

Privacy Protection Statement

Thank you for your interest in our website and our company.

The protection of your privacy and your personal data is very important to us. Therefore we store and process your data based on the General Data Protection Regulation (GDPR) of the European Union.

Privacy Policy

We have written this privacy policy (version 10.02.2022-121942918) 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 and **graphics** are used. We are thus informing in clear and simple language that we only process personal data in the context of our business activities if there is a legal basis for it. This is certainly not possible with brief, unclear and legal-technical statements, as is often standard on the Internet when it comes to data protection. I hope you find the following explanations interesting and informative. Maybe you will also find some information that you have not been familiar with.

If you still have questions, we 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.

Scope

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

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

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

Legal bases

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

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

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

1. **Consent** (Article 6 Paragraph 1 lit. a GDPR): You have given us your consent to process data for a specific purpose. An example would be the storage of data you entered into a contact form.
2. **Contract** (Article 6 Paragraph 1 lit. b GDPR): We process your data in order to fulfill a contract or pre-contractual obligations with you. For example, if we conclude a sales contract with you, we need personal information in advance.
3. **Legal obligation** (Article 6 Paragraph 1 lit. c GDPR): If we are subject to a legal obligation, we will process your data. For example, we are legally required to keep invoices for our bookkeeping. These usually contain personal data.
4. **Legitimate interests** (Article 6 Paragraph 1 lit. f GDPR): In the case of legitimate interests that do not restrict your basic rights, we reserve the right to process personal data. For example, we have to process certain data in order to be able to operate our website securely and economically. Therefore, the processing is a legitimate interest.

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

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

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

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

Contact details for data protection

We do not have a data protection officer, as this is not required for CNSystems.
If you have any questions about data protection, please contact

CNSystems Medizintechnik GmbH
Reininghausstrasse 13
8020 Graz
Austria

E-Mail: office@cnsystems.com

Phone: [+43 316 723456 0](tel:+433167234560)

Company details: <https://www.cnsystems.com/de/impressum/>

Storage Period

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

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

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

Rights in accordance with the General Data Protection Regulation

You are granted the following rights in accordance with the provisions of the GDPR (General Data Protection Regulation) and the Austrian Data Protection Act (DSG):

- right to rectification (article 16 GDPR)
- right to erasure (“right to be forgotten”) (article 17 GDPR)
- right to restrict processing (article 18 GDPR)
- right to notification – notification obligation regarding rectification or erasure of personal data or restriction of processing (article 19 GDPR)
- right to data portability (article 20 GDPR)
- Right to object (article 21 GDPR)
- right not to be subject to a decision based solely on automated processing – including profiling – (article 22 GDPR)

If you think that the processing of your data violates the data protection law, or that your data protection rights have been infringed in any other way, you can lodge a complaint with your

respective regulatory authority. For Austria this is the data protection authority, whose website you can access at <https://www.data-protection-authority.gv.at/>.

Austria Data protection authority

Manager: Mag. Dr. Andrea Jelinek
Address: Barichgasse 40-42, 1030 Wien
Phone number.: +43 1 52 152-0
E-mail address: dsb@dsb.gv.at
Website: <https://www.dsb.gv.at/>

Data transfer to third countries

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

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

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

Security of data processing operations

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


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

TLS encryption with https

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

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






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

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

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

Communications

Communications Overview

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

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

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

Affected persons

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

Telephone

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

Email

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

Online forms

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

Legal bases

Data processing is based on the following legal bases:

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

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)

What are cookies?

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

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

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

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

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

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

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

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

Name: _ga
Value: GA1.2.1326744211.152121942918-9
Purpose: Differentiation between website visitors
Expiry date: after 2 years

A browser should support these minimum sizes:

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

Which types of cookies are there?

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

There are 4 different types of cookies:

Essential cookies

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

Purposive cookies

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

Target-orientated cookies

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

Advertising cookies

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

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

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

Purpose of processing via cookies

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

Which data are processed?

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

Storage period of cookies

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

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

Right of objection – how can I erase cookies?

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

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

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

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

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

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

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

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

Legal basis

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






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

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

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

Web hosting

Web hosting Overview

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

What is web hosting?

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

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

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

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

Why do we process personal data?

The purposes of data processing are:

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

Which data are processed?

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

- the full address (URL) of the accessed website (e. g. <https://www.examplepage.uk/examplesubpage.html?tid=121942918>)
- browser and browser version (e.g. Chrome 87)
- the operating system used (e.g. Windows 10)
- the address (URL) of the previously visited page (referrer URL) (e. g. <https://www.examplepage.uk/icamefromhere.html/>)
- the host name and the IP address of the device from the website is being accessed from (e.g. COMPUTERNAME and 194.23.43.121)
- date and time
- in so-called web server log files

How long is the data stored?

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

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

Legal basis

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

DomainFactory Privacy Policy

We use DomainFactory for our website, which is a web hosting provider, among other things. The provider of this service is the German company domainfactory GmbH, Oskar-Messter-Str. 33, 85737 Ismaning, Germany. You can find out more about the data that is processed by DomainFactory in their Privacy Policy at <https://www.df.eu/de/datenschutz/>.

WordPress.com Privacy Policy

We use WordPress.com for our website, which is a modular website system. The provider of this service is the American company Automattic Inc., 60 29th Street #343, San Francisco, CA 94110, USA.

WordPress.com also processes data in the USA, among other countries. We would like to note, that according to the European Court of Justice, there is currently no adequate level of

protection for data transfers to the USA. This can be associated with various risks to the legality and security of data processing.

WordPress.com 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, paragraphs 2 and 3 of the GDPR). These clauses oblige WordPress.com to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses here: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

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

Facebook Pixel Privacy Policy

We use Facebook's Facebook pixel on our website. 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. For example, if you buy a product on our website, the Facebook pixel is triggered and stores your actions on our website 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.1.1568287647279.257405483-6121942918-7

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_50ae8267e2bdf1253ec1a5769f48e062121942918-3

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/ads/preferences/?entry_product=ad_settings_screen. 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.

We would like to note, that according to the European Court of Justice, there is currently no adequate level of protection for data transfer to the USA. Data processing is done mainly through Facebook Pixel. This may lead to data not being anonymously processed and stored. Furthermore, US government authorities may get access to individual data. The data may also get linked to data from other Facebook services you have a user account with.

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

Google Analytics Privacy Policy

Google Analytics Privacy Policy Overview



Affected parties: website visitors




Purpose: Evaluation of visitor information to optimise the website.



Processed data: Access statistics that contain data such as the location of access, device data, access duration and time, navigation behaviour, click behaviour and IP addresses. You can find more details on this in the privacy policy below.



Storage period: depending on the properties used

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

What is Google Analytics?

We use the tracking and analysis tool Google Analytics (GA) of the US-American company Google LLC (1600 Amphitheatre Parkway Mountain View, CA 94043, USA). Google Analytics collects data on your actions on our website. Whenever you click a link for example, this action is saved in a cookie and transferred to Google Analytics. With the help of reports which we receive from Google Analytics, we can adapt our website and our services better to your wishes. In the following, we will explain the tracking tool in more detail, and most of all, we will inform you what data is saved and how you can prevent this.

Google Analytics is a tracking tool with the purpose of conducting data traffic analysis of our website. For Google Analytics to work, there is a tracking code integrated to our website. Upon your visit to our website, this code records various actions you perform on your website. As soon as you leave our website, this data is sent to the Google Analytics server, where it is stored.

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

- Target audience reports: With the help of target audience reports we can get to know our users better and can therefore better understand who is interested in our service.
- Advertising reports: Through advertising reports we can analyse our online advertising better and hence improve it.
- Acquisition reports: Acquisition reports provide us helpful information on how we can get more people enthusiastic about our service.
- Behaviour reports: With these reports, we can find out how you interact with our website. By the means of behaviour reports, we can understand what path you go on our website and what links you click.
- Conversion reports: A conversion is the process of leading you to carry out a desired action due to a marketing message. An example of this would be transforming you from a mere website visitor into a buyer or a newsletter subscriber. Hence, with the help of these reports we can see in more detail, if our marketing measures are successful with you. Our aim is to increase our conversion rate.
- Real time reports: With the help of these reports we can see in real time, what happens on our website. It makes us for example see, we can see how many users are reading this text right now.

Why do we use Google Analytics on our website?

The objective of our website is clear: We want to offer you the best possible service. Google Analytics' statistics and data help us with reaching this goal.

Statistically evaluated data give us a clear picture of the strengths and weaknesses of our website. On the one hand, we can optimise our page in a way, that makes it easier to be found by interested people on Google. On the other hand, the data helps us to get a better understanding of you as our visitor. Therefore, we can very accurately find out what we must improve on our website, in order to offer you the best possible service. The analysis of that data also enables us to carry out our advertising and marketing measures in a more individual and more cost-effective way. After all, it only makes sense to show our products and services exclusively to people who are interested in them.

What data is stored by Google Analytics?

With the aid of a tracking code, Google Analytics creates a random, unique ID which is connected to your browser cookie. That way, Google Analytics recognises you as a new user. The next time you visit our site, you will be recognised as a “recurring” user. All data that is collected gets saved together with this very user ID. Only this is how it is made possible for us to evaluate and analyse pseudonymous user profiles.

To analyse our website with Google Analytics, a property ID must be inserted into the tracking code. The data is then stored in the corresponding property. Google Analytics 4-property is standard for every newly created property. An alternative however, is the Universal Analytics Property. Depending on the property that is being used, data are stored for different periods of time.

Your interactions on our website are measured by tags such as cookies and app instance IDs. Interactions are all kinds of actions that you perform on our website. If you are also using other Google systems (such as a Google Account), data generated by Google Analytics can be linked with third-party cookies. Google does not pass on any Google Analytics data, unless we as the website owners authorise it. In case it is required by law, exceptions can occur.

The following cookies are used by Google Analytics:

Name: `_ga`

Value: 2.1326744211.152121942918-5

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: 2.1687193234.152121942918-1

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

Verwendungszweck: 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

Name: AMP_TOKEN

Value: No information

Purpose: This cookie has a token which is used to retrieve the user ID by the AMP Client ID Service. Other possible values suggest a logoff, a request or an error.

Expiration date: After 30 seconds up to one year

Name: __utma

Value: 1564498958.1564498958.1564498958.1

Purpose: With this cookie your behaviour on the website can be tracked and the site performance can be measured. The cookie is updated every time the information is sent to Google Analytics.

Expiration date: After 2 years

Name: __utmt

Value: 1

Purpose: Just like __gat_gtag_UA_<property-id> this cookie is used for keeping the requirement rate in check.

Expiration date: After 10 minutes

Name: __utmb

Value: 3.10.1564498958

Purpose: This cookie is used to determine new sessions. It is updated every time new data or information gets sent to Google Analytics.

Expiration date: After 30 minutes

Name: __utmc

Value: 167421564

Purpose: This cookie is used to determine new sessions for recurring visitors. It is therefore a session cookie, and only stays stored until you close the browser again.

Expiration date: After closing the browser

Name: __utmz

Value: m|utmccn=(referral)|utmcmd=referral|utmcct=

Purpose: This cookie is used to identify the source of the number of visitors to our website. This means, that the cookie stored information on where you came to our website from. This could be another site or an advertisement.

Expiration date: After 6 months

Name: __utmv

Value: No information

Purpose: The cookie is used to store custom user data. It gets updated whenever information is sent to Google Analytics.

Expiration date: After 2 years

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

Below we will give you an overview of the most important data that can be evaluated by Google Analytics:

Heatmaps: Google creates so-called Heatmaps on our website. These Heatmaps make it possible to see the exact areas you click on, so we can get information on what routes you make on our website.

Session duration: Google calls the time you spend on our website without leaving it session duration. Whenever you are inactive for 20 minutes, the session ends automatically.

Bounce rate If you only look at one page of our website and then leave our website again, it is called a bounce.

Account creation: If you create an account or make an order on our website, Google Analytics collects this data.

IP-Address: The IP address is only shown in a shortened form, to make it impossible to clearly allocate it.

Location: Your approximate location and the country you are in can be defined by the IP address. This process is called IP location determination.

Technical information: Information about your browser type, your internet provider and your screen resolution are called technical information.

Source: Both, Google Analytics as well as ourselves, are interested what website or what advertisement led 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.

How long and where is the data stored?

Google has servers across the globe. Most of them are in America and therefore your data is mainly saved on American servers. Here you can read detailed information on where Google's data centres are located: <https://www.google.com/about/datacenters/inside/locations/?hl=en>

Your data is allocated to various physical data mediums. This has the advantage of allowing to retrieve the data faster, and of protecting it better from manipulation. Every Google data centre has respective emergency programs for your data. Hence, in case of a hardware failure at Google or a server error due to natural disasters, the risk for a service interruption stays relatively low.

The data retention period depends on the properties used. When using the newer Google Analytics 4-properties, the retention period of your user data is set to 14 months. For so-called

event data, we have the option of choosing a retention period of either 2 months or 14 months.

Google Analytics has a 26 months standardised period of retaining your user data. After this time, your user data is deleted. However, we have the possibility to choose the retention period of user data ourselves. There are the following five options:

- Deletion after 14 months
- Deletion after 26 months
- Deletion after 38 months
- Deletion after 50 months
- No automatical deletion

Additionally, there is the option for data to be deleted only if you no longer visit our website within a period determined by us. In this case, the retention period will be reset every time you revisit our website within the specified period.

As soon as the chosen period is expired, the data is deleted once a month. This retention period applies to any of your data which is linked to cookies, user identification and advertisement IDs (e.g. cookies of the DoubleClick domain). Any report results are based on aggregated information and are stored independently of any user data. Aggregated information is a merge of individual data into a single and bigger unit.

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 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 generally want to deactivate, delete or manage all cookies (independently of Google Analytics), you can use one of the guides that are available for any browser:

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

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

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

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

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

Legal basis

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 have legitimate interest in analysing the behaviour of website visitors, in order to technically and economically improve our offer. With Google 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 Google Analytics if you have given your consent.

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

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

We hope we could provide you with the most important information about data processing by Google Analytics. If you want to find out more on the tracking service, we recommend these two

links: <https://marketingplatform.google.com/about/analytics/terms/gb/> and <https://support.google.com/analytics/answer/6004245?hl=en>.

Google Analytics Deactivation Link

By clicking on the following **deactivation link** you can prevent Google from tracking your further visits. Caution: The deletion of cookies, the use of your browser's incognito/private mode or the use of a different browser may lead to your data being collected again.

Deactivate Google Analytics

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>.


Google Analytics' Data Processing Amendment


By accepting the amendment on data processing in Google Analytics, we entered a contract with Google concerning the use of Google Analytics.


You can find out more about the amendment on data processing for Google Analytics here: https://support.google.com/analytics/answer/3379636?hl=en&utm_id=ad


Web Analytics


Web Analytics Privacy Policy Overview

 Affected parties: visitors to the website

 Purpose: Evaluation of visitor information to optimise the website.

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

 Storage period: depending on the respective web analytics tool used

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

What is Web Analytics?

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

Why do we run Web Analytics?

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

particularly popular. All this information helps us to optimise our website and adapt it to your needs, interests and wishes.

Which data are processed?

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

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

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

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

Duration of data processing

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

Right to object

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

Legal basis

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

In addition to consent, we have a legitimate interest in analysing the behaviour of website visitors, which enables us to technically and economically improve our offer. With Web






Analytics, we can recognise website errors, identify attacks and improve profitability. The legal basis for this is **Art. 6 para. 1 lit. f of the GDPR (legitimate interests)**. Nevertheless, we only use these tools if you have given your consent.

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

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

Google Tag Manager Privacy Policy

Google Tag Manager Privacy Policy Overview

-  Affected parties: website visitors
-  Purpose: Organisation 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)

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.

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.

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 we could not find out 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.

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.

In our individual data protection texts on the different tools you can find out how long the respective tracking tools store your data.

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 data protection texts on the different tracking tools you can find detailed information on how you can delete or manage your data.

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

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

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

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

Use of SalesViewer® technology

This website uses SalesViewer® technology from SalesViewer® GmbH on the basis of the website operator's legitimate interests (Section 6 paragraph 1 lit.f GDPR) in order to collect and save data on marketing, market research and optimisation purposes.

In order to do this, a javascript based code, which serves to capture company-related data and according website usage. The data captured using this technology are encrypted in a non-retrievable one-way function (so-called hashing). The data is immediately pseudonymised and is not used to identify website visitors personally.

The data stored by Salesviewer will be deleted as soon as they are no longer required for their intended purpose and there are no legal obligations to retain them.

The data recording and storage can be repealed at any time with immediate effect for the future, by clicking on <https://www.salesviewer.com/opt-out> in order to prevent SalesViewer® from recording your data. In this case, an opt-out cookie for this website is saved on your device. If you delete the cookies in the browser, you will need to click on this link again.

Email-Marketing

Email Marketing Overview



Affected parties: newsletter subscribers



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



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



Storage duration: for the duration of the subscription



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

What is Email-Marketing?

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

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

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

general, the time of registration and registration confirmation are stored, as well as your IP address. Moreover, any change you make to your data that we have on file is also logged.

Why do we use Email-Marketing?

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

Which data are processed?

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

Duration of data processing

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

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

Withdrawal – how can I cancel my subscription?

You have the option to cancel your newsletter subscription at any time. All you have to do is revoke your consent to the newsletter subscription. This usually only takes a few seconds or a

few clicks. Most of the time you will find a link at the end of every email, via which you will be able to cancel the subscription. Should you not be able to find the link in the newsletter, you can contact us by email and we will immediately cancel your newsletter subscription for you.

Legal basis

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


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

CleverReach Privacy Policy


We use CleverReach on our website, which is a service for our email marketing. The service provider is the German company CleverReach GmbH & Co. KG, Schafjückenweg 2, 26180 Rastede, Germany. You can find out more about the data that is processed through the use of CleverReach in the privacy policy at <https://www.cleverreach.com/de/datenschutz/>

Facebook Privacy Policy


Facebook Privacy Policy Overview


 Affected parties: website visitors

 Purpose: service optimisation

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

You can find more details in the Privacy Policy below.

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

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

What are Facebook tools?

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

If your data is collected and forwarded via our embedded Facebook elements or via our Facebook page (fanpage), both we and Facebook Ireland Ltd. are responsible for this. However, should any further processing occur, then Facebook is solely responsible for this

data. Our joint commitments were also set out in a publicly available agreement at https://www.facebook.com/legal/controller_addendum. It e.g. states that we must clearly inform you about the use of Facebook tools on our website. We are also responsible for ensuring that the tools are securely integrated into our website and are in accordance with the applicable privacy laws. Facebook, on the other hand, is e.g. responsible for the data security of Facebook's products. If you have any questions about Facebook's data collection and processing, you can contact the company directly. Should you direct the question to us, we are obliged to forward it to Facebook.

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

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

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

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

Why do we use Facebook tools on our website?

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

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

What data is stored by Facebook tools?

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

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

Moreover, not only contact data, but also “event data” is transferred. These data are the information we receive about you on our website. To give an example, it allows us to see what subpages you visit or what products you buy from us. Facebook does not disclose the obtained information to third parties (such as advertisers), unless the company has an explicit permission or is legally obliged to do so. Also, “event data” can be linked to contact information, which helps Facebook to offer improved, customised adverts. Finally, after the previously mentioned matching process, Facebook deletes the contact data.

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

How long and where are the data stored?

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

How can I erase my data or prevent data retention?

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

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

- 1) Click on settings in the top right side in Facebook.
- 2) Then, click “Your Facebook information” in the left column.
- 3) Now click on “Deactivation and deletion”.

4) Choose “Permanently delete account” and then click on “Continue to account deletion”.

5) Enter your password, click on “continue” and then on “Delete account”.

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

Chrome: Clear, enable and manage cookies in Chrome

Safari: Manage cookies and website data in Safari

Firefox: Clear cookies and site data in Firefox

Internet Explorer: Delete and manage cookies

Microsoft Edge: Delete cookies in Microsoft Edge

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

Legal basis

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

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


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


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

Social Media


Social Media Privacy Policy Overview


 Affected parties: website visitors

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

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

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

 Storage period: depending on the social media platforms used

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

What is Social Media?

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

Why do we use Social Media?

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

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

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

Please note that when you use social media platforms or our built-in elements, your data may also be processed outside the European Union, as many social media channels, such as Facebook or Twitter, are American companies. As a result, you may no longer be able to easily claim or enforce your rights regarding your personal data.

Which data are processed?

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

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

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

Duration of data processing

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

Right to object

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

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

Legal basis

If you have consented to the processing and storage of your data by integrated social media elements, this consent serves as the legal basis for data processing (**Art. 6 para. 1 lit. a GDPR**). Generally, provided you have given your consent, your data will also be stored and processed on the basis of our legitimate interest (**Art. 6 para. 1 lit. f GDPR**) in maintaining fast and good communication with you and other customers and business partners.

Nevertheless, we only use the tools if you have consented. Most social media platforms also set cookies on your browser to store data. We therefore recommend you to read our privacy policy on cookies carefully and to take a look at the privacy policy or cookie policy of the respective service provider.

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

LinkedIn Privacy Policy

LinkedIn Privacy Policy Overview



Affected parties: website visitors



Purpose: optimisation of our service



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

More details can be found in the privacy policy below.



Storage period: the data is generally deleted within 30 days



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

What is LinkedIn?

On our website we use social plugins from the social media network LinkedIn, of the LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA. Social plugins can be feeds, content sharing or a link to our LinkedIn page. Social plugins are clearly marked with the well-known LinkedIn logo and for example allow sharing interesting content directly via our website. Moreover, LinkedIn Ireland Unlimited Company Wilton Place in Dublin is responsible for data processing in the European Economic Area and Switzerland.

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

LinkedIn is the largest social network for business contacts. In contrast to e.g. Facebook, LinkedIn focuses exclusively on establishing business connections. Therefore, companies can

present services and products on the platform and establish business relationships. Many people also use LinkedIn to find a job or to find suitable employees for their own company. In Germany alone, the network has over 11 million members. In Austria there are about 1.3 million.

Why do we use LinkedIn on our website?

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

What data are stored by LinkedIn?

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

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

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

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

Name: bcookie

Value: =2&34aab2aa-2ae1-4d2a-8baf-c2e2d7235c16121942918-

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

Expiry date: after 2 years

Name: lang

Value: v=2&lang=en-gb

Purpose: This cookie saves your default or preferred language.

Expiry date: after end of session

Name: lidc

Value: 1818367:t=1571904767:s=AQF6KNnJ0G121942918...

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

Expiry date: after 24 hours

Name: rtc

Value: kt0Irv3NF3x3t6xvDgGrZGDKkX

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

Expiry date: after 2 minutes

Name: JSESSIONID

Value: ajax:1219429182900777718326218137

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

Expiry date: after end of session

Name: bscookie

Value: "v=1&201910230812...

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

Expiry date: after 2 years

Name: fid

Value: AQHj7li23ZBcqAAAA...

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

Expiry date: after 7 days

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

How long and where are the data stored?

In general, LinkedIn retains your personal data for as long as the company considers it necessary for providing its services. However, LinkedIn deletes your personal data when you delete your account. In some exceptional cases, LinkedIn keeps some summarised and anonymised data, even account deletions. As soon as you delete your account, it may take up to a day until other people can no longer see your data. LinkedIn generally deletes the data within 30 days. However, LinkedIn retains data if it is necessary for legal reasons. Also, data that can no longer be assigned to any person remains stored even after the account is closed. The data are stored on various servers in America and presumably also in Europe.

How can I delete my data or prevent data retention?

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

How to access account data in your LinkedIn profile:

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

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

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

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

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

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

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

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

Legal basis

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

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

LinkedIn uses standard contractual clauses approved by the EU Commission as the basis for data processing by recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, and especially in the USA) or data transfer there (= Art. 46, paragraph

2 and 3 of the GDPR). These clauses oblige LinkedIn to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses here: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847

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

WordPress-Emojis Privacy Policy

In our blog, we also use emojis and smilies. We most probably don't need to explain in more detail what emojis are. After all, you know those smiling, angry or sad faces. They are graphic elements or files that we make available, which are loaded from another server. The service provider for WordPress emojis and smilies is Automattic Inc., 60 29th Street #343, San Francisco, CA 94110, USA. This third-party provider stores your IP address in order to be able to transmit the emoji files to your browser.

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


Automattic 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, paragraphs 2 and 3 of the GDPR). These clauses oblige Automattic to comply with the EU's level of data protection when processing relevant data outside the EU. These clauses are based on an implementing order by the EU Commission. You can find the order and the clauses here: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.


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



Online Marketing

Online Marketing Privacy Policy Overview

 Affected parties: visitors to the website

 Purpose: Evaluation of visitor information for website optimisation

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

 Storage period: depending on the Online Marketing tools used
 Legal basis: Art. 6 para. 1 lit. a GDPR (consent), Art. 6 para. 1 lit. f GDPR (legitimate interests)

What is Online Marketing?

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

Why do we use Online Marketing tools?

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

Which data are processed?

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

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

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

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

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

Duration of data processing

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

Right of withdrawal

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

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

Legal basis

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

Moreover, we have a legitimate interest in measuring our online marketing activities in anonymised form, in order to use this data for optimising our offer and our Marketing. The

corresponding legal basis for this is **Art. 6 para. 1 lit. f GDPR (legitimate interests)** .
Nevertheless, we only use these tools if you have given your consent.

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

Google Ads (Google AdWords) Conversion Tracking Privacy Policy

Google Ads (Google AdWords) Conversion Tracking Privacy Policy Overview



Affected parties: visitors to the website



Purpose: economic success and service optimisation.



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



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



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

What is Google Ads conversion tracking?

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

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

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

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

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

What data is stored with Google Ads conversion tracking?

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

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

Name: Conversion

Value: EhMI_aySuoyv4gIVled3Ch0llweVGAEgt-mr6aXd7dYISAGQ121942918-3

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

Expiry date: after 3 months

Name: _gac

Value: 1.1558695989.EAlalQobChMliOmEgYO04gIVj5AYCh2CBAPrEAAAYASAAEgIYQfD_BwE

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

Expiry date: after 3 months

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

As soon as you complete an action on our website, Google identifies the cookie and saves your action as a so-called conversion. For as long as you surf our website, provided the cookie has not expired, both Google and us can determine that you found your way to us via a Google ad. Then, the cookie is read and sent back to Google Ads, together with the conversion data. Moreover, other cookies may also be used for measuring conversions. Google Ads' conversion tracking can be fine-tuned and improved with the aid of Google Analytics. Furthermore, ads which Google displays in various places across the web, might be placed under our domain with the name "__gads" or "_gac".

Since September 2017, analytics.js retains various campaign information with the _gac cookie. This cookie stores data, as soon as you open one of our sites that has been set up for Google Ads' auto-tagging. In contrast to cookies that are placed for Google domains, Google

can only read these conversion cookies when you are on our website. We do neither collect nor receive any personal data. We do obtain a report with statistical evaluations by Google. With the help thereof, we can not only see the total number of users who clicked our ad, but also what advertising measures were well received.

How long and where is the data stored?

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

How can I erase my data or prevent data retention?

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

Chrome: Clear, enable and manage cookies in Chrome

Safari: Manage cookies and website data in Safari

Firefox: Clear cookies and site data in Firefox

Internet Explorer: Delete and manage cookies

Microsoft Edge: Delete cookies in Microsoft Edge

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

Legal basis

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

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

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

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

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

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.

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

LinkedIn uses standard contractual clauses approved by the EU Commission as the basis for data processing by recipients based in third countries (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.


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

Cookie Consent Management Platform


Cookie Consent Management Platform Overview

 Affected parties: Website visitors

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

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

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

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

What is a cookie consent management platform?

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

Why do we use a cookie management tool?

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

Which data are processed?

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

Duration of data processing

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

Right of objection

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

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

Legal basis

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

BorlabsCookie Privacy Policy


On our website we use BorlabsCookie, which is one of the tools that store your consent to cookies. The provider of this service is the German company Borlabs – Benjamin A. Borschein, Rübenkamp 32, 22305 Hamburg, Germany. You can find out more about the data that is processed by the use of BorlabsCookie in their Privacy Policy at <https://borlabs.io/privacy/>.

Audio & Video


Audio & Video Privacy Policy Overview


 Affected parties: website visitors

 Purpose: service optimisation

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

You can find more details in the Privacy Policy below.

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

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

What are audio and video elements?

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

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

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

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

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

Which data are retained by audio & video elements?

When you visit a page on our website with e.g. an embedded video, your server connects to the service provider's server. Thus, your data will also be transferred to the third-party provider, where it will be stored. Certain data is collected and stored regardless of whether you have an account with the third party provider or not. This usually includes your IP address, browser type, operating system and other general information about your device. Most providers also collect information on your web activity. This e.g. includes the session duration, bounce rate, the buttons you clicked or information about the website you are using the

service on. This data is mostly stored via cookies or pixel tags (also known as web beacons). Any data that is pseudonymised usually gets stored in your browser via cookies. In the respective provider's Privacy Policy, you can always find more information on the data that is stored and processed.

Duration of data processing

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

Right to object

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

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

Legal basis

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

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)

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.

Vimeo is a video platform that was founded in 2004 and introduced video streaming in HD quality in 2007. Since 2015 it has been possible to stream in 4k Ultra HD. The use of the portal is free of charge, but it also contains certain paid content. Compared to the market leader YouTube, Vimeo attaches great importance to valuable content in good quality. On the one hand, the portal offers a lot of artistic content such as music videos and short films. On the other hand, it also offers useful documentaries on a broad spectrum of topics.

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.

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: pl1046149876.614422590121942918-4

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: `GA1.2.1522249635.1578401280121942918-7`

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: 1.1.770887836.1578401279121942918-3

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.

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. Vimeo correspond to the EU-U.S. Privacy Shield Framework and are therefore allowed to collect and use information from users within the EU, and to transfer this data to the USA.

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.

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

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


You can find out more about the use of cookies at Vimeo at https://vimeo.com/cookie_policy. Furthermore, you can find more information on privacy at Vimeo at <https://vimeo.com/privacy>.

YouTube Privacy Policy


YouTube Privacy Policy Overview


 Affected parties: website visitors

 Purpose: optimising our service

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

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

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

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

What is YouTube?

We have integrated YouTube videos to our website. Therefore, we can show you interesting videos directly on our site. YouTube is a video portal, which has been a subsidiary company of Google LLC since 2006. The video portal is operated by YouTube, LLC, 901 Cherry Ave., San Bruno, CA 94066, USA. When you visit a page on our website that contains an embedded YouTube video, your browser automatically connects to the servers of YouTube or Google.

Thereby, certain data are transferred (depending on the settings). Google is responsible for YouTube's data processing and therefore Google's data protection applies.

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

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

Why do we use YouTube videos on our website?

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

What data is stored by YouTube?

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

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

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

Name: YSC

Value: b9-CV6ojl5Y121942918-1

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: zILlvCIZSkqGsSwI/AU1aZI6HY7121942918-

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

Expiry date: after 2 years

Name: CONSENT

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

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

Expiry date: after 19 years

Name: HSID

Value: AcRwpgUik9Dveht0I

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

Expiry date: after 2 years

Name: LOGIN_INFO

Value: AFmmF2swRQIhALi6aL...

Purpose: This cookie stores information on your login data.

Expiry date: after 2 years

Name: SAPISID

Value: 7oaPxog-pZsJuuF5/AnUdDUIsJ9iJz2vdM

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: oQfNKjAsI121942918-

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

Expiry date: after 2 years

Name: SIDCC

Value: AN0-TYuqub2JOcDTyL

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

Expiry date: after 3 months

How long and where is the data stored?

The data YouTube receive and process on you are stored on Google's servers. Most of these servers are in America.

At <https://www.google.com/about/datacenters/inside/locations/?hl=en> you can see where Google's data centres are located. Your data is distributed across the servers. Therefore, the data can be retrieved quicker and is better protected against manipulation.

Google stores collected data for different periods of time. You can delete some data anytime, while other data are automatically deleted after a certain time, and still other data are stored by Google for a long time. Some data (such as elements on "My activity", photos, documents or products) that are saved in your Google account are stored until you delete them.

Moreover, you can delete some data associated with your device, browser, or app, even if you are not signed into a Google Account.

How can I erase my data or prevent data retention?

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

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

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

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

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

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

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

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

Legal basis

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

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

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


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

Font Awesome Privacy Policy

Font Awesome Privacy Policy Overview


 Affected parties: website visitors

 Purpose: service optimisation

 Processed data: data such as the IP address and loaded icon files

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

 Storage period: data is stored for a few weeks in unidentifiable form

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

What is Font Awesome?

On our website we use Font Awesome by the American company Fonticons (307 S. Main St., Suite 202, Bentonville, AR 72712, USA). Upon your visit to one of our websites, the Font Awesome web font, i.e. the icons, are loaded via the Font Awesome Content Delivery Network

(CDN). This way texts, fonts and icons are displayed appropriately on every device. In this privacy policy we will go into more detail on data storage and data processing by this service.

Icons play an increasingly important role on websites. Font Awesome is a web font specifically designed for web designers and web developers. With Font Awesome icons can for example be scaled and coloured as desired using the CSS stylesheet language. Thus, they now replace old picture icons. Font Awesome CDN is the easiest way to load icons or fonts onto your website. To do this, we only had to embed a short line of code into our website.

Why do we use Font Awesome on our website?

Font Awesome enables our websites' content to be depicted better. This eases your navigation on our website, and helps you grasp its content better. The icons can sometimes even be used to replace whole words and save space. This is particularly useful when optimising content specifically for smartphones. The icons are inserted as HTML code instead of as an image, which allows us to edit the icons with CSS exactly as we want. Simultaneously, Font Awesome also lets us improve our loading speed, as it only contains HTML elements and no icon images. All these advantages help us to make our website even clearer, faster and more refined for you.

Which data are stored by Font Awesome?

The Font Awesome Content Delivery Network (CDN) is used to load icons and symbols. CDNs are server networks that are distributed around the world. They make it possible to quickly load files from locations in close proximity. When you open one of our pages, the respective icons will be provided by Font Awesome.

For the web fonts to be loaded, your browser has to connect to the servers of Fonticons, Inc. For this, your IP address will be identified. Font Awesome also collects data on which icon files are downloaded, as well as when they are downloaded. Furthermore, technical data such as your browser version, screen resolution or the time when you accessed the page are also transmitted.

These data are collected and stored for the following reasons:

- to optimise Content Delivery Networks
- to identify and fix technical errors
- to protect CDNs from misuse and attacks
- to calculate fees from Font Awesome Pro customers
- to identify the popularity of icons
- to establish which computer and software you are using

If your browser does not allow web fonts, one of your PC's standard fonts will be used automatically. Moreover, as far as we are currently aware, no cookies will be set. We are keeping in contact with Font Awesome's privacy department and will let you know as soon as we find out more.

How long and where are the data stored?

Font Awesome stores data about the use of the Content Delivery Network also on servers in the United States of America. However, the CDN servers are located all across the world and store user data in your proximity. The data is usually only stored for a few weeks in an identifiable form. Aggregated statistics on the use of the CDNs may also be stored for longer. However, these do not include any personal data.

How can I erase my data or prevent data retention?

As far as we are aware, Font Awesome does not store any personal data via Content Delivery Networks. If you do not want data about the used icons to be stored, you will unfortunately not be able to visit our website. If your browser does not allow web fonts, no data will be transmitted or saved. In this case your computer's default font will be used.

Legal basis

If you have agreed to the use of Font Awesome, your consent is the legal basis for the corresponding data processing. According to **Art. 6 Paragraph 1 lit. a GDPR (consent)** this consent represents the legal basis for personal data processing, as can occur when it is collected by Font Awesome.

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

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

Font Awesome 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 Font Awesome 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

If you want to find out more about Font Awesome and their data handling, we recommend you to read their Privacy Policy at <https://fontawesome.com/privacy> along with the help page at <https://fontawesome.com/help>.

Google Fonts Privacy Policy


Google Fonts Privacy Policy Overview


 Affected parties: website visitors

 Purpose: service optimisation

 Processed data: data such as IP address, CSS and font requests

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

 Storage period: Google stores font files for one year

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

What are Google Fonts?

On our website we use Google Fonts, by the company Google Inc. (1600 Amphitheatre Parkway Mountain View, CA 94043, USA).

To use Google Fonts, you must log in and set up a password. Furthermore, no cookies will be saved in your browser. The data (CSS, Fonts) will be requested via the Google domains fonts.googleapis.com and fonts.gstatic.com. According to Google, all requests for CSS and fonts are fully separated from any other Google services. If you have a Google account, you do not need to worry that your Google account details are transmitted to Google while you use Google Fonts. Google records the use of CSS (Cascading Style Sheets) as well as the utilised fonts and stores these data securely. We will have a detailed look at how exactly the data storage works.

Google Fonts (previously Google Web Fonts) is a directory with over 800 fonts that Google provides its users free of charge.

Many of these fonts have been published under the SIL Open Font License license, while others have been published under the Apache license. Both are free software licenses.

Why do we use Google Fonts on our website?

With Google Fonts we can use different fonts on our website and do not have to upload them to our own server. Google Fonts is an important element which helps to keep the quality of our website high. All Google fonts are automatically optimised for the web, which saves data volume and is an advantage especially for the use of mobile terminal devices. When you use our website, the low data size provides fast loading times. Moreover, Google Fonts are secure Web Fonts. Various image synthesis systems (rendering) can lead to errors in different browsers, operating systems and mobile terminal devices. These errors could optically distort parts of texts or entire websites. Due to the fast Content Delivery Network (CDN) there are no cross-platform issues with Google Fonts. All common browsers (Google Chrome, Mozilla Firefox, Apple Safari, Opera) are supported by Google Fonts, and it reliably operates on most modern mobile operating systems, including Android 2.2+ and iOS 4.2+ (iPhone, iPad, iPod).

We also use Google Fonts for presenting our entire online service as pleasantly and as uniformly as possible.

Which data is stored by Google?

Whenever you visit our website, the fonts are reloaded by a Google server. Through this external cue, data gets transferred to Google's servers. Therefore, this makes Google recognise that you (or your IP-address) is visiting our website. The Google Fonts API was developed to reduce the usage, storage and gathering of end user data to the minimum needed for the proper depiction of fonts. What is more, API stands for „Application Programming Interface“ and works as a software data intermediary.

Google Fonts stores CSS and font requests safely with Google, and therefore it is protected. Using its collected usage figures, Google can determine how popular the individual fonts are. Google publishes the results on internal analysis pages, such as Google Analytics. Moreover, Google also utilises data of its own web crawler, in order to determine which websites are using Google fonts. This data is published in Google Fonts' BigQuery database. Entrepreneurs and developers use Google's webservice BigQuery to be able to inspect and move big volumes of data.

One more thing that should be considered, is that every request for Google Fonts automatically transmits information such as language preferences, IP address, browser version, as well as the browser's screen resolution and name to Google's servers. It cannot be clearly identified if this data is saved, as Google has not directly declared it.

How long and where is the data stored?

Google saves requests for CSS assets for one day in a tag on their servers, which are primarily located outside of the EU. This makes it possible for us to use the fonts by means of a Google stylesheet. With the help of a stylesheet, e.g. designs or fonts of a website can get changed swiftly and easily.

Any font related data is stored with Google for one year. This is because Google's aim is to fundamentally boost websites' loading times. With millions of websites referring to the same fonts, they are buffered after the first visit and instantly reappear on any other websites that are visited thereafter. Sometimes Google updates font files to either reduce the data sizes, increase the language coverage or to improve the design.

How can I erase my data or prevent it being stored?

The data Google stores for either a day or a year cannot be deleted easily. Upon opening the page this data is automatically transmitted to Google. In order to clear the data ahead of time, you have to contact Google's support at <https://support.google.com/?hl=en-GB&tid=121942918>. The only way for you to prevent the retention of your data is by not visiting our website.

Unlike other web fonts, Google offers us unrestricted access to all its fonts. Thus, we have a vast sea of font types at our disposal, which helps us to get the most out of our website. You

can find out more answers and information on Google Fonts at <https://developers.google.com/fonts/faq?tid=121942918>. While Google does address relevant elements on data protection at this link, it does not contain any detailed information on data retention.

It proves rather difficult to receive any precise information on stored data by Google.

Legal basis

If you have consented to the use of Google Fonts, 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 it is processed by Google Fonts.

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

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

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


You can find more information on which data is generally retained by Google and what this data is used at <https://policies.google.com/privacy?hl=en-GB>.

Google Maps Privacy Policy

Google Maps Privacy Policy Overview


 Affected parties: website visitors

 Purpose: service optimisation

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

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

 Storage duration: depending on the retained data

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

What is Google Maps?

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

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

Why do we use Google Maps on our website?

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

What data is stored by Google Maps?

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

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

Name: NID

Value: 188=h26c1Ktha7fCQTx8rXgLyATyITJ121942918-5

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

Expiration date: after 6 months

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

How long and where is the data stored?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Legal basis

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

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

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


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


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

Google reCAPTCHA Privacy Policy

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)

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 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. reCAPTCHA and Captchas in general are used every time bots could manipulate or misuse certain actions (such as registrations, surveys, etc.).

Why do we use reCAPTCHA on our website?

We only want to welcome people from flesh and bones 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.

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-121942918-8

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: U7j1v3dZa1219429180xgZFmiqWppRWKOr

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: 0WmuWqy121942918zILzqV_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: gEAABBCjJMXcl0dSAAAANbqc121942918-4

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.

How long and where are the data stored?

Due to the integration of reCAPTCHA, your data will be transferred to the Google server. Google have not disclosed where exactly this data is stored, despite repeated inquiries. But even without confirmation from Google, it can be assumed that data such as mouse interaction, length of stay on a website or language settings are stored on the European or American Google servers. 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.

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=121942918>.

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.

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

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

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>.

All texts are copyrighted.