, Device, browser characteristics (User Agent), and timestamp.**

**Note:** We do not claim for this list to be extensive, as LinkedIn may change the choice of data collected.

The IP addresses and members' direct identifiers are removed within seven days in order to make the data pseudonymous. The pseudonymized data is then deleted within 180 days.

We do not receive any personal data. We only receive aggregate reports on the demographics of our target audience and the performance of our ads.

LinkedIn also processes data in the United States, among other countries. Currently LinkedIn is not a participant of the [Data Privacy Framework Program](#). We would like to note, that US companies that do not participate in the Data Privacy Framework Program are not certified by the European Commission as having an adequate level of data protection. This can be associated with various risks to the legality and security of data processing. More information can be found at [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_23\\_3752](https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752) as well at [https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf\\_en](https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en).



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

You can find more information about the standard contractual clauses at LinkedIn at <https://de.linkedin.com/legal/l/dpa> or <https://www.linkedin.com/legal/l/eu-sccs>






You can find out more about LinkedIn Insight Tag at <https://www.linkedin.com/help/linkedin/answer/a427660>. You can also find out more about the data that is processed through the use of the LinkedIn Insight Tag in their Privacy Policy at <https://de.linkedin.com/legal/privacy-policy>.

We have entered a Data Processing Agreement (DPA) with LinkedIn in accordance with Article 28 of the General Data Protection Regulation (GDPR). In our general section “Data Processing Agreement (DPA)” you can find out what a DPA is exactly and what it must contain.

This agreement is a legal requirement as LinkedIn processes personal data on our behalf. It clarifies that LinkedIn may only process any data they receive from us according to our instructions and in compliance with the GDPR. You can find the link to the Data Processing Agreement (DPA) at <https://www.linkedin.com/legal/l/dpa?>.

## 15. Audio & Video

### Audio & Video Privacy Policy Overview

-  Affected parties: website visitors
-  Purpose: service optimisation
-  Processed data: Data such as contact details, user behaviour, device information and IP addresses can be stored.  
You can find more details in the Privacy Policy below.
-  Storage period: data are retained for as long as necessary for the provision of the service
-  Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

### 15.1 What are audio and video elements?

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

Audio and video elements are integrated functional elements of platforms such as YouTube, and Vimeo..

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

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

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

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

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

## 15.4 Duration of data processing

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

## 15.5 Right to object

You also retain the right and the option to revoke your consent to the use of cookies or third-party providers at any time. This can be done either via our cookie management tool or via other opt-out functions. You can e.g. also prevent data retention via cookies by

managing, deactivating or erasing cookies in your browser. The legality of the processing up to the point of revocation remains unaffected.






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

## 15.6 Legal basis

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

## 15.7 Vimeo Privacy Policy

### Vimeo Privacy Policy Overview

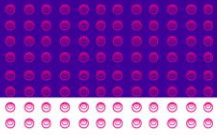
-  Affected parties: website visitors
-  Purpose: optimising our service
-  Processed data: Data such as contact details, data on user behaviour, information about your device and IP address may be stored. You can find more details on this in privacy policy below.
-  Storage period: data are generally stored for as long as is necessary for the purpose of the service
-  Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

### 15.7.1 What is Vimeo?

On our website, we use videos of the company Vimeo. This video portal is operated by Vimeo LLC, 555 West 18th Street, New York, New York 10011, USA. With the help of a plug-in, we can display interesting video material directly on our website. Consequently, some of your data may be transmitted to Vimeo. In this privacy policy we want to explain to you what data this is, why we use Vimeo and how you can manage your data or prevent data transmission.

### 15.7.2 Why do we use Vimeo on our website?

The aim of our website is to provide you the best possible content, in the easiest and most accessible way we can. We will only be satisfied with our service, once we have reached that goal. The video service Vimeo supports us in achieving this goal. Vimeo gives us the opportunity to present high quality content to you directly on our website. Instead of us



merely giving you a link to an interesting video, you can watch the video here with us. This extends our service and makes it easier for you to access interesting content. Therefore, in addition to our texts and images, we can also offer video content.

### 15.7.3 What data is stored on Vimeo?

When you open a site on our website that has a Vimeo video embedded to it, your browser will connect to Vimeo's servers, and a data transmission will take place. The data are then collected, stored and processed on Vimeo's servers. Regardless of whether you have a Vimeo account or not, Vimeo collects data about you. This includes your IP address, technical information about your browser type, your operating system or very basic device information. Furthermore, Vimeo store information on what website you use their service on and which actions (web activities) you carry out on our website. These web activities include e.g. session duration, bounce rate or which button you clicked on our site that contains a Vimeo function. Vimeo can track and store these actions using cookies and similar technologies.

If you are logged in as a registered member of Vimeo, more data may be collected, since a bigger number of cookies may already have been set in your browser. Furthermore, your actions on our website are directly linked to your Vimeo account. To prevent this, you must log out of Vimeo while "surfing" our website.

Below we will show you an array of cookies Vimeo sets when you are on a website containing an integrated Vimeo function. This list is not exhaustive and assumes that you do not have a Vimeo account.

**Name:** player

**Value:** ""

**Purpose:** This cookie saves your settings before you play an embedded Vimeo video. This will ensure you to receive your preferred settings again next time you watch a Vimeo video.

**Expiry date:** after one year

**Name:** vuid

**Value:** pl1046149876.614422590112024533-4

**Purpose:** This cookie collects information about your actions on websites that have a Vimeo video embedded to them.

**Expiry date:** after 2 years

Note: These two cookies are set every time as soon as you are on a website that has a Vimeo video embedded to it. If you watch the video and click a button such as "share" or "like", additional cookies will be set. These can also be third-party cookies such as `_ga` or `_gat_UA-76641-8` from Google Analytics or `_fbp` from Facebook. The exact cookies that are set depends on your interaction with the video.

The following list will show a selection of cookies that could be placed when you interact with a Vimeo video:

**Name:** `_abexps`

**Value:** `%5B%5D`

**Purpose:** This Vimeo cookie helps Vimeo to remember your settings. For example, this can be a pre-set language, a region or a username. The cookie generally stores data on





how you use Vimeo.

**Expiry date:** after one year

**Name:** continuous\_play\_v3

**Value:** 1

**Purpose:** This cookie is a first-party cookie from Vimeo. The cookie collects information on how you use Vimeo's service. For example, the cookie stores details on when you pause a video and resume it.

**Expiry date:** after one year

**Name:** \_ga

**Value:** GA1.2.1522249635.1578401280112024533-7

**Purpose:** This cookie is a third-party cookie from Google. By default, analytics.js uses the \_ga cookie to store the user ID. Thus, it serves to differentiate between website visitors.

**Expiry date:** after 2 years

**Name:** \_gcl\_au

**Value:** 1.1.770887836.1578401279112024533-3

**Purpose:** This third-party cookie from Google AdSense is used to improve the efficiency of ads on websites.

**Expiry date:** after 3 months

**Name:** \_fbp

**Value:** fb.1.1578401280585.310434968

**Purpose:** This is a Facebook cookie. It is used to display adverts or advertising products from Facebook or other advertisers.

**Expiry date:** after 3 months

Vimeo use this data to improve their own service, to communicate with you and to implement their own targeted advertising measures. On their website they emphasise that only first-party cookies (i.e. cookies from Vimeo itself) are used for embedded videos, provided you do not interact with the video.

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

Vimeo is headquartered in White Plains, New York (USA). However, their services are offered worldwide. For this, the company uses computer systems, databases and servers in the United States and other countries. Thus, your data may also be stored and processed on servers in America. Vimeo stores the data until the company no longer has an economical reason for keeping it. Then the data will be deleted or anonymised.

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

You always have the option to manage cookies in your browser. If you do not want Vimeo to set cookies and collect information about you for example, you can delete or deactivate cookies in your browser settings at any time. These settings vary a little depending on the browser. Please note that after deactivating/deleting cookies, various functions may no longer be fully available. The following instructions show how you can manage or delete cookies in your browser.

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



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

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

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

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

If you are a registered Vimeo member, you can also manage cookies in Vimeo's settings.

### 15.7.6 Legal basis

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




Vimeo also processes data in the United States, among other countries. Currently Vimeo is not a participant of the [Data Privacy Framework Program](#). We would like to note, that US companies that do not participate in the Data Privacy Framework Program are not certified by the European Commission as having an adequate level of data protection. This can be associated with various risks to the legality and security of data processing. More information can be found at [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_23\\_3752](https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752) as well at [https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf\\_en](https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en).

Vimeo uses standard contractual clauses approved by the EU Commission as basis for data processing by recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, and especially in the USA) or data transfer there (= Art. 46, paragraphs 2 and 3 of the GDPR). These clauses oblige Vimeo to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses here: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2847](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)


You can find out more about the use of cookies at Vimeo at [https://vimeo.com/cookie\\_policy](https://vimeo.com/cookie_policy). Furthermore, you can find more information on privacy at Vimeo at <https://vimeo.com/privacy>.

## 15.8 YouTube Privacy Policy

### YouTube Privacy Policy Overview

-  Affected parties: website visitors
-  Purpose: optimising our service
-  Processed data: Data such as contact details, data on user behaviour, information about your device and IP address may be stored.

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

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

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

### 15.8.1 What is YouTube?

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

For us to be able to display videos on our website, YouTube provides a code snippet that we have integrated to our website.

### 15.8.2 Why do we use YouTube videos on our website?

YouTube is the video platform with the most visitors and best content. We strive to offer you the best possible user experience on our website, which of course includes interesting videos. With the help of our embedded videos, we can provide you other helpful content in addition to our texts and images.

### 15.8.3 What data is stored by YouTube?

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

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

In the following list we show you cookies that were placed in the browser during a test. On the one hand, we show cookies that were set without being logged into a YouTube account. On the other hand, we show you what cookies were placed while being logged in. We do



not claim for this list to be exhaustive, as user data always depend on how you interact with YouTube.

**Name:** YSC

**Value:** b9-CV6ojI5Y112024533-1

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

**Expiry date:** after end of session

**Name:** PREF

**Value:** f1=50000000

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

**Expiry date:** after 8 months

**Name:** GPS

**Value:** 1

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

**Expiry date:** after 30 minutes

**Name:** VISITOR\_INFO1\_LIVE

**Value:** 95Chz8bagyU

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

Expiry date: after 8 months

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

**Name:** APISID

**Value:** zILivClZSkqGsSwI/AU1aZl6HY7112024533-

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

**Expiry date:** after 2 years

**Name:** CONSENT

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

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

**Expiry date:** after 19 years

**Name:** HSID

**Value:** AcRwpgUik9Dveht0l

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

**Expiry date:** after 2 years

**Name:** LOGIN\_INFO

**Value:** AFmmF2swRQlhALl6aL...

**Purpose:** This cookie stores information on your login data.

**Expiry date:** after 2 years

**Name:** SAPISID

**Value:** 7oaPxoG-pZsJuuF5/AnUdDUlsJ9iJz2vdM

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

your interests.

**Expiry date:** after 2 years

**Name:** SID

**Value:** oQfNKjAsI112024533-

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

**Expiry date:** after 2 years

**Name:** SIDCC

**Value:** AN0-TYuqub2JOcDTyL

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

**Expiry date:** after 3 months

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

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

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

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

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

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

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

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

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

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

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

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

### 15.8.6 Legal basis

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

Youtube (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](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](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847)

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

## 16. Security & Anti-spam

### 16.1 Google reCAPTCHA

#### Google reCAPTCHA Privacy Policy Overview

-  Affected parties: website visitors
  -  Purpose: Service optimisation and protection against cyber attacks
  -  Processed data: data such as IP address, browser information, operating system, limited location and usage data
- You can find more details on this in the Privacy Policy below.
-  Storage duration: depending on the retained data
  -  Legal bases: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)





### 16.1.1 What is reCAPTCHA?

Our primary goal is to provide you an experience on our website that is as secure and protected as possible. To do this, we use Google reCAPTCHA from Google Inc. (1600 Amphitheater Parkway Mountain View, CA 94043, USA). With reCAPTCHA we can determine whether you are a real person from flesh and bones, and not a robot or a spam software. By spam we mean any electronically undesirable information we receive involuntarily. Classic CAPTCHAS usually needed you to solve text or picture puzzles to check. But thanks to Google's reCAPTCHA you usually do not have to do such puzzles. Most of the times it is enough to simply tick a box and confirm you are not a bot. With the new Invisible reCAPTCHA version you don't even have to tick a box. In this privacy policy you will find out how exactly this works, and what data is used for it.

reCAPTCHA is a free captcha service from Google that protects websites from spam software and misuse by non-human visitors. This service is used the most when you fill out forms on the Internet. A captcha service is a type of automatic Turing-test that is designed to ensure specific actions on the Internet are done by human beings and not bots. During the classic Turing-test (named after computer scientist Alan Turing), a person differentiates between bot and human. With Captchas, a computer or software program does the same. Classic captchas function with small tasks that are easy to solve for humans but provide considerable difficulties to machines. With reCAPTCHA, you no longer must actively solve puzzles. The tool uses modern risk techniques to distinguish people from bots. The only thing you must do there, is to tick the text field "I am not a robot". However, with Invisible reCAPTCHA even that is no longer necessary. reCAPTCHA, integrates a JavaScript element into the source text, after which the tool then runs in the background and analyses your user behaviour. The software calculates a so-called captcha score from your user actions. Google uses this score to calculate the likelihood of you being a human, before entering the captcha. If Google determines that a visitor is suspicious, they must solve a CAPTCHA challenge before they can submit the form.

### 16.1.2 Why do we use reCAPTCHA on our website?

We only want to welcome humans on our side and want bots or spam software of all kinds to stay away. Therefore, we are doing everything we can to stay protected and to offer you the highest possible user friendliness. For this reason, we use Google reCAPTCHA from Google. Thus, we can be pretty sure that we will remain a "bot-free" website. Using reCAPTCHA, data is transmitted to Google to determine whether you genuinely are human. reCAPTCHA thus ensures our website's and subsequently your security. Without reCAPTCHA it could e.g. happen that a bot would register as many email addresses as possible when registering, in order to subsequently "spam" forums or blogs with unwanted advertising content. With reCAPTCHA we can avoid such bot attacks.

### 16.1.3 What data is stored by reCAPTCHA?

reCAPTCHA collects personal user data to determine whether the actions on our website are made by people. Thus, IP addresses and other data Google needs for its reCAPTCHA service, may be sent to Google. Within member states of the European Economic Area, IP addresses are almost always compressed before the data makes its way to a server in the

USA. Moreover, your IP address will not be combined with any other of Google's data, unless you are logged into your Google account while using reCAPTCHA. Firstly, the reCAPTCHA algorithm checks whether Google cookies from other Google services (YouTube, Gmail, etc.) have already been placed in your browser. Then reCAPTCHA sets an additional cookie in your browser and takes a snapshot of your browser window.

The following list of collected browser and user data is not exhaustive. Rather, it provides examples of data, which to our knowledge, is processed by Google.

Referrer URL (the address of the page the visitor has come from)

- IP-address (z.B. 256.123.123.1)
- Information on the operating system (the software that enables the operation of your computers. Popular operating systems are Windows, Mac OS X or Linux)
- Cookies (small text files that save data in your browser)
- Mouse and keyboard behaviour (every action you take with your mouse or keyboard is stored)
- Date and language settings (the language and date you have set on your PC is saved)
- All Javascript objects (JavaScript is a programming language that allows websites to adapt to the user. JavaScript objects can collect all kinds of data under one name)
- Screen resolution (shows how many pixels the image display consists of)
- Google may use and analyse this data even before you click on the "I am not a robot" checkmark. In the Invisible reCAPTCHA version, there is no need to even tick at all, as the entire recognition process runs in the background. Moreover, Google have not given details on what information and how much data they retain.

The following cookies are used by reCAPTCHA: With the following list we are referring to Google's reCAPTCHA demo version at <https://www.google.com/recaptcha/api2/demo>. For tracking purposes, all these cookies require a unique identifier. Here is a list of cookies that Google reCAPTCHA has set in the demo version:

**Name:** IDE

**Value:** WqTUmlnmv\_qXyi\_DGNPLESKnRNrpgXoy1K-pAZtAkMbHI-112024533-8

**Purpose:** This cookie is set by DoubleClick (which is owned by Google) to register and report a user's interactions with advertisements. With it, ad effectiveness can be measured, and appropriate optimisation measures can be taken. IDE is stored in browsers under the domain doubleclick.net.

**Expiry date:** after one year

**Name:** 1P\_JAR

**Value:** 2019-5-14-12

**Purpose:** This cookie collects website usage statistics and measures conversions. A conversion e.g. takes place, when a user becomes a buyer. The cookie is also used to display relevant adverts to users. Furthermore, the cookie can prevent a user from seeing the same ad more than once.

**Expiry date:** after one month

**Name:** ANID

**Value:** U7j1v3dZa1120245330xgZFmiqWppRWKOr

**Purpose:** We could not find out much about this cookie. In Google's privacy statement, the cookie is mentioned in connection with "advertising cookies" such as "DSID", "FLC", "AID" and "TAID". ANID is stored under the domain google.com.

**Expiry date:** after 9 months

**Name:** CONSENT

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

**Purpose:** This cookie stores the status of a user's consent to the use of various Google services. CONSENT also serves to prevent fraudulent logins and to protect user data from unauthorised attacks.

**Expiry date:** after 19 years

**Name:** NID

**Value:** 0WmuWqy112024533zILzqV\_nmt3sDXwPeM5Q

**Purpose:** Google uses NID to customise advertisements to your Google searches. With the help of cookies, Google "remembers" your most frequently entered search queries or your previous ad interactions. Thus, you always receive advertisements tailored to you. The cookie contains a unique ID to collect users' personal settings for advertising purposes.

**Expiry date:** after 6 months

**Name:** DV

**Value:** gEAABBCjJMXcI0dSAAAANbqc112024533-4

**Purpose:** This cookie is set when you tick the "I am not a robot" checkmark. Google Analytics uses the cookie personalised advertising. DV collects anonymous information and is also used to distinct between users.

**Expiry date:** after 10 minutes

**Note:** We do not claim for this list to be extensive, as Google often change the choice of their cookies.

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

Due to the integration of reCAPTCHA, your data will be transferred to the Google server. The IP address that your browser transmits to Google does generally not get merged with other Google data from the company's other services. However, the data will be merged if you are logged in to your Google account while using the reCAPTCHA plug-in. Google's diverging privacy policy applies for this.

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

If you want to prevent any data about you and your behaviour to be transmitted to Google, you must fully log out of Google and delete all Google cookies before visiting our website or use the reCAPTCHA software. Generally, the data is automatically sent to Google as soon as you visit our website. To delete this data, you must contact Google Support at <https://support.google.com/?hl=en-GB&tid=112024533>.

If you use our website, you agree that Google LLC and its representatives automatically collect, edit and use data.

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

### 16.1.6 Legal basis

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

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


You can find out a little more about reCAPTCHA on Google's web developer page at <https://developers.google.com/recaptcha>. Google goes into the technical development of the reCAPTCHA in more detail here, but you will look in vain for detailed information about data storage and data protection issues. A good overview of the basic use of data by Google can be found in the in-house data protection declaration at <https://policies.google.com/privacy?hl=en-GB>.


## 17. Data processing within the context of the internal whistleblowing system

### 17.1 Whistleblowing & Ethics Reporting Channel


#### Whistleblowing & Ethics Reporting Channel Overview

 Affected parties: Whistleblowers or persons affected by the whistleblowing or the person assisting the whistleblower, or persons affected by follow-up measures or involved in follow-up measures

 Purpose: to receive notices of violations of the law in the areas mentioned in § 3 paragraphs 3, 4 and 5 HSchG in a secure and confidential way

 Processed data: First name, surname, e-mail, postal address, telephone number, the content of the report.

 Storage duration: check below

 Legal bases: Art. 6 para. 1 lit. c GDPR (legal obligation), Art. 6 para. 1 lit. f GDPR (legitimate interests)

#### 17.1.1 What is the Whistleblowing & Ethics Reporting Channel and what data is stored?

We provide you the opportunity to report indications of legal violations in a trusted environment through the Whistleblower and Ethics Reporting Channel. The Whistleblower and Ethics Reporting Channel is operated by PwC PricewaterhouseCoopers Wirtschaftsprüfung und Steuerberatung GmbH ('PwC Tax') and oehner & partner rechtsanwaelte gmbh ('PwC Legal, hereinafter together 'PwC'). PwC is responsible for processing and reviewing the reports submitted in accordance with legal requirements. PwC then will review the validity of the report, develop appropriate follow-up measures and recommendations for action and send them to us in anonymous form.

The reports submitted by you as well as your personal data will be treated confidentially by PwC. Your personal data will only be disclosed, unless required by law, if you request this in the individual case.

We, on the other hand, do not have direct access to the personal data of your report. However, your personal data may result from the follow-up measures in connection with the whistleblowing report. Should we process personal data, this is done in accordance with Art. 6 para. 1 lit. c GDPR for the fulfilment of a legal obligation (§ 8 Whistleblower Protection Act). The confidentiality and security of your data has the highest priority for us.

The web form is hosted in the EU. All data is processed on secure servers in Europe.

We take all indications of reported legal violations seriously! We do not tolerate any violations of the law. All incoming reports are checked by PwC. The consequential actions resulting from the reports are determined by us according to the recommendations of PwC.

If a follow-up measure resulting from the report requires the transfer of personal data to a supervisory authority, public authority or court, this is done in accordance with Article 6 (1) (c) GDPR and on the basis of legitimate interests in accordance with Article 6 (1) (f) GDPR.

If you are a person affected by the notice, the data subject rights (right to information, right to access, right to rectification, right to erasure, right to restriction of processing, right to object



and right to notification of a personal data breach) do not apply as long as this is necessary to achieve the purposes of the notice.

The whistleblower reporting system and more information on how it works can be found [here](#). Here is also the link for the underlying [EU directive](#).

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

We will delete the data accrued within the scope of the notice as soon as they are no longer required for the processing of the procedure. The data will be deleted no later than 30 days after the conclusion of the procedure. Insofar as statutory retention obligations exist, the data will be stored for the duration of the legally prescribed retention obligation.

### 17.1.3 Legal notice:

- Your reports may lead to investigations. This applies to both internal and regulatory investigations. Your information may also have serious consequences for other persons and for us. For this reason, only share information that is true to the best of your knowledge. If you knowingly provide false or misleading information, you will not be protected and you will face consequences.
- The Whistleblower and Ethics Reporting Channel is not designed to be an emergency hotline. Therefore, please do not use this channel to report an immediate threat or acute risk. In the event of an immediate threat or acute risk, notify the appropriate department. If necessary, also inform the relevant authorities.
- In addition to reporting through our Whistleblower and Ethics Reporting Channel, you also have the option of submitting any reports to the regulatory reporting channel (external reporting channel). Please note that such reports may result in regulatory investigations that are beyond our control or the control of PwC. We therefore encourage you to use our reporting channel so that we have the opportunity to respond appropriately to any legal violations.
- Please note that legal protection can only be provided in limited circumstances in case of public disclosure of reports, for example on the internet or in the press. The protection against retaliation measures is primarily given if you have previously informed an internal or external reporting channel and have not received a timely response about them taking appropriate follow-up action to your report or another exceptional case is given. Please note: Disclosure of information can lead to considerable damage for us! We therefore encourage you to use our reporting channel or otherwise contact us prior to disclosure.
- Please note that the Whistleblower and Ethics Reporting Channel is only set up for certain reporting topics. These topics result from the web form.

All texts are copyrighted.