



SIGN8 AG c/o SWISS COMPANY AG  
Bahnhofstrasse 21  
CH-6300 Zug

T: +41 (0)41 533 03 95  
info@sign8.ch  
www.sign8.ch

## 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 AG 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 data protection laws.

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 AG 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.....	6
§ 5	Analysis tools and advertising.....	8
§ 6	Newsletter.....	9
§ 7	Plug-ins and Tools.....	10
§ 8	eCommerce and payment service providers .....	11
§ 9	Handling applicant data .....	11
§ 10	Data processing in the context of our Certification Services .....	12

## **§ 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 certification services. The term "personal data" comprises all data that can be used to personally identify you. For detailed information about data protection under Swiss law, including the Federal Act on Data Protection (FADP / DSG 2023) ("DSG"), please consult the following Privacy Policy.

### **1.2. Data recording on this website**

#### **a) Who is the responsible party for data processing?**

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 in this Privacy Policy. In accordance with the FADP (DSG 2023), this party is responsible for determining the purposes and means of the processing of personal data.

#### **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 primarily comprises of 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 given consent 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 lodge a complaint with the Federal Data Protection and Information Commissioner (FDPIC) in Switzerland.

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 you visit this website. Such analyses are performed primarily with what we refer to as analysis programs. These tools are used either based on your consent or, where strictly necessary for website functionality, on legitimate interest in accordance with FADP (DSG 2023).

**§ 2 Hosting**

We host 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. Strato acts as a data processor under our instructions in accordance with Art. 8 FADP (DSG 2023). Data processing at Strato occurs based on our legitimate interest in reliable website operation. Where applicable, processing is based on your consent for storage of cookies or access to information on your device (e.g., device fingerprinting), which may be revoked at any time.

For more information, please consult the Strato Data Privacy Policy: <https://www.strato.de/datenschutz/>.

**§ 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 seriously. Hence, we handle your personal data as confidential information and in compliance with the statutory data protection regulations and this Privacy Policy.

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 Privacy Policy 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**

The responsible party for data processing, incl. its means and purposes, on this website is:

SIGN8 AG c/o SWISS COMPANY AG  
Bahnhofstrasse 21  
6300 Zug  
Telephone: +41 (0)41 533 03 95  
E-Mail: [info@sign8.ch](mailto:info@sign8.ch)  
Website: [www.sign8.ch](http://www.sign8.ch)

### **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 such cases, the deletion will take place after these reasons cease to apply.

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

The processing of personal data is lawful if it complies with the general data protection principles as set out in Art. 6 FADP (DSG 2023).

If you have given your consent to the processing of your personal data, such processing is carried out on the basis of Art. 6 para. 6 FADP (DSG 2023). Where particularly sensitive personal data within the meaning of Art. 5 lit. c FADP (DSG 2023) are processed, your explicit consent is required in accordance with Art. 6 para. 7 lit. a FADP (DSG 2023). Consent may be revoked at any time with effect for the future.

If the processing of your personal data is necessary for the performance of a contract to which you are a party or for the implementation of pre-contractual measures, the processing is carried out in accordance with Art. 6 para. 1 and para. 2 FADP (DSG 2023), provided that the processing is proportionate and limited to what is necessary for the intended purpose.

Where the processing of personal data is required to comply with a legal obligation under Swiss law, such processing is lawful pursuant to Art. 6 para. 1 FADP (DSG 2023).

In addition, personal data may be processed where this is necessary to safeguard the overriding private interests of the controller or of third parties, provided that such processing complies with the principles of lawfulness, proportionality, purpose limitation and data security as set out in Art. 6 FADP (DSG 2023).

If you have consented to the use of cookies or similar technologies and to the access to information on your end device, such processing is based on your consent in conjunction with the applicable provisions of Swiss telecommunications law.

Where personal data is transferred to recipients in third countries that do not ensure an adequate level of data protection, such transfer is carried out in accordance with Art. 16 et seq. FADP (DSG 2023), in particular on the basis of appropriate safeguards or your explicit consent pursuant to Art. 17 para. 1 lit. a FADP (DSG 2023), where applicable.

Information on the specific legal basis applicable to each individual processing operation is provided in the relevant sections of this Privacy Policy.

### **3.5. Designation of a data protection officer**

We have appointed the following data protection officer:

[XXX]

### **3.6. Recipients of personal data**

We disclose personal data only when required to fulfill a contract, to comply with legal obligations, or based on our legitimate interest under Swiss law, or where another legal basis permits such disclosure. Data processors are engaged based on contractual obligations to process personal data only according

to our instructions and in compliance with Swiss law. Joint processing agreements are used where applicable.

### **3.7. Revocation of your consent to data processing**

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.

### **3.8. Right to object to data processing**

You may request the restriction of processing of your personal data if you contest the accuracy of your data, if the processing is unlawful, or if the data are no longer needed by us but are required by you to assert, exercise, or defend legal claims. We will comply with such requests to the extent required by law and will consider your interests and our legal obligations.

For purposes of direct marketing, you may request that your personal data no longer be used for such advertising as we honor your preference to opt out of promotional communications.

### **3.9. Right to log a complaint with the competent supervisory agency**

Under Art. 36 FADP (DSG 2023), you may lodge a complaint with the Federal Data Protection and Information Commissioner if you believe your data protection rights have been violated. This right exists irrespective of any other administrative or court proceedings.

### **3.10. Right to data portability**

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

### **3.11. 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. We will comply with such requests subject to mandatory retention obligations and other legal requirements, including those under ZertES if applicable.

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.

### **3.12. Right to demand processing restrictions**

You may request that we restrict the processing of your personal data in accordance with Art. 25 DSG in the following cases:

- If you contest the accuracy of your personal data while we verify this.
- If the processing of your personal data is unlawful and you prefer restriction instead of deletion.
- If we no longer need your personal data but you require it to assert, exercise, or defend legal claims.

Restricted data may only be processed further with your consent, for the assertion or defense of legal claims, to protect the rights of others, or for overriding public interest reasons recognized under Swiss law.

### **3.13. 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.

### **3.14. 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.

### **3.15. 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 permanently on your device (permanent cookies). Session cookies are automatically deleted once you end your visit. Permanent cookies remain on your device until you actively delete them or until your browser automatically deletes them.

Cookies can be set 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 serve a variety of purposes. Many cookies are technically essential, since certain website functions would not work without them (e.g., shopping cart or video display). Other cookies may be used to analyze user behavior or for marketing purposes.

Cookies that are not strictly necessary for the operation of the website are stored only with your informed consent, in accordance with Art. 8 DSG. You may configure your browser to notify you whenever cookies are set and to accept cookies only in specific cases. You may also reject cookies entirely or delete them automatically when the browser closes. If cookies are deactivated, some 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 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 is being used to obtain the consent for the use of cookies required by law.

#### **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 applicable law.

#### **4.4. Request by contact form, e-mail, telephone, or fax**

If you contact us via our contact form, by e-mail, telephone or fax, your request, including all resulting personal data (e.g., name, request) will be stored and processed by us for the purpose of processing your request. We will not share this information without your consent.

The processing of these data is based on your consent or on the necessity to fulfill contractual or pre-contractual obligations; the consent can be revoked at any time.

Information submitted via the contact form remains with us until you request deletion, revoke consent, or the purpose of storage no longer exists. Mandatory statutory retention periods under Swiss law remain unaffected.

#### **4.5. 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 Corporation GmbH, Trinkausstraße 7, 40213 Düsseldorf (hereinafter "Zoho Corporation"), 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 because 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 the consent, insofar as the consent includes the storage of cookies or access to information in the user's terminal device (e.g. device fingerprinting). Consent can be revoked at any time.

Further information can be found in Zoho SalesIQ's Privacy Policy: <https://www.zoho.com/de/privacy.html>.

#### **4.6. 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 our legitimate interest to use the most efficient customer management and customer communication. If appropriate consent has been obtained, the processing is carried out exclusively on the basis of the consent, insofar the consent includes the storage of cookies or the access to information in the user's end device (e.g., device fingerprinting). This consent can be revoked at any time.

Details can be found in the Zoho CRM Privacy Policy: <https://www.zoho.com/privacy.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 and/or our legitimate interest under Art. 6(1)(a) and/or (f) DSG. You may revoke your consent at any time.

Details can be found here: <https://policies.google.com/privacy/frameworks> and <https://business.safety.google/controllerterms/>. Data transmission to the United States is conducted with appropriate contractual and technical safeguards to ensure an adequate level of protection in accordance with FADP (DSG 2023).

## 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 and/or our legitimate interest under Art. 6 para. 1 FADP (DSG 2023). 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>. Data transmission to the United States is conducted with appropriate contractual and technical safeguards to ensure an adequate level of protection in accordance with FADP (DSG 2023).

## § 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 Switzerland and the European Union is stored and processed exclusively in data centers with adequate data protection safeguards, in accordance with the FADP (DSG 2023) and applicable EU law where relevant. The data region is automatically assigned based on the domain selected during registration and the IP address. When logging in via [campaigns.zoho.eu](https://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 use of these services occurs on the basis of your consent and/or our legitimate interest under Art. 6 para. 1 FADP (DSG 2023). You can revoke your consent at any time with effect for the future.

Data transmission to the United States is conducted with appropriate contractual and technical safeguards to ensure an adequate level of protection in accordance with FADP (DSG 2023).

#### **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 DSG. 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. The storage in the blacklist is indefinite unless your objection under DSG outweighs 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.

The use of these services occurs on the basis of your consent and/or our legitimate interest under Art. 6 para. 1 FADP (DSG 2023). You can revoke your consent at any time with effect for the future.

Data transmission to the United States is conducted with appropriate contractual and technical safeguards to ensure an adequate level of protection in accordance with FADP (DSG 2023).

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

## **§ 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 use of these services occurs on the basis of your consent and/or our legitimate interest under Art. 6 para. 1 FADP (DSG 2023). You can revoke your consent at any time with effect for the future.

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 use of these services occurs on the basis of your consent and/or our legitimate interest under Art. 6 para. 1 FADP (DSG 2023). You can revoke your consent at any time with effect for the future. 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 in compliance with applicable employment law and commercial retention requirements 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 FADP (DSG 2023)) 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 consent (Art. 6 FADP (DSG 2023)) or if statutory data retention requirements preclude the deletion.

# **§ 10 Data processing in the context of our Certification Services**

## **10.1. Purpose and scope**

This section explains the processing of personal data in connection with the use of our certification services according to the Swiss Federal Act on Electronic Signatures (ZertES) ("Certification Services"). It complements the general privacy information provided in this Privacy Policy.

## **10.2. Categories of data subjects**

- Individuals creating a (qualified/regulated) electronic signature or seal
- Authorized representatives or users of organizations
- Contractual partners of SIGN8 (e.g., API customers, resellers)
- Individuals identified during registration for Certification Services (e.g., via Videoldent)
- Recipients of signed or sealed documents (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 e-ID data, verification records (as required)
- Access data: user ID, tokens, OAuth information, API keys
- Signature data: signature evidence, certificates, audit trails (as required)

#### **10.4. Purposes of data processing**

We process personal data to verify the identity of users and to provide certificates, electronic signatures and seals. Personal data are also processed to meet legal record-keeping obligations, such as logging signatures. 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 ZertES and the provision of additional services booked by the customer.

#### **10.5. Retention periods**

- Certificate/signature logs: at least 11 years, up to 30 years (depending on purpose, legal obligation, and security level)
- Identification data: generally 11 years after certificate expiry (in accordance with ZertES)
- 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

#### **10.6. Recipients and processors**

- Identification service providers (e.g., Videoldent providers, e-ID services, SMS gateway API)
- Operators of (qualified/regulated) signature and seal infrastructure (e.g., 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 applicable data protection laws.

#### **10.7. Security and certification**

We comply with the requirements for Certification Services under ZertES and applicable regulation. Operations are conducted using certified security modules (e.g., HSM) with strict access controls and comprehensive logging.

#### **10.8. Notes on automated processing**

The creation of (qualified/regulated) electronic signatures and seals may be partially automated, but only at the explicit request of the authorized user or an authorized interface (e.g., via API).

#### **10.9. Data subject rights**

All data subject rights under FADP (DSG 2023) apply as described in this Privacy Policy. Please note that certain data may not be deleted before the expiry of statutory retention periods.