



SIGN8 GmbH
Fürstenrieder Str. 5
80687 München

T: +49 89 2153 7472 000
info@sign8.eu
www.sign8.eu

Privacy Policy

Data protection is a matter of trust, and we are aware of the responsibility that comes with it. We respect your privacy and your rights and are committed to handling personal data responsibly, transparently and in full compliance with applicable legal requirements.

In principle, it is possible to use the websites of SIGN8 GmbH without providing any personal data. However, if a data subject wishes to make use of specific services offered by our company via our website, the processing of personal data may become necessary. If the processing of personal data is required and there is no statutory basis for such processing, we generally obtain the consent of the data subject.

The processing of personal data, such as a data subject's name, address, email address or telephone number, is always carried out in compliance with applicable laws, in particular the General Data Protection Regulation (GDPR) and the country-specific data protection provisions applicable to SIGN8 GmbH.

By means of this Privacy Policy, our company seeks to inform the public about the nature, scope and purpose of the personal data collected, used and processed by us. Furthermore, this Privacy Policy informs data subjects about their rights.

As the controller responsible for the processing, SIGN8 GmbH has implemented numerous technical and organizational measures to ensure the most complete protection possible of personal data processed via this website. Nevertheless, internet-based data transmissions may in principle have security vulnerabilities, so that absolute protection cannot be guaranteed. For this reason, each data subject is free to transmit personal data to us by alternative means, for example by telephone.

Content

§ 1	Overview of data protection at SIGN8.....	2
§ 2	Hosting	3
§ 3	General information and mandatory information.....	3
§ 4	Recording of data on this website.....	7
§ 5	Analysis tools and advertising.....	10
§ 6	Newsletter	11
§ 7	Plug-ins and Tools	12
§ 8	eCommerce and payment service providers	13
§ 9	Handling applicant data	13
§ 10	Data Processing in the Context of Our (Qualified) Trust Services	14

§ 1 Overview of data protection at SIGN8

1.1. General information

The following information will provide you with an easy to navigate overview of what will happen with your personal data when you visit this website and use our trust services. The term “personal data” comprises all data that can be used to personally identify you.

1.2. Data recording on this website

a) Who is the responsible party for the recording of data on this website (i.e., the “controller”)?

The data on this website is processed by the operator of the website, whose contact information is available under section “Information about the responsible party (referred to as the “controller” in the GDPR) in this Privacy Policy.

b) How do we record your data?

We collect your data as a result of your sharing of your data with us. This may, for instance be information you enter into our contact form.

Other data shall be recorded by our IT systems automatically or after you consent to its recording during your website visit. This data comprises primarily technical information (e.g., web browser, operating system, or time the site was accessed). This information is recorded automatically when you access this website.

c) What are the purposes we use your data for?

A portion of the information is generated to guarantee the error free provision of the website. Other data may be used to analyze your user patterns. If contracts can be concluded or initiated via the website, the transmitted data will also be processed for contract offers, orders or other order enquiries.

d) What rights do you have as far as your information is concerned?

You have the right to receive information about the source, recipients, and purposes of your archived personal data at any time without having to pay a fee for such disclosures. You also have the right to demand that your data are rectified or eradicated. If you have consented to data processing, you have the option to revoke this consent at any time, which shall affect all future data processing. Moreover, you have the right to demand that the processing of your data be restricted under certain circumstances. Furthermore, you have the right to log a complaint with the competent supervising agency.

Please do not hesitate to contact us at any time if you have questions about this or any other data protection related issues.

e) Analysis tools and tools provided by third parties

There is a possibility that your browsing patterns will be statistically analyzed when your visit this website. Such analyses are performed primarily with what we refer to as analysis programs.



§ 2 Hosting

We are hosting the content of our website at the following provider: Strato AG, Otto-Ostrowski-Straße 7, 10249 Berlin (hereinafter referred to as "Strato"). When you visit our website, Strato records various logfiles, including your IP addresses. For more information, please consult the Strato Data Privacy Policy: <https://www.strato.de/datenschutz/>.

Strato is used on the basis of Art. 6(1)(f) GDPR. We have a legitimate interest in a depiction of our website that is as reliable as possible. If appropriate consent has been obtained, the processing is carried out exclusively on the basis of Art. 6(1)(a) GDPR and § 25 (1) TDDDG, insofar the consent includes the storage of cookies or the access to information in the user's end device (e.g., device fingerprinting) within the meaning of the TDDDG. This consent can be revoked at any time.

§ 3 General information and mandatory information

3.1. Data protection

The operators of this website and its pages take the protection of your personal data very seriously. Hence, we handle your personal data as confidential information and in compliance with the statutory data protection regulations and this Data Protection Declaration.

Whenever you use this website, a variety of personal information will be collected. Personal data comprises data that can be used to personally identify you. This Data Protection Declaration explains which data we collect as well as the purposes we use this data for. It also explains how, and for which purpose the information is collected.

We herewith advise you that the transmission of data via the Internet (i.e., through e-mail communications) may be prone to security gaps. It is not possible to completely protect data against third-party access.

3.2. Information about the responsible party (referred to as the "controller" in the GDPR)

The data processing controller on this website is:

SIGN8 GmbH
Fürstenrieder Str. 5
80687 München
Phone: 089 21537472000
E-Mail: customerservice@sign8.eu

3.3. Storage duration

Unless a more specific storage period has been specified in this privacy policy, your personal data will remain with us until the purpose for which it was collected no longer applies. If you assert a justified request for deletion or revoke your consent to data processing, your data will be deleted, unless we have other legally permissible reasons for storing your personal data (e.g., tax or commercial law retention periods); in the latter case, the deletion will take place after these reasons cease to apply.



3.4. General information on the legal basis for the data processing on this website

If you have consented to data processing, we process your personal data on the basis of Art. 6(1)(a) GDPR or Art. 9 (2)(a) GDPR, if special categories of data are processed according to Art. 9 (1) DSGVO. In the case of explicit consent to the transfer of personal data to third countries, the data processing is also based on Art. 49 (1)(a) GDPR. If you have consented to the storage of cookies or to the access to information in your end device (e.g., via device fingerprinting), the data processing is additionally based on § 25 (1) TDDDG. The consent can be revoked at any time. If your data is required for the fulfillment of a contract or for the implementation of pre-contractual measures, we process your data on the basis of Art. 6(1)(b) GDPR. Furthermore, if your data is required for the fulfillment of a legal obligation, we process it on the basis of Art. 6(1)(c) GDPR. Furthermore, the data processing may be carried out on the basis of our legitimate interest according to Art. 6(1)(f) GDPR. Information on the relevant legal basis in each individual case is provided in the following paragraphs of this privacy policy.

3.5. Designation of a data protection officer

We have appointed a data protection officer.

Mprotect365 GmbH
Nordstraße 17-21
04105 Leipzig
Phone: 089 21537472000
E-Mail: datenschutz@sign8.eu

3.6. Information on the data transfer to third-party countries that are not secure under data protection law and the transfer to US companies that are not DPF-certified

We use, among other technologies, tools from companies located in third-party countries that are not safe under data protection law, as well as US tools whose providers are not certified under the EU-US Data Privacy Framework (DPF). If these tools are enabled, your personal data may be transferred to and processed in these countries. We would like you to note that no level of data protection comparable to that in the EU can be guaranteed in third countries that are insecure in terms of data protection law.

We would like to point out that the US, as a secure third-party country, generally has a level of data protection comparable to that of the EU. Data transfer to the US is therefore permitted if the recipient is certified under the "EU-US Data Privacy Framework" (DPF) or has appropriate additional assurances. Information on transfers to third-party countries, including the data recipients, can be found in this Privacy Policy.

3.7. Recipients of personal data

In the scope of our business activities, we cooperate with various external parties. In some cases, this also requires the transfer of personal data to these external parties. We only disclose personal data to external parties if this is required as part of the fulfillment of a contract, if we are legally obligated to do so (e.g., disclosure of data to tax authorities), if we have a legitimate interest in the disclosure pursuant to Art. 6 (1)(f) GDPR, or if another legal basis permits the disclosure of this data. When using processors, we only disclose personal data of our customers on the basis of a valid contract on data processing. In the case of joint processing, a joint processing agreement is concluded.



3.8. Revocation of your consent to the processing of data

A wide range of data processing transactions are possible only subject to your express consent. You can also revoke at any time any consent you have already given us. This shall be without prejudice to the lawfulness of any data collection that occurred prior to your revocation.

3.9. Right to object to the collection of data in special cases; right to object to direct advertising (Art. 21 GDPR)

In the event that data are processed on the basis of Art. 6(1)(e) or (f) GDPR, you have the right to at any time object to the processing of your personal data based on grounds arising from your unique situation. This also applies to any profiling based on these provisions. To determine the legal basis on which any processing of data is based, please consult this data protection declaration. If you log an objection, we will no longer process your affected personal data, unless we are in a position to present compelling protection-worthy grounds for the processing of your data that outweigh your interests, rights and freedoms, or if the purpose of the processing is the claiming, exercising or defence of legal entitlements (objection pursuant to Art. 21(1) GDPR).

If your personal data is being processed in order to engage in direct advertising, you have the right to object to the processing of your affected personal data for the purposes of such advertising at any time. This also applies to profiling to the extent that it is affiliated with such direct advertising. If you object, your personal data will subsequently no longer be used for direct advertising purposes (objection pursuant to Art. 21(2) GDPR).

3.10. Right to log a complaint with the competent supervisory agency

In the event of violations of the GDPR, data subjects are entitled to log a complaint with a supervisory agency, in particular in the member state where they usually maintain their domicile, place of work or at the place where the alleged violation occurred. The right to log a complaint is in effect regardless of any other administrative or court proceedings available as legal recourses.

3.11. Right to data portability

You have the right to have data that we process automatically on the basis of your consent or in fulfillment of a contract handed over to you or to a third party in a common, machine-readable format. If you should demand the direct transfer of the data to another controller, this will be done only if it is technically feasible.

3.12. Information about, rectification and eradication of data

Within the scope of the applicable statutory provisions, you have the right to demand information about your archived personal data, their source and recipients as well as the purpose of the processing of your data at any time. You may also have a right to have your data rectified or eradicated. If you have questions about this subject matter or any other questions about personal data, please do not hesitate to contact us at any time.



3.13. Right to demand processing restrictions

You have the right to demand the imposition of restrictions as far as the processing of your personal data is concerned. To do so, you may contact us at any time. The right to demand restriction of processing applies in the following cases:

- In the event that you should dispute the correctness of your data archived by us, we will usually need some time to verify this claim. During the time that this investigation is ongoing, you have the right to demand that we restrict the processing of your personal data.
- If the processing of your personal data was/is conducted in an unlawful manner, you have the option to demand the restriction of the processing of your data instead of demanding the eradication of this data.
- If we do not need your personal data any longer and you need it to exercise, defend or claim legal entitlements, you have the right to demand the restriction of the processing of your personal data instead of its eradication.
- If you have raised an objection pursuant to Art. 21(1) GDPR, your rights and our rights will have to be weighed against each other. As long as it has not been determined whose interests prevail, you have the right to demand a restriction of the processing of your personal data.

If you have restricted the processing of your personal data, these data – with the exception of their archiving – may be processed only subject to your consent or to claim, exercise or defend legal entitlements or to protect the rights of other natural persons or legal entities or for important public interest reasons cited by the European Union or a member state of the EU.

3.14. SSL and/or TLS encryption

For security reasons and to protect the transmission of confidential content, such as purchase orders or inquiries you submit to us as the website operator, this website uses either an SSL or a TLS encryption program. You can recognize an encrypted connection by checking whether the address line of the browser switches from "http://" to "https://" and also by the appearance of the lock icon in the browser line.

If the SSL or TLS encryption is activated, data you transmit to us cannot be read by third parties.

3.15. Encrypted payment transactions on this website

If you are under an obligation to share your payment information (e.g. account number if you give us the authority to debit your bank account) with us after you have entered into a fee-based contract with us, this information is required to process payments.

Payment transactions using common modes of paying (Visa/MasterCard, debit to your bank account) are processed exclusively via encrypted SSL or TLS connections. You can recognize an encrypted connection by checking whether the address line of the browser switches from "http://" to "https://" and also by the appearance of the lock icon in the browser line.

If the communication with us is encrypted, third parties will not be able to read the payment information you share with us.



3.16. Rejection of unsolicited e-mails

We herewith object to the use of contact information published in conjunction with the mandatory information to be provided in our Site Notice to send us promotional and information material that we have not expressly requested. The operators of this website and its pages reserve the express right to take legal action in the event of the unsolicited sending of promotional information, for instance via SPAM messages.

§ 4 Recording of data on this website

4.1. Cookies

Our websites and pages use what the industry refers to as “cookies.” Cookies are small data packages that do not cause any damage to your device. They are either stored temporarily for the duration of a session (session cookies) or they are permanently archived on your device (permanent cookies). Session cookies are automatically deleted once you terminate your visit. Permanent cookies remain archived on your device until you actively delete them, or they are automatically eradicated by your web browser.

Cookies can be issued by us (first-party cookies) or by third-party companies (so-called third-party cookies). Third-party cookies enable the integration of certain services of third-party companies into websites (e.g., cookies for handling payment services).

Cookies have a variety of functions. Many cookies are technically essential since certain website functions would not work in the absence of these cookies (e.g., the shopping cart function or the display of videos). Other cookies may be used to analyze user behavior or for promotional purposes.

Cookies, which are required for the performance of electronic communication transactions, for the provision of certain functions you want to use (e.g., for the shopping cart function) or those that are necessary for the optimization (required cookies) of the website (e.g., cookies that provide measurable insights into the web audience), shall be stored on the basis of Art. 6(1)(f) GDPR, unless a different legal basis is cited. The operator of the website has a legitimate interest in the storage of required cookies to ensure the technically error-free and optimized provision of the operator’s services. If your consent to the storage of the cookies and similar recognition technologies has been requested, the processing occurs exclusively on the basis of the consent obtained (Art. 6(1)(a) GDPR and § 25 (1) TDDDG); this consent may be revoked at any time.

You have the option to set up your browser in such a manner that you will be notified any time cookies are placed and to permit the acceptance of cookies only in specific cases. You may also exclude the acceptance of cookies in certain cases or in general or activate the delete-function for the automatic eradication of cookies when the browser closes. If cookies are deactivated, the functions of this website may be limited.

Which cookies and services are used on this website can be found in this privacy policy.



4.2. Consent with Cookie Notice & Compliance

Our website uses the consent technology of Cookie Notice & Compliance for GDPR to obtain your consent for the archiving of certain cookies on your device or for the use of certain technologies and for the data protection compliant documentation of the former.

The provider of the tool is Hu-manity Rights Inc., 300 Carnegie Center, Suite 150, Princeton, NJ, New Jersey 08540, USA (hereinafter referred to as "Hu-manity Rights Inc."). When you gain access to our website, a connection with the servers of Hu-manity Rights Inc. is established to obtain your consent and other declarations related to the use of cookies. Subsequently, Hu-manity Rights Inc. stores a cookie in your browser to be able to allocate the granted consent and their revocation to you. The thus recorded data is stored until you ask us to delete it, delete the Hu-manity Rights consent cookie yourself or the purpose of data archiving is no longer valid. This does not affect mandatory statutory retention periods.

Cookie Notice & Compliance for GDPR is being used to obtain the consent for the use of cookies required by law. The legal basis is Art. 6(1)(c) GDPR.

4.3. Data processing

We have concluded a data processing agreement (DPA) for the use of the above-mentioned service. This is a contract mandated by data privacy laws that guarantees that they process personal data of our website visitors only based on our instructions and in compliance with the GDPR.

4.4. Contact form

If you submit inquiries to us via our contact form, the information provided in the contact form as well as any contact information provided therein will be stored by us in order to handle your inquiry and in the event that we have further questions. We will not share this information without your consent.

The processing of these data is based on Art. 6(1)(b) GDPR, if your request is related to the execution of a contract or if it is necessary to carry out pre-contractual measures. In all other cases the processing is based on our legitimate interest in the effective processing of the requests addressed to us (Art. 6(1)(f) GDPR) or on your agreement (Art. 6(1)(a) GDPR) if this has been requested; the consent can be revoked at any time.

The information you have entered into the contact form shall remain with us until you ask us to eradicate the data, revoke your consent to the archiving of data or if the purpose for which the information is being archived no longer exists (e.g., after we have concluded our response to your inquiry). This shall be without prejudice to any mandatory legal provisions, in particular retention periods.

4.5. Request by e-mail, telephone, or fax

If you contact us by e-mail, telephone or fax, your request, including all resulting personal data (name, request) will be stored and processed by us for the purpose of processing your request. We do not pass these data on without your consent.

These data are processed on the basis of Art. 6(1)(b) GDPR if your inquiry is related to the fulfillment of a contract or is required for the performance of pre-contractual measures. In all other cases, the data are processed on the basis of our legitimate interest in the effective handling of inquiries submitted to



us (Art. 6(1)(f) GDPR) or on the basis of your consent (Art. 6(1)(a) GDPR) if it has been obtained; the consent can be revoked at any time.

The data sent by you to us via contact requests remain with us until you request us to delete, revoke your consent to the storage or the purpose for the data storage lapses (e.g. after completion of your request). Mandatory statutory provisions - in particular statutory retention periods - remain unaffected.

4.6. Zoho SalesIQ

We use Zoho SalesIQ (hereinafter "Zoho SalesIQ") to process user inquiries via our support channels or via live chat systems. The provider is Zoho SalesIQ GmbH, Trinkausstraße 7, 40213 Düsseldorf, whose parent company is based in India.

Messages that you send to us are stored in the Zoho SalesIQ ticket system or answered by our employees in live chat. When you communicate with us via Zoho SalesIQ, we and Zoho SalesIQ store, among other things, your name and e-mail address, if you have provided them, and your chat history. The browser you use, your operating system, your IP address and your location are also recorded. This data is summarized in a profile.

The messages sent to us remain with us until you ask us to delete them or the purpose for data storage no longer applies (e.g. after your request has been processed). Mandatory statutory provisions - in particular statutory retention periods - remain unaffected.

Zoho SalesIQ is used on the basis of Art. 6 (1)(f) GDPR. We have a legitimate interest in processing your inquiries as quickly, reliably, and efficiently as possible. If a corresponding consent has been requested, the processing is carried out exclusively on the basis of Art. 6 (1)(a) GDPR and § 25 (1) TDDDG, insofar as the consent includes the storage of cookies or access to information in the user's terminal device (e.g. device fingerprinting) within the meaning of the TDDDG. Consent can be revoked at any time.

According to its own statement, Zoho SalesIQ stores the data of EU users exclusively on its servers in the European Union.

Further information can be found in Zoho SalesIQ's privacy policy: <https://www.zoho.com/salesiq/gdpr.html>.

4.7. Zoho CRM

We use Zoho CRM on this website. Provider is Zoho Corporation (see above).

Zoho CRM enables us, in particular, to manage existing and potential customers and customer contacts and to organize sales and communication processes. Using the CRM system also enables us to analyze and optimize our customer-related processes. The customer data is stored on Zoho CRM's servers. Details of Zoho CRM's functions can be found here: <https://www.zoho.com/de/crm/features.html>.

The use of Zoho CRM is based on Art. 6(1)(f) GDPR. The website operator has a legitimate interest the most efficient customer management and customer communication. If appropriate consent has been obtained, the processing is carried out exclusively on the basis of Art. 6(1)(a) GDPR and § 25 (1) TDDDG, insofar the consent includes the storage of cookies or the access to information in the user's end device (e.g., device fingerprinting) within the meaning of the TDDDG. This consent can be revoked at any time.



The data transfer to third countries outside the European Union is based on the standard contractual clauses of the EU Commission.

Details can be found in the Zoho CRM privacy policy: <https://www.zoho.com/privacy.html> and <https://www.zoho.com/gdpr.html>.

§ 5 Analysis tools and advertising

5.1. Google Ads

The website operator uses Google Ads. Google Ads is an online promotional program of Google Ireland Limited ("Google"), Gordon House, Barrow Street, Dublin 4, Ireland.

Google Ads enables us to display ads in the Google search engine or on third-party websites, if the user enters certain search terms into Google (keyword targeting). It is also possible to place targeted ads based on the user data Google has in its possession (e.g., location data and interests; target group targeting). As the website operator, we can analyze these data quantitatively, for instance by analyzing which search terms resulted in the display of our ads and how many ads led to respective clicks.

The use of these services occurs on the basis of your consent pursuant to Art. 6(1)(a) GDPR and § 25(1) TDDDG. You may revoke your consent at any time.

Data transmission to the US is based on the Standard Contractual Clauses (SCC) of the European Commission. Details can be found here: <https://policies.google.com/privacy/frameworks> and <https://business.safety.google/controllerterms/>.

The company is certified in accordance with the "EU-US Data Privacy Framework" (DPF). The DPF is an agreement between the European Union and the US, which is intended to ensure compliance with European data protection standards for data processing in the US. Every company certified under the DPF is obliged to comply with these data protection standards. For more information, please contact the provider under the following link: <https://www.dataprivacyframework.gov/participant/5780>.

5.2. Google Conversion-Tracking

This website uses Google Conversion Tracking. The provider of this service is Google Ireland Limited ("Google"), Gordon House, Barrow Street, Dublin 4, Ireland.

With the assistance of Google Conversion Tracking, we are in a position to recognize whether the user has completed certain actions. For instance, we can analyze the how frequently which buttons on our website have been clicked and which products are reviewed or purchased with particular frequency. The purpose of this information is to compile conversion statistics. We learn how many users have clicked on our ads and which actions they have completed. We do not receive any information that would allow us to personally identify the users. Google as such uses cookies or comparable recognition technologies for identification purposes.

The use of these services occurs on the basis of your consent pursuant to Art. 6(1)(a) GDPR and § 25(1) TDDDG. You may revoke your consent at any time.



For more information about Google Conversion Tracking, please review Google's data protection policy at: <https://policies.google.com/privacy?hl=en>

The company is certified in accordance with the "EU-US Data Privacy Framework" (DPF). The DPF is an agreement between the European Union and the US, which is intended to ensure compliance with European data protection standards for data processing in the US. Every company certified under the DPF is obliged to comply with these data protection standards. For more information, please contact the provider under the following link: <https://www.dataprivacyframework.gov/participant/5780>.

§ 6 Newsletter

6.1. Newsletter data

If you would like to receive the newsletter offered on the website, we require an e-mail address from you as well as information that allows us to verify that you are the owner of the e-mail address provided and that you agree to receive the newsletter. Further data is not collected or only on a voluntary basis. For the handling of the newsletter, we use newsletter service providers, which are described below.

6.2. Zoho Campaigns

This website uses Zoho Campaigns to send out newsletters. Provider is Zoho Corporation (see above).

Zoho Campaigns is a service that can be used, in particular, to organize and analyze the sending of newsletters. The information you enter to subscribe to the newsletter is stored on Zoho Campaigns' servers.

6.3. Data analysis by Zoho Campaigns

Zoho Campaigns allows us to analyze our newsletter campaigns. For example, we can see whether a newsletter message has been opened and which links have been clicked on, if any. In this way we can determine which links have been clicked on most often.

We can also see if certain previously defined actions were performed after opening/clicking (conversion rate). For example, we can see whether you have made a purchase after clicking on the newsletter. If you do not want to receive analyses of Zoho Campaigns, you must unsubscribe from the newsletter. We provide a link to this in every newsletter message. Zoho Campaigns also allows us to classify the recipients of the newsletter into different categories ("clustering"). The newsletter recipients can be classified, for example, by age, gender, or place of residence. In this way, the newsletter can be better adapted to the respective target groups. If you do not wish to receive analyses of Zoho Campaigns, you must unsubscribe from the newsletter. You will find a link to this in every newsletter message.

6.4. Data localization

Zoho Campaigns uses data localization. This means that customer data from the European Union is stored and processed exclusively in data centers within Europe. The data region is automatically assigned based on the domain selected during registration and the IP address. When logging in via campaigns.zoho.eu, the European data center is assigned by default. For more information about data



localization at Zoho and the data centers used, visit <https://www.zoho.com/know-your-datacenter.html> and <https://www.zoho.com/campaigns/help/developers/data-centers.html>.

Detailed information about the characteristics of Zoho Campaigns can be found at the following link: <https://www.zoho.com/campaigns/features.html>.

The Zoho Campaigns' privacy policy can be found at <https://www.zoho.com/privacy.html> and <https://www.zoho.com/gdpr.html>.

6.5. Legal basis

The data processing is based on your consent (Art. 6(1)(a) GDPR). You can revoke this consent at any time with effect for the future.

The data transfer to the USA is based on the standard contractual clauses of the EU Commission. Details can be found here: <https://www.zoho.com/privacy.html>.

6.6. Duration of storage

The data that you provide us with for the purpose of subscribing to the newsletter will be stored by us or the newsletter service provider until you unsubscribe from the newsletter and will be deleted from the newsletter distribution list or deleted after the newsletter has been cancelled. We reserve the right to delete email addresses within the scope of our legitimate interest under Art. 6(1)(f) GDPR. Data stored by us for other purposes remain unaffected.

After you have been removed from the newsletter distribution list, your email address may be stored by us or the newsletter service provider in a blacklist, if such action is necessary to prevent future mailings. The data from the blacklist will only be used for this purpose and will not be merged with other data. This serves both your interest and our interest in compliance with legal requirements when sending out newsletters (legitimate interest in the sense of Art. 6(1)(f) GDPR). The storage in the blacklist is not limited in time. You can object to the storage if your interests outweigh our legitimate interest.

§ 7 Plug-ins and Tools

We use "Google reCAPTCHA" (hereinafter referred to as "reCAPTCHA") on this website. The provider is Google Ireland Limited ("Google"), Gordon House, Barrow Street, Dublin 4, Ireland.

The purpose of reCAPTCHA is to determine whether data entered on this website (e.g., information entered into a contact form) is being provided by a human user or by an automated program. To determine this, reCAPTCHA analyzes the behavior of the website visitors based on a variety of parameters. This analysis is triggered automatically as soon as the website visitor enters the site. For this analysis, reCAPTCHA evaluates a variety of data (e.g., IP address, time the website visitor spent on the site or cursor movements initiated by the user). The data tracked during such analyses are forwarded to Google.

reCAPTCHA analyses run entirely in the background. Website visitors are not alerted that an analysis is underway.



Data are stored and analyzed on the basis of Art. 6(1)(f) GDPR. The website operator has a legitimate interest in the protection of the operator's websites against abusive automated spying and against SPAM. If appropriate consent has been obtained, the processing is carried out exclusively on the basis of Art. 6(1)(a) GDPR and § 25 (1) TDDDg, insofar the consent includes the storage of cookies or the access to information in the user's end device (e.g., device fingerprinting) within the meaning of the TDDDg. This consent can be revoked at any time.

For more information about Google reCAPTCHA please refer to the Google Data Privacy Declaration and [Terms Of Use](https://policies.google.com/terms?hl=en) under the following links: <https://policies.google.com/privacy?hl=en> and <https://policies.google.com/terms?hl=en>.

The company is certified in accordance with the "EU-US Data Privacy Framework" (DPF). The DPF is an agreement between the European Union and the US, which is intended to ensure compliance with European data protection standards for data processing in the US. Every company certified under the DPF is obliged to comply with these data protection standards. For more information, please contact the provider under the following link: <https://www.dataprivacyframework.gov/participant/5780>.

§ 8 eCommerce and payment service providers

We collect, process, and use personal customer and contract data for the establishment, content arrangement and modification of our contractual relationships. Data with personal references to the use of this website (usage data) will be collected, processed, and used only if this is necessary to enable the user to use our services or required for billing purposes. The legal basis for these processes is Art. 6(1)(b) GDPR.

The collected customer data shall be deleted upon completion of the order or termination of the business relationship and upon expiration of any existing statutory archiving periods. This shall be without prejudice to any statutory archiving periods.

§ 9 Handling applicant data

We offer website visitors the opportunity to submit job applications to us (e.g., via e-mail, via postal services or by submitting the online job application form). Below, we will brief you on the scope, purpose and use of the personal data collected from you in conjunction with the application process. We assure you that the collection, processing, and use of your data will occur in compliance with the applicable data privacy rights and all other statutory provisions and that your data will always be treated as strictly confidential.

9.1. Scope and purpose of the collection of data

If you submit a job application to us, we will process any affiliated personal data (e.g., contact and communications data, application documents, notes taken during job interviews, etc.), if they are required to make a decision concerning the establishment or an employment relationship. The legal grounds for the aforementioned are § 26 BDSG according to German Law (Negotiation of an Employment Relationship), Art. 6(1)(b) GDPR (General Contract Negotiations) and – provided you have given us your consent – Art. 6(1)(a) GDPR. You may revoke any consent given at any time. Within our



company, your personal data will only be shared with individuals who are involved in the processing of your job application.

If your job application should result in your recruitment, the data you have submitted will be archived on the grounds of § 26 BDSG and Art. 6(1)(b) GDPR for the purpose of implementing the employment relationship in our data processing system.

9.2. Data Archiving Period

If we are unable to make you a job offer or you reject a job offer or withdraw your application, we reserve the right to retain the data you have submitted on the basis of our legitimate interests (Art. 6(1)(f) GDPR) for up to 6 months from the end of the application procedure (rejection or withdrawal of the application). Afterwards the data will be deleted, and the physical application documents will be destroyed. The storage serves in particular as evidence in the event of a legal dispute. If it is evident that the data will be required after the expiry of the 6-month period (e.g., due to an impending or pending legal dispute), deletion will only take place when the purpose for further storage no longer applies.

Longer storage may also take place if you have given your agreement (Article 6(1)(a) GDPR) or if statutory data retention requirements preclude the deletion.

§ 10 Data Processing in the Context of Our (Qualified) Trust Services

10.1. Purpose and Scope

This section explains the processing of personal data in connection with the use of SIGN8 GmbH's (qualified) trust services under Regulation (EU) No. 910/2014, as amended (the "eIDAS Regulation"), in particular with regard to advanced and qualified electronic signatures, qualified electronic seals, and qualified timestamping services. It complements the general privacy information provided in this Privacy Policy.

10.2. Categories of Data Subjects

- Individuals creating an advanced or qualified electronic signature, a qualified electronic seal, or a qualified timestamp
- Authorized representatives or users of organizations
- Contractual partners of SIGN8 (e.g., API customers, resellers)
- Individuals identified during registration for qualified trust services (e.g., via Videoident)
- Recipients of signed documents or timestamps (if verified)

10.3. Categories of Personal Data Processed

- Identity data: name, date of birth, identification documents (as required)
- Contact information: address, email, phone number (as required)
- Identification proofs: video or eID data, verification records (as required)



- Access data: user ID, tokens, OAuth information, API keys
- Signature and timestamp data: signature evidence, qualified certificates, audit trails (as required)

10.4. Purposes of Data Processing

SIGN8 GmbH processes personal data to verify the identity of users and to provide qualified certificates, electronic signatures, electronic seals, and qualified timestamps. Personal data are also processed to meet legal record-keeping obligations, such as logging signatures and timestamps. Furthermore, data processing supports the provision of customer support and contractual services, as well as the detection of misuse and system monitoring. Finally, processing serves the purpose of documentation and auditing under the German Trust Services Act (VDG) and the provision of additional services booked by the customer.

10.5. Legal Bases for Processing

- Article 6(1)(b) GDPR (performance of a contract)
- Article 6(1)(c) GDPR (legal obligations under eIDAS and VDG)
- Article 6(1)(f) GDPR (legitimate interests, e.g., security and fraud prevention)

10.6. Retention Periods

- Certificate, signature, and timestamp logs: at least 7 years, up to 30 years (depending on purpose, legal obligation, and security level)
- Identification data: generally 7 years after certificate expiry (in accordance with VDG and eIDAS)
- API usage data: 1–2 years
- Support and contractual data: according to commercial and tax retention requirements
- Data not subject to retention obligations are generally deleted within 30 days

10.7. Recipients and Processors

- Identification service providers (e.g., Videoident providers, eID services, SMS gateway API)
- Operators of qualified signature, seal, and timestamp infrastructure (e.g., QSCD/HSM services)
- Technical infrastructure partners (e.g., hosting, certificate management)
- Internal authorized personnel (e.g., support, compliance, IT)

An up-to-date list of processors and subcontractors is available upon request. Any transfer of personal data outside the EU is conducted in compliance with the GDPR (e.g., via Standard Contractual Clauses).



10.8. Security and Certification

SIGN8 GmbH complies with the requirements for qualified trust services under the eIDAS Regulation, the Trust Services Act (VDG), and applicable ETSI standards. Operations are conducted using certified security modules (e.g., QSCD/HSM) with strict access controls and comprehensive logging.

10.9. Notes on Automated Processing

The creation of qualified electronic signatures, seals, or timestamps may be partially automated, but only at the explicit request of the authorized user or an authorized interface (e.g., via API). Automated decision-making as defined in Article 22 GDPR does not take place.

10.10. Data Subject Rights

All data subject rights under Articles 15 to 22 GDPR (access, rectification, erasure, restriction, data portability, objection) apply as described in Section 3 of this Privacy Policy. Please note that certain data may not be deleted before the expiry of statutory retention periods under the eIDAS Regulation and VDG.

10.11. Transparency and Trust Services-Specific Notes

In the provision of (qualified) trust services under the eIDAS Regulation, SIGN8 GmbH processes personal data of end users and authorized users exclusively for the provision of qualified trust services, including qualified timestamping services. This includes the delivery of signature, seal, and timestamp services, compliance with regulatory obligations, auditing, and support. Processing is conducted solely on the basis of the GDPR and the eIDAS Regulation, respecting the rights of data subjects and using appropriate technical and organizational measures to secure personal data.

