

Privacy Policy

Privacy Policy Introduction and Overview

We have written this privacy policy (version 07.02.2026-113102646) in order to explain to you, in accordance with the provisions of the [General Data Protection Regulation \(EU\) 2016/679](#) and applicable national laws, which personal data (data for short) we as the controller – and the processors commissioned by us (e.g. providers) – process, will process in the future and what legal options you have. The terms used are to be considered gender-neutral.

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

Privacy policies usually sound very technical and use legal terminology. However, this privacy policy is intended to describe the most important things to you as simply and transparently as possible. So long as it aids transparency, technical **terms are explained in a reader-friendly manner, links** to further information are provided and **graphics** are used. We are thus informing in clear and simple language that we only process personal data in the context of our business activities if there is a legal basis for it. This is certainly not possible with brief, unclear and legal-technical statements, as is often standard on the internet when it comes to data protection. I hope you find the following explanations interesting and informative. Maybe you will also find some information that you have not been familiar with.

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

Scope

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

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

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

Legal bases

In the following privacy policy, we provide you with transparent information on the legal principles

and regulations, i.e. the legal bases of the General Data Protection Regulation, which enable us to process personal data.

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

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

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

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

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

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

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

Contact details of the data protection controller

If you have any questions about data protection or the processing of personal data, you will find below the contact details of the controller in accordance with Article 4(7) of the EU General Data Protection Regulation (GDPR):

AdSimple GmbH
Fabriksgasse 20,
2230 Gänserndorf,
Österreich

E-Mail: office@chatreact.ai

Phone: [+43 2282 60 715](tel:+43228260715)

Company details: <https://www.chatreact.ai/imprint/>

Storage Period

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

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

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

Rights in accordance with the General Data Protection Regulation

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

- According to Article 15 DSGVO, you have the right to information about whether we are processing data about you. If this is the case, you have the right to receive a copy of the data and to know the following information:
 - for what purpose we are processing;
 - the categories, i.e. the types of data that are processed;
 - who receives this data and if the data is transferred to third countries, how security can be guaranteed;
 - how long the data will be stored;
 - the existence of the right to rectification, erasure or restriction of processing and the right to object to processing;
 - that you can lodge a complaint with a supervisory authority (links to these authorities can be found below);
 - the origin of the data if we have not collected it from you;
 - Whether profiling is carried out, i.e. whether data is automatically evaluated to arrive at a personal profile of you.
- You have a right to rectification of data according to Article 16 GDPR, which means that we must correct data if you find errors.
- You have the right to erasure (“right to be forgotten”) according to Article 17 GDPR, which specifically means that you may request the deletion of your data.
- According to Article 18 of the GDPR, you have the right to restriction of processing, which means that we may only store the data but not use it further.

- According to Article 20 of the GDPR, you have the right to data portability, which means that we will provide you with your data in a standard format upon request.
- According to Article 21 DSGVO, you have the right to object, which entails a change in processing after enforcement.
 - If the processing of your data is based on Article 6(1)(e) (public interest, exercise of official authority) or Article 6(1)(f) (legitimate interest), you may object to the processing. We will then check as soon as possible whether we can legally comply with this objection.
 - If data is used to conduct direct advertising, you may object to this type of data processing at any time. We may then no longer use your data for direct marketing.
 - If data is used to conduct profiling, you may object to this type of data processing at any time. We may no longer use your data for profiling thereafter.
- According to Article 22 of the GDPR, you may have the right not to be subject to a decision based solely on automated processing (for example, profiling).
- You have the right to lodge a complaint under Article 77 of the GDPR. This means that you can complain to the data protection authority at any time if you believe that the data processing of personal data violates the GDPR.

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

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

Austria Data protection authority

Manager: Dr. Matthias Schmidl

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 scope of the GDPR (third countries) if you consent to this processing or if there is another legal permission. This is particularly true when processing is legally required or necessary for the performance of a contractual relationship, and in any case, only to the extent permitted by law. Your consent is in most cases the primary reason for us to process data in third countries. Processing of personal data in third countries such as the USA, where many software providers offer services and have their server locations, may mean that personal data is processed and stored in unexpected ways.

We explicitly point out that, according to the opinion of the European Court of Justice, there is currently only an adequate level of protection for data transfers to the USA if a US company processing personal data of EU citizens in the USA is an active participant in the EU-US Data Privacy Framework. More information can be found at:

https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en

Data processing by US services that are not active participants in the EU-US Data Privacy Framework may result in data not being anonymized and processed, if applicable. Additionally, US government authorities may potentially have access to individual data. Furthermore, it may occur that collected data is linked with data from other services of the same provider, if you have a corresponding user account. Where possible, we try to use server locations within the EU, if offered.

We will inform you in the appropriate sections of this privacy policy in more detail about data transfers to third countries, if applicable.

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

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

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

What are cookies?

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

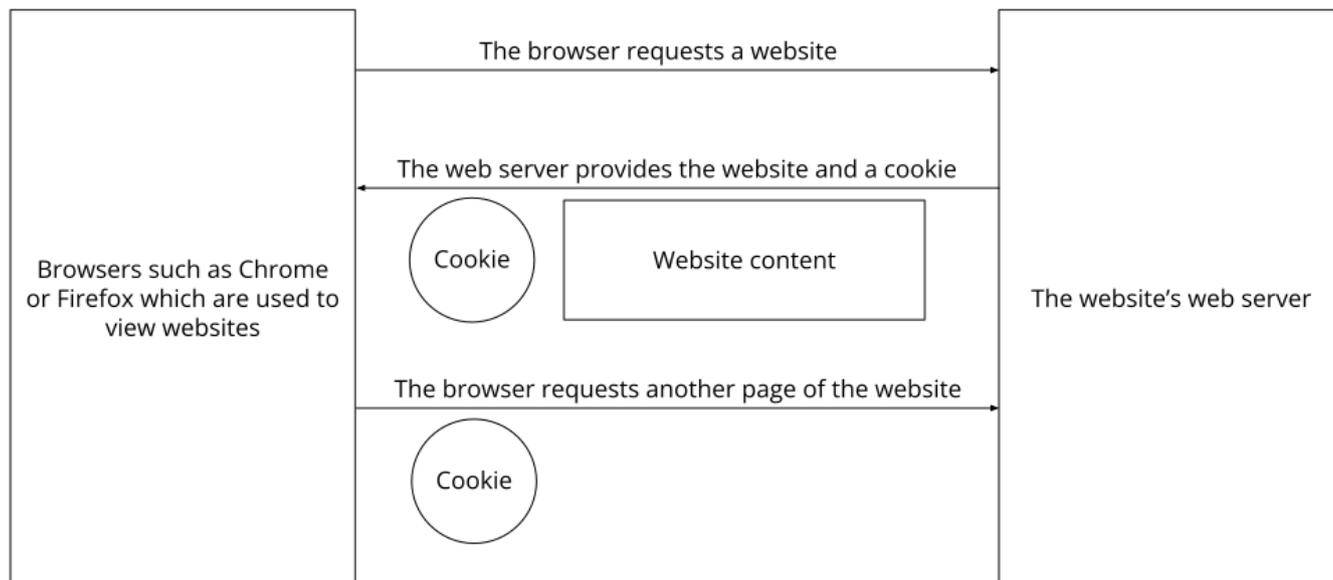
In the following we explain what cookies are and why they are used, so that you can better understand the following privacy policy.

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

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

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

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



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

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

Name: _ga

Value: GA1.2.1326744211.152113102646-9

Purpose: Differentiation between website visitors

Expiry date: after 2 years

A browser should support these minimum sizes:

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

Which types of cookies are there?

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

There are 4 different types of cookies:

Essential cookies

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

Purposive cookies

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

Target-orientated cookies

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

Advertising cookies

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

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

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

Purpose of processing via cookies

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

Which data are processed?

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

Storage period of cookies

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

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

Right of objection – how can I erase cookies?

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

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

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

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

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

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

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

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

Legal basis

The so-called “cookie directive” has existed since 2009. It states that the storage of cookies requires your **consent** (Article 6 Paragraph 1 lit. a GDPR). Within countries of the EU, however, the reactions to these guidelines still vary greatly. In Austria, however, this directive was implemented in Section 165 (3) of the Telecommunications Act (2021). In Germany, the cookie guidelines have not been implemented as national law. Instead, this guideline was largely implemented in Section 15 (3) of the Telemedia Act (TMG), which has been replaced by the Digital Services Act (DSA) since May 2024.

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.

Contact Form

Contact Form Summary

 Data Subjects: Website visitors who enter data into a contact form

 Purpose: Processing inquiries and communication in the context of pre-contractual measures or existing interest in our services

 Processed Data: Name, email address, phone number (if provided), message content, IP address, technical metadata (e.g., timestamp, browser information)

 Storage Duration: Data will be deleted as soon as it is no longer necessary for processing the inquiry and no legal retention obligations apply.

Legal Bases: Consent (Art. 6 para. 1 lit. a GDPR), Legitimate Interest (Art. 6 para. 1 lit. f GDPR), Contract or pre-contractual measures (Art. 6 para. 1 lit. b GDPR)

What is a contact form?

A contact form is a web form you can fill out on our website to get in touch with us easily. Typically, personal data such as your name, email address, and your message are transmitted to us. This information helps us respond to your inquiries more effectively and contact you directly.

Why do we use a contact form?

We offer a contact form to make it quick and easy for you to communicate with us. Whether you have questions about our services, want to give feedback, or have other concerns – the contact form allows you to reach out directly. The information you provide will be used solely to process your inquiry and to contact you. If the inquiry leads to further steps, such as providing an offer or entering into a contract, we may also use the data for those purposes.

What data is processed?

The specific data we process depends on the information you provide in the contact form. In general, this includes:

- Name
- Email address
- Phone number (optional)
- Message content
- Date and time of submission
- IP address and technical metadata (for security and traceability)

This information helps us understand and respond to your inquiry more efficiently.

How long is the data stored?

We store contact form data only as long as necessary to process your inquiry. If a business relationship arises, the same retention periods as for customer data apply. In certain cases (e.g., legal disputes), longer retention periods may be required. Of course, we do not share your data with third parties without your explicit consent.

Legal basis

The legal bases for processing your data via the contact form are Art. 6 para. 1 lit. a GDPR (consent – by submitting the form), Art. 6 para. 1 lit. b GDPR (pre-contractual measures), and Art. 6 para. 1 lit. f GDPR (legitimate interest – efficient communication and organization of inquiries). If you voluntarily provide special categories of personal data, processing is based on Art. 9 para. 2 lit. a GDPR (explicit consent).

Customer Data

Customer Data Overview

 Affected parties: Customers or business and contractual partners

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

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

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

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

What is customer data?

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

Why do we process customer data?

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

What data is processed?

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

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

- Name
- Contact address
- Email address
- Phone number
- Your birthday
- Payment data (invoices, bank details, payment history, etc.)
- Contract data (duration, contents)

- Usage data (websites visited, access data, etc.)
- Metadata (IP address, device information)

How long is the data stored?

We erase corresponding customer data as soon as we no longer need it to fulfill our contractual obligations and purposes, and as soon as the data is also no longer necessary for possible warranty and liability obligations. This can for example be the case when a business contract ends.

Thereafter, the limitation period is usually 3 years, although longer periods may be possible in individual cases. Of course, we also comply with the statutory retention requirements. Your customer data will certainly not be passed on to third parties unless you have given your explicit consent.

Legal Basis

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

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

Registration

Registration Overview

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

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

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

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

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

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

Please only enter the data we need for the registration. In case you are registering on behalf of a third party, please only enter data for which you have the approval of the party you are registering

for. If possible, use a secure password that you don't use anywhere else and an email address that you check regularly.

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

What is a registration?

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

Why do we process personal data?

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

Which data is processed?

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

During registration, we process the following types of data:

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

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

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

Storage time

We store the entered data for at least as long as the account associated with the data exists with us and is in use – and as long as there are contractual obligations between you and us. In case the

contract ends, we retain the data until the respective claims get time-barred. Moreover, we store your data as long as we are subject to legal storage obligations, if applicable. Following that, we keep any accounting records (invoices, contract documents, account statements, etc.) of the contract for 10 years (§ 147 AO) and other relevant business documents for 6 years (§ 247 HGB) after accrual.

Right to object

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

Legal Basis

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

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

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

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

Registration with real names

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

Registration with pseudonyms

You can use a pseudonym for the registration, which means you don't have to register with your real name. This ensures that your real name cannot be processed by us.

Storage of the IP address

During registration, login and account use, we store your IP address for security reasons in order to

be able to determine legitimate use.

Public Profile

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

Two Factor Authentication (2FA)

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

Web hosting

Web hosting Overview

 Affected parties: visitors to the website

 Purpose: professional hosting of the website and security of operations

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

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

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

What is web hosting?

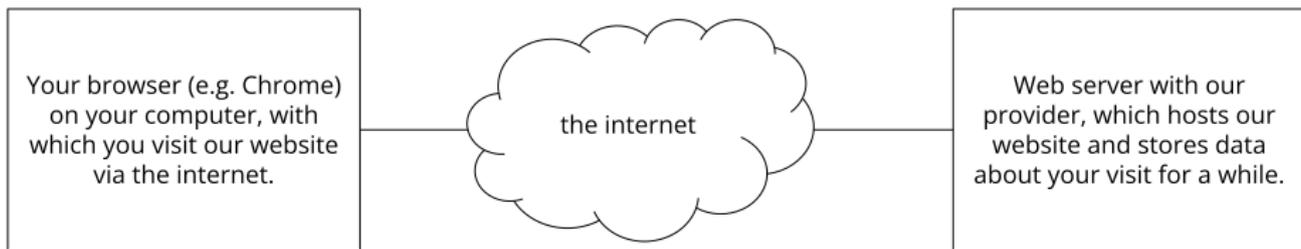
Every time you visit a website nowadays, certain information – including personal data – is automatically created and stored, including on this website. This data should be processed as sparingly as possible, and only with good reason. By website, we mean the entirety of all websites on your domain,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

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

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

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

Illustration:



Why do we process personal data?

The purposes of data processing are:

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

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=113102646>)
- 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.

Amazon Web Services (AWS) Privacy Policy

We use Amazon Web Services (AWS) for our website, which is a web hosting provider, among other things. The provider of this service is the American company Amazon Web Services, Inc., 410 Terry Avenue North, Seattle WA 98109, USA.

Amazon processes data from you, among other things, in the USA. Amazon is an active participant in the EU-US Data Privacy Framework, which regulates the correct and secure transfer of personal data from EU citizens to the USA. More information can be found at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Additionally, Amazon uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Amazon commits to maintaining the European data protection level when processing your relevant data, even if the data is stored, processed, and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the decision and the corresponding Standard Contractual Clauses here: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

The Amazon data processing terms and conditions (Data Processing Addendum), which correspond to the standard contractual clauses, can be found at https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf.

You can find out more about the data that are processed through the use of Amazon Web Services (AWS) in their Privacy Policy at https://aws.amazon.com/privacy/?nc1=h_ls.

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.

Amazon Simple Email Service Privacy Policy

We also use the email marketing tool Amazon Simple Email Service. The provider of this service is the American company Amazon Web Services, Inc., 410 Terry Avenue North, Seattle WA 98109, USA.

Amazon processes data from you, among other things, in the USA. Amazon is an active participant in the EU-US Data Privacy Framework, which regulates the correct and secure transfer of personal data from EU citizens to the USA. More information can be found at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Additionally, Amazon uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Amazon commits to maintaining the European data protection level when processing your relevant data, even if the data is stored, processed, and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the decision and the corresponding Standard Contractual Clauses here: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

The Amazon data processing terms and conditions (Data Processing Addendum), which correspond to the standard contractual clauses, can be found at https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf.

You can find out more about the data that is processed through the use of Amazon Simple Email Service in their Privacy Policy at https://aws.amazon.com/privacy/?nc1=f_pr.

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

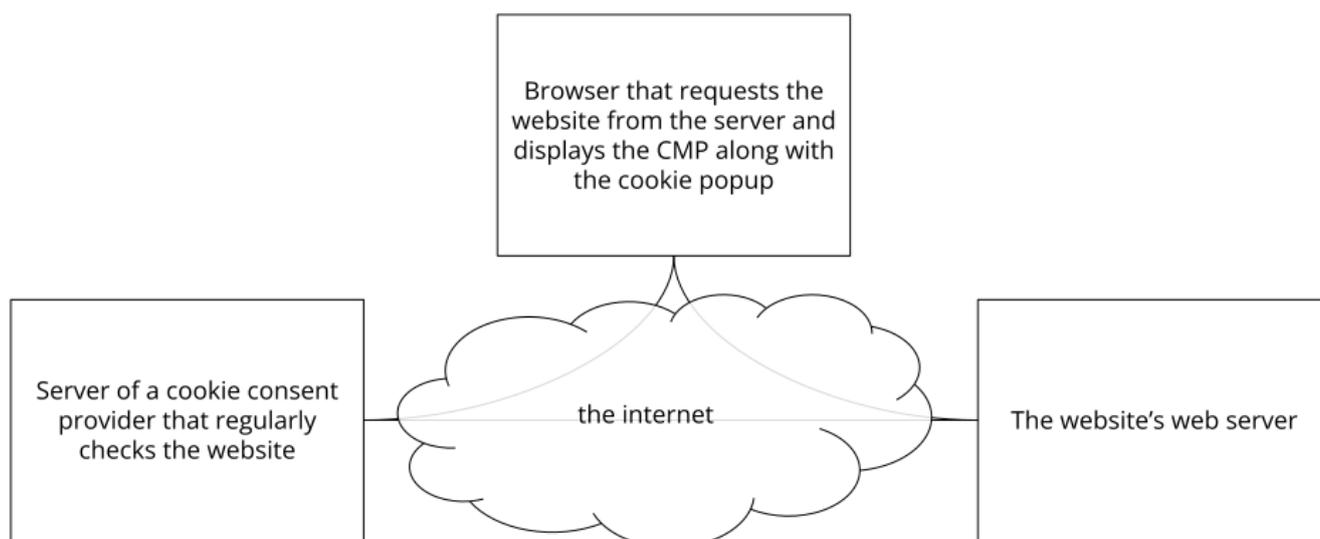
 Processed data: data for managing cookie settings such as IP address, time of consent, type of consent and individual consent. You can find more details on this directly with the tool that is being used.

 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).

AdSimple Consent Manager Privacy Policy

AdSimple Consent Manager Privacy Policy Overview

 Affected parties: Website visitors

 Purpose: Obtaining 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 under in the privacy policy below.

 Storage period: the used cookie expires after one year

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

What is the AdSimple Consent Manager?

On our website we use the AdSimple Consent Manager of the software development and online marketing company AdSimple GmbH, Fabriksgasse 20, 2230 Gänserndorf, Austria. The AdSimple Consent Manager offers us, among other things, the opportunity to provide you with a cookie notice that is comprehensive and compliant with data protection laws. This gives you the opportunity to decide which cookies you want to allow or deny. By using this software, data is sent from you to AdSimple, where it is stored. In this privacy policy we inform you on why we use the AdSimple Consent Manager, which data is transferred and stored and how you can prevent this data transfer.

The AdSimple Consent Manager is a software that scans our website to identify and categorise all existing cookies. Additionally, you as the website visitor will be informed on the use of cookies via a cookie notice script. Then you can decide yourself which cookies you want to allow or deny.

Why do we use the AdSimple Consent Manager on your website?

We want to offer you maximum transparency when it comes to data protection. Before we can do so, we need to exactly determine which cookies have ended up on our website over time. Since the AdSimple consent manager regularly scans our website and locates all cookies, we have full control over these cookies and can therefore act in compliance with the GDPR. This enables us to inform you precisely on the use of cookies on our website.

Moreover, you will always receive an up-to-date cookie notice that is data-protection compliant. This enables you to decide yourself which cookies you want to allow or deny via the checkbox system.

Which data are stored by the AdSimple Consent Manager?

If you agree to cookies on our website, AdSimple Consent Manager will set the following cookie:

Name: acm_status

Value: "":true,"statistics":true,"marketing":true,"socialmedia":true,"settings":true}

Purpose: This cookie saves the status of your consent. This enables our website to read and adhere to the latest status, even during future visits.

Expiry date: after one year

How long and where are the data stored?

All data collected by the AdSimple Consent Manager is transferred and stored exclusively within the European Union. The collected data is stored on the AdSimple servers at Hetzner GmbH in Germany. Therefore, only AdSimple GmbH and Hetzner GmbH have access to the data.

How can I erase my data or prevent data retention?

You have the right to access and delete your personal data at any time. You can prevent data collection and storage by for example rejecting the use of cookies via the cookie notification script. Another option to prevent data processing or to manage it according to your wishes is your browser. Depending on the browser you use, managing cookies differs slightly. Below you will find links to the instructions for the most common browsers:

[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

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 (1) (a) GDPR), this consent is also the legal basis for the use of cookies and the processing of your data. The AdSimple Consent Manager is used to manage your consent to cookies and to enable you to give your consent. 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 (1) lit.f GDPR).

We hope we were able to provide you with a good overview of data traffic and data processing by AdSimple Consent Manager. If you want to learn more about this tool, we recommend the description page at <https://www.adsimple.at/consent-manager/>.

Payment providers

Payment Providers Privacy Policy Overview

 Affected parties: visitors to the website

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

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

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

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

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

What is a payment provider?

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

Why do we use payment providers on our website?

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

Which data are processed?

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

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

Duration of data processing

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

Right to object

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

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

Legal basis

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

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

Stripe Privacy Policy

Stripe Privacy Policy Overview

 Affected parties: website visitors

 Purpose: optimising the payment process on our website

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

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

 Storage period: data is stored until the collaboration with Stripe is terminated

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

What is Stripe?

On our website we use a payment tool by Stripe, an American technology company and online payment service. Stripe Payments Europe (Europe Ltd., 1 Grand Canal Street Lower, Grand Canal

Dock, Dublin, Ireland) is responsible for customers within the EU. Therefore, if you choose Stripe as your payment method, your payment will be processed via Stripe Payments. Hence, the data required for the payment process is forwarded to Stripe where it is then stored. In this privacy policy we will give you an overview of Stripe's data processing and retention. Moreover, we will explain why we use Stripe on our website.

The technology company Stripe offers payment solutions for online payments. Stripe enables us to accept credit and debit card payments in our webshop while it handles the entire payment process. A major advantage of Stripe is that you never have to leave our website or shop during the payment process. Moreover, payments are processed very quickly via Stripe.

Why do we use Stripe on our website?

We of course want to offer the best possible service with both our website and our integrated online shop. After all, we would like you to feel comfortable on our site and take advantage of our offers. We know that your time is valuable and therefore, payment processing in particular must work quickly and smoothly. In addition to our other payment providers, with Stripe we have found a partner that guarantees secure and fast payment processing.

What data are stored by Stripe?

If you choose Stripe as your payment method, your personal data (transaction data) will be transmitted to Stripe where it will be stored. These data include the payment method (i.e. credit card, debit card or account number), bank sort code, currency, as well as the amount and the payment date. During a transaction, your name, email address, billing or shipping address and sometimes your transaction history may also be transmitted. These data are necessary for authentication. Furthermore, Stripe may also collect relevant data for the purpose of fraud prevention, financial reporting and for providing its services in full. These data may include your name, address, telephone number as well as your country in addition to technical data about your device (such as your IP address).

Stripe does not sell any of your data to independent third parties, such as marketing agencies or other companies that have nothing to do with Stripe. However, data may be forwarded to internal departments, a limited number of Stripe's external partners or for legal compliance reasons. What is more, Stripe uses cookies to collect data. Here is a selection of cookies that Stripe may set during the payment process:

Name: m

Value: edd716e9-d28b-46f7-8a55-e05f1779e84e040456113102646-5

Purpose: This cookie appears when you select your payment method. It saves and recognises whether you are accessing our website via a PC, tablet or smartphone.

Expiry date: after 2 years

Name: __stripe_mid

Value: fc30f52c-b006-4722-af61-a7419a5b8819875de9113102646-1

Purpose: This cookie is required for carrying out credit card transactions. For this purpose, the

cookie stores your session ID.

Expiry date: after one year

Name: __stripe_sid

Value: 6fee719a-c67c-4ed2-b583-6a9a50895b122753fe

Purpose: This cookie also stores your ID. Stripe uses it for the payment process on our website.

Expiry date: after end of the session

How long and where are the data stored?

Generally, personal data are stored for the duration of the provided service. This means that the data will be stored until we terminate our cooperation with Stripe. However, in order to meet legal and official obligations, Stripe may also store personal data for longer than the duration of the provided service. Furthermore, since Stripe is a global company, your data may be stored in any of the countries Stripe offers its services in. Therefore, your data may be stored outside your country, such as in the USA for example.

How can I erase my data or prevent data retention?

Please note that when you use 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 simply be transferred to, as well as stored and processed in insecure third countries, unless there are suitable guarantees (such as EU standard contractual clauses) between us and the respective non-European service provider.

You always reserve the right to information, correction and deletion of your personal data. Should you have any questions, you can contact the Stripe team at <https://support.stripe.com/contact/email>.

You can erase, deactivate or manage cookies in your browser that Stripe uses for its functions. This works differently depending on which browser you are using. Please note, however, that if you do so the payment process may no longer work. 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](#)

Legal basis

For the processing of contractual or legal relationships (**Art. 6 para. 1 lit. b GDPR**), we offer the payment service provider Sofortüberweisung in addition to the conventional bank/credit

institutions. Successful use of the service also requires your **consent (Art. 6 para. 1 lit. a GDPR)**, provided the use of cookies is necessary for it.

Stripe processes data from you, among other things, in the USA. Stripe is an active participant in the EU-US Data Privacy Framework, which regulates the correct and secure transfer of personal data from EU citizens to the USA. More information can be found at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Additionally, Stripe uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Stripe commits to maintaining the European data protection level when processing your relevant data, even if the data is stored, processed, and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the decision and the corresponding Standard Contractual Clauses here: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

We have now given you a general overview of Stripe's data processing and retention. If you want more information, Stripe's detailed privacy policy at <https://stripe.com/privacy> is a good source.

External Online Platforms Introduction

External Online Platforms Privacy Policy Overview

 Affected parties: website visitors or visitors to the external online platforms

 Purpose: Presentation and optimisation of our service, as well as establishing contact with visitors & interested parties

 Data processed: data such as phone numbers, email addresses, contact details, user behaviour data, information about your device and your IP address.
More details can be found directly with the respective platform used.

 Storage duration: depends on the platforms used

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

What are external online platforms?

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

Why do we use external online platforms?

In addition to our website, we also want to display our offer on other platforms in order to reach more customers. External online marketplaces such as Amazon, eBay or Digistore24 offer large sales websites that show our products to people who may not know our website. Moreover, built-in elements on our site may also lead to an external online platform. Any data that is processed and stored by the respective online platform is used by the business to log the payment process and also to conduct web analyses.

The aim of these analyses is to enable the development of more precise and personal marketing and advertising strategies. Depending on your interaction with a platform, the evaluated data may be used to draw appropriate conclusions about your interests and to create a so-called user profile on you. This also allows the platforms to show customised advertisements or products to you. For this purpose, cookies are usually set in your browser in order to store data on your usage behaviour.

Please note that when using the platforms or our built-in elements, your data may also be processed outside the European Union, since online platforms such as Amazon or eBay are American companies. As a result, you may not be able to claim or enforce your rights in relation to your personal data as easily.

Which data is processed?

Exactly which data is stored and processed depends on the respective external platform. But usually, it is data such as phone numbers, email addresses, data you enter in a contact form, along with user data (e. g. which buttons you click and which pages you view during your visit), as well as information about your device and IP address. In most cases, the majority of this data is stored in cookies. If you have a profile on an external platform and are logged in there, your data can be linked to any such profile. The collected data is stored on the servers of the platforms used, where it is processed. You can find out exactly how an external platform stores, manages and processes data in the respective privacy policy. If you have any questions about data storage and data processing, or if you want to assert corresponding rights, we recommend that you contact the platform directly.

Duration of data processing

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

Right to object

You also have the right and the opportunity to revoke your consent to the use of cookies at any time. This can be done either via our cookie management tool or via opt-out functions on the respective external platform. You can also prevent data collection through cookies by managing,

deactivating or erasing the cookies in your browser.

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

Legal Basis

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

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

Amazon (Europe) Privacy Policy

We also use the online trading platform Amazon (Europe). The provider of this service is the American company Amazon Inc. The responsible entity for the European region is the company Amazon Europe Core S.à r.l. (Société à responsabilité limitée), 38 avenue John F. Kennedy, L-1855 Luxembourg.

Amazon processes data from you, among other things, in the USA. Amazon is an active participant in the EU-US Data Privacy Framework, which regulates the correct and secure transfer of personal data from EU citizens to the USA. More information can be found at

https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Additionally, Amazon uses so-called Standard Contractual Clauses (Article 46(2) and (3) GDPR). Standard Contractual Clauses (SCC) are template clauses provided by the EU Commission and are designed to ensure that your data complies with European data protection standards, even when transferred and stored in third countries (such as the USA). Through the EU-US Data Privacy Framework and the Standard Contractual Clauses, Amazon commits to maintaining the European data protection level when processing your relevant data, even if the data is stored, processed, and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the decision and the corresponding Standard Contractual Clauses here:

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

Amazon's data processing addendum (AWS GDPR DATA PROCESSING), which corresponds to the standard contractual clauses, can be found at

https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf.

You can find out more about the data that is processed by Amazon in their Privacy Policy at

https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010&ref_=footer_privacy.

OpenAI Privacy Policy

OpenAI Privacy Policy Overview

 Affected parties: website visitors

 Purpose: Optimization of the website offering.

 Processed data: Depending on the inputs and previous settings. More details can be found below in this privacy policy.

 Storage period: Data is generally stored as long as it 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)

We use the application programming interface (API) of the US-based company OpenAI for our website. The service provider is OpenAI OpCo, LLC, located at 3180 18th Street, San Francisco, CA, USA.

What is OpenAI?

OpenAI specializes in the development of artificial intelligence (AI) and machine learning. The company was founded by a group of researchers and technology entrepreneurs, with the two most well-known founders being Elon Musk and Sam Altman. OpenAI's mission is to promote the development of AI systems while ensuring that the technology has a societal benefit. OpenAI's most well-known product is ChatGPT, but the company also offers other products that we can access through the API interface.

Why do we use OpenAI services on our website?

We use services from OpenAI on our website to provide you with a better and interactive user experience. With the help of OpenAI tools, you can directly interact with our website and ask questions, for example. If ChatGPT satisfactorily answers your questions, it provides you with quick assistance, saving you from waiting for an email response from us. The tool is available to you at any time, day or night, enhancing our customer service and improving your user experience on our website. We also utilize OpenAI products to develop our own solutions and applications for our company.

What data is stored by OpenAI products?

The data that is stored depends on your inputs and the specific AI tool being used. All inputs made in the tool are processed. OpenAI generally processes natural language, images, and other data formats that can be used to train machine learning models. This data is used to improve or train the capabilities of the respective tool. When using OpenAI products, your IP address is processed. However, as a general rule, unless you enter personal data, these data (except for the IP address) are not processed or stored. All entered data is anonymized and encrypted to protect your privacy to the best extent possible. The tool does not use cookies to store or process data without your consent. The entered data is solely used to improve the quality of the AI results.

Here is an overview of the most commonly collected data by OpenAI products:

- Information about the content of the chat conversations
- Information about the type of questions asked
- Information about device type, browser, and operating system
- Information about the user's IP address
- Audio recordings
- Image inputs

How long and where are the data stored?

In general, the entered data is stored by OpenAI because the tools use the relevant data to train themselves. However, there is also a function that allows us to disable chat history, so that the data cannot be used for training purposes. If we activate this function, ChatGPT or OpenAI will only store your data for 30 days after it has been collected or entered by you.

If you choose to enter personal data such as your email address or name, these pieces of information may also be permanently stored in a database. However, before this happens, your consent for data processing must be obtained.

How can I delete my data or prevent data storage?

Under the data protection law of the European Union, you have the right to access, update, delete, or restrict your data. However, you can only prevent complete data processing by not using OpenAI products.

Legal basis for the processing of personal data

If personal data is collected, the use of OpenAI products requires consent. According to Art. 6(1)(a) of the GDPR (Consent), this consent serves as the legal basis for the processing of personal data by OpenAI products.

In addition to consent, we also have a legitimate interest in optimizing our service to improve our offering technically and economically. With the help of OpenAI products, we enhance your user experience on our website and expand our support services. The legal basis for this is provided by Art. 6(1)(f) of the GDPR (Legitimate interests).

OpenAI processes your data, among other things, in the United States. We would like to inform you that, according to the opinion of the European Court of Justice, there is currently no adequate level of protection for data transfers to the United States. This may entail various risks for the legality and security of data processing.

As the basis for data processing involving recipients located in third countries (outside the European Union, Iceland, Liechtenstein, Norway, especially the United States) or the transfer of data to such countries, OpenAI uses standard contractual clauses (= Art. 46(2) and (3) of the GDPR). Standard contractual clauses (SCC) are template agreements provided by the European Commission and are designed to ensure that your data is processed in compliance with European data protection standards, even when transferred and stored in third countries (such as the United States). Through these clauses, OpenAI commits to complying with the European data protection

level when processing your personal data, even if the data is stored, managed, or otherwise processed in the United States. We have also agreed on the applicability of the SCC within our contractual relationship with OpenAI. These clauses are based on an implementing decision of the European Commission (Implementing Decision (EU) 2021/914 of the Commission of June 4, 2021). You can find the decision and the corresponding standard contractual clauses, among other things, here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=en

We hope that we have provided you with the essential information about the data processing by OpenAI. You can learn more about the data processing by OpenAI in the privacy policy at <https://openai.com/policies/privacy-policy>.

Vercel Privacy Policy

We use Vercel on our website, which is a cloud deployment platform. The provider of this service is the American company Vercel Inc., 340 S Lemon Ave #4133, Walnut, CA 91789.

Vercel 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.

Vercel 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, Vercel 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 the Data Processing Addendum, which corresponds to the Standard Contractual Clauses at <https://vercel.com/legal/dpa>.

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

Explanation of the terminology used

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

are definitions, we will also list the GDPR texts here and add our own further explanations if necessary.

Processor

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Consent

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Data concerning health

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

“Data concerning health” means personal data related to the physical or mental health of

a natural person, including the provision of health care services, which reveal information about his or her health status;

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

Personal Data

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

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

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

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

health Data

- Data relating to sexual orientation or sex life

Profiling

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Controller

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Processing

Definition according to Article 4 of the GDPR

For the purposes of this Regulation, the term means:

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

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

Closing Remarks

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

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

If you have any questions about data protection on our website, please do not hesitate to contact us or the responsible body. We wish you all the best and hope to soon welcome you to our website again.

All texts are copyrighted.