

Privacy policy regarding the use of inSign software

Transparency is the basis of our self-image. Therefore, in accordance with the relevant legal requirements, in particular the EU General Data Protection Regulation (GDPR), we would like to inform you below about the processing of your personal data in connection with the use of the PrismaLife customer portal and your rights.

1. Who is responsible for data processing and who is the contact person?

PrismaLife AG is responsible for data processing.

Our contact details are:

PrismaLife AG
Industriering 40
9491 Ruggell
Liechtenstein
Phone: +423 220 01 00
Email address: info@prismalife.com

For data protection matters, please contact our data protection officer at the above postal address or by email: dataprotection@prismalife.com

2. How, for what purpose and on what legal basis is your data processed?

2.1 Access to the inSign software

As a user (e.g. employee of PrismaLife AG, insurance intermediary, policyholder, etc.), we may process personal data such as your email address and/or mobile phone number and, if applicable, your first and last name to grant you access to the inSign software

2.1.1 Obligation to provide data/consequences of not providing data

If you do not provide us with the data described in section 2.1, we cannot guarantee you access to the inSign software and thus to the electronic signing of a document.

2.1.2 Legal basis for processing

The legal basis for the processing of your personal data for the provision of your access data is Art. 6 (1) (b) GDPR (pre-contractual measure or contractual obligation).

2.1.3 Storage period

If the inSign software is not used, the documents, including the access data, will be deleted after 30 days.

2.2 Provision of an electronic signature

PrismaLife AG uses the inSign software to encrypt electronic signatures. The software records the biometric data of the electronic signature provided (writing speed, writing direction, writing pauses and, if applicable, pressure intensity) as an advanced electronic signature in accordance with eIDAS (Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions) and encrypts it using an asymmetric cryptographic method (known as the RSA cryptosystem). We store and use this data during our contractual relationship for the establishment, implementation or termination of this contractual relationship. In order to rule out manipulation, a notary has generated the public and private keys required for this asymmetric encryption method and subsequently taken the private key into custody. For verification purposes in the event of a dispute over the authenticity of your signature, we may request this notary to decrypt individual data records and release the decrypted data records for the purpose of asserting, exercising and defending legal claims.

On devices with touch-sensitive screens, e.g. tablets or convertibles, the signature can be provided directly on this device. On notebooks and PCs, the signature is captured either in the supplementary inSign app or in a signature web client (also supports Windows phones) for smartphones. Alternatively, the signature can also be provided on the smartphone via a browser (i.e. without an app).

2.2.1 Obligation to provide data/consequences of non-provision

If you do not give your consent to the processing of your biometric data, you will not be able to sign documents electronically.

2.2.2 Legal basis for processing

Before submitting an electronic signature in a document, you give your consent to the processing of your biometric data in the inSign software (Art. 6(1)(a) GDPR and Art. 9(2)(a) GDPR in conjunction with Art. 7 GDPR). The time, i.e. the date and time of the signature, is printed on the document and an inSign transaction ID is generated.

Your consent to the processing of your biometric data in connection with the provision of an electronic signature can be revoked at any time by contacting PrismaLife AG (Art. 7(3) GDPR). Please note the consequences of non-provision described in section 2.2.1.

Please note that the revocation of your consent only applies to the future. Processing that took place before the revocation is not affected.

Where necessary, we also process your data beyond the actual use to protect our legitimate interests or those of third parties in accordance with Art. 6 (1) (f) GDPR, unless your interests or fundamental rights and freedoms requiring the protection of personal data prevail.

These include, among others:

- Asserting legal claims and defending against legal disputes, ensuring the fulfilment of your claims;
- Ensuring the IT security and IT operations of the insurance company, performing stress tests, developing new products and systems and adapting existing ones, migrating data to ensure the viability and integrity of the systems and, in a broader sense, the integrity of the processed data;
- Measures for business management and further development of processes, services and products.

2.2.3 Storage period

We store your biometric data from your electronic signature for as long as it is necessary for the above-mentioned purposes. It may be stored for the period during which claims can be made against our company (statutory limitation period of three or up to thirty years).

Personal data relating to contracts and the services used are not stored in your browser. This does not apply to photos and documents that you may have temporarily stored on your computer or smartphone before submitting them, or to messages that you have downloaded to your device. You are responsible for deleting this data or determining how long it is stored.

2.3 Connection data and system security

When using the inSign software, your browser transmits data to our server (see above). With each of these transmissions, the following additional information ("connection data") is also transmitted to our server:

- Your IP address

This connection data is also stored as a log file by our servers as standard for the purposes of system security and error analysis.

2.3.1 Legal basis for the processing of connection data

Connection data is only transmitted if a technical connection is required for transmission within the scope of the respective functionalities of the inSign software. As a rule, the legal basis for the processing of your data is Art. 6 (1) (b) GDPR (pre-contractual measure or contractual obligation).

The storage of connection data via use for the technical connection is based on our legitimate interest in accordance with Art. 6 (1) (f) GDPR. Our legitimate interest is to ensure the stability and security of the system and to eliminate malfunctions.

2.3.2 Storage period and criteria for determining the storage period

Connection data processed in the inSign software is deleted after the expiry of the statutory retention periods.

3. Recording of page views

When you visit the inSign software website, the browser used on your device automatically sends information to the server of this website. This information is temporarily stored in a so-called log file.

The following information is collected without your intervention and stored until it is automatically deleted:

- IP address of the requesting computer

- > Date and time of access
- > Name and URL of the file accessed
- > Browser used and, if applicable, the operating system of your computer and the name of your access provider

We process the aforementioned data for the following purposes

- > Ensuring a smooth connection to the website
- > Ensuring convenient use of our website
- > Evaluating system security and stability
- > Other administrative purposes

The legal basis for data processing is Art. 6 (1) (f) GDPR. Our legitimate interest follows from the purposes listed above for data collection. Under no circumstances do we use the collected data for the purpose of drawing conclusions about your person. The access history is stored until the end of the process or for a maximum of 30 days.

4. Use of cookies on the website for the purpose of providing an electronic signature

Cookies are small text files that are stored locally in the visitor's internet browser and are used for recognition purposes via the user's IP address. PrismaLife AG currently uses such cookies. Further information can be found at: <https://www.prismalife.com/en/insigncookies/>

5. Data security

This site uses SSL encryption for security reasons and to protect the transmission of confidential content that you, as a user, send to us as the site operator. An encrypted connection can be recognised by the fact that the address line of the browser changes from "http://" to "https://" and by the lock symbol in the browser line.

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

6. Ihre Datenschutzrechte

Under the General Data Protection Regulation, you as the data subject have the right to information under Art. 15 GDPR, the right to rectification under Art. 16 GDPR, the right to erasure under Art. 17 GDPR, the right to restriction of processing under Art. 18 GDPR, and the right to data portability under Art. 20 GDPR. Furthermore, you have a right of withdrawal under Art. 7(3) GDPR and a right to object under Art. 21 GDPR. If you exercise your above-mentioned rights, we will check whether the legal requirements for this are met. In addition, you have the right to lodge a complaint with a data protection supervisory authority (Art. 77 GDPR).

The data protection supervisory authority responsible for us is:

Datenschutzstelle Liechtenstein
Kirchstrasse 8
Postfach 684
9490 Vaduz
Liechtenstein

You can exercise all your rights by sending an email to dataprotection@prismalife.com or by sending by post.

To ensure that our response can be addressed to you as the data subject, you must identify yourself or provide information that will help us identify you.

Information about your right to object under Article 21 of the General Data Protection Regulation (GDPR)

Right to object in individual cases

You have the right to object at any time, on grounds relating to your particular situation, to the processing of personal data concerning you which is carried out on the basis of Article 6(1)(f) GDPR (data processing based on a balancing of interests).

If you object, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms, or the processing serves to assert, exercise or defend legal claims.

The objection can be made informally and should be addressed to:

PrismaLife AG
Industriering 40
9491 Ruggell
Liechtenstein
E-mail address: info@prismalife.com

If you have any questions about this privacy policy, please contact PrismaLife AG using the contact details above.

Note:

This "Privacy policy regarding the use of inSign software" may be updated at a later date due to changes, e.g. in legal provisions.