ZealiD Privacy Policy

Date	Version	Comments	Signed
2018-04-24	1.0	GDPR compliance first draft	PH, RA
2018-05-21	2.0	Minimal viable compliance setup – documentation/procedures	PH, TZ, RA
2018-07-19	2.1	Policies combined from different documents into new word document	PH
2018-07-23	2.12	Selected additions to governance	TZ
2019-12-11	2.13	Name change update	PH
2021-04-26	2.14	Several updates	EM
2021-04-28	2.15	Several updates	EM
2022-06-16	2.16	General review and update	EM
2023-01-16	2.17	Updated data processing purposes	EM
2023-02-23	2.18	Update related to data processing for ID verification by Money Transfer Service	EM
2023-06-12	2.19	Updates on data processing terms in cases of certificates' revocations	EM

1. General

We are ZealiD AB, a company registered with Bolagsverket in Sweden with registration number 556972-4288, whose principal place of business is at Norrlandsgatan 10, 111 56 Stockholm.

ZealiD is also registered with Swedish Authority for Privacy Protection (*IMY),* no 556972-4288.

ZealiD AB and its trading brand name ZealiD are hereinafter referred to as ”ZealiD”/“we”/“us”/”our”. We provide the website at https://www.zealid.com (“the Website”), the ZealiD Mobile Application (“Mobile App”), downloadable via a smartphone from the Google Play Store and Apple App Store online stores, and the Services accessible via the Website at https://my.zealid.com/en (“the Platform”).

This Privacy Policy explains the reason for processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer (DPO) and the data protection supervisory body.

ZealiD respects your privacy. This Privacy Policy has been developed to inform you about the privacy practices followed by ZealiD in connection to our website, products and services.

This Privacy policy applies where you have a direct relationship with ZealiD - i.e. if you are one of our Customers, Users, Suppliers, Contractors, job applicants, existing or former employees, then ZealiD will be acting as Data Controller (makes decisions) in respect of the personal information that we process about you. This Privacy Policy does not apply to products or services offered by our partners or other third-party services or websites.

All the definitions used in this Privacy Policy are understood in the way it is described in the respective ZealiD Trust Service Practice Statement (TSPS) and ZealiD QeID Certificate Practice Statement (CPS) available at https://www.zealid.com/en/repository, as well as Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR).

1.1. Data Controller

The data controller for personal data collected by ZealiD is ZealiD AB, having its registered office at Norrlandsgatan 10, 111 56 Stockholm, Sweden (headquarters).

1.2. Document owner

Document owner and contact person is the ZealiD AB Data Protection Officer (DPO): Enrika Masalskiene, dpo@zealid.com.

1.3. Data protection

The DPO leads data protection activities at ZealiD and works closely with the Compliance, IT Security and Management Board.

2. Collection of Personal Data

We collect information from you when you interact with ZealiD irrespectively of the channel and manner of the interaction for the specified purposes and lawful basis for processing:

Data Subject categories	**Purpose for data processing**	**Personal data being processed**	**Lawful basis for processing**	**Retention period**
Users of ZealiD Mobile App	Obtain contact data	Mobile phone number, e-mail address, type of mobile device, language preference, interactions (if any) with ZealiD Customer Care Team	Consent & necessity for compliance with a legal obligation	1 year from the registration or until the User deletes Mobile App
Users applying for the qualified certificates and electronic signatures	Identify and verify Subscriber's identity	First name, last name, date of birth, gender, nationality, address, including city and country (when available), personal number (or other serial number), email, mobile phone number; Facemap generated after liveness check; identity document information (type, country, number, issuing authority, date of issue, expiration date); pictures of ID documents; NFC signature, personal photo extracted from NFC Chip	Consent & necessity for compliance with a legal obligation	30 days from the day application date (if the application is unsuccessful)
Subscribers to whom the qualified certificates and electronic signatures are being issued	Ensure compliance for the evidence package	First name, last name, date of birth, gender, nationality, address, including city and country (when available), personal number (or other serial number), email, mobile phone number; Facemap generated after liveness check; identity document information (type, country, number, issuing authority, date of issue, expiration date); pictures of ID documents; NFC signature, personal photo extracted from NFC Chip; certificate number	Consent & necessity for compliance with a legal obligation	12 years; this period begins when the certificate expires
ZealiD Subscribers using ID verification by Money Transfer Service	Verify Subscriber's identity	First name, last name, transaction status, money transfer related data (account number, transaction amount, transaction date), relationship to the specific Customer	Consent	Money transfer related data - 30 days from the transaction date Subscriber relationship to

Data Subject categories	**Purpose for data processing**	**Personal data being processed**	**Lawful basis for processing**	**Retention period**
				the Customer data - 2 years from the transaction date
Natural persons interacting with ZealiD customer service	Ensure contractual obligations	Information provided during a phone call or via email or chat	Consent & legitimate interest	1 year from the contact with the customer service date
Natural persons to whom issued certificates where revoked	Ensure contractual obligations	First name, last name, date of birth, phone number, address, reason for revocation, connection ID (*optional*)	Consent & necessity for compliance with a legal obligation	14 years; this period begins when the certificate is being revoked
Natural persons on whom we receive data when providing services to our Customers or Subscribers*	Ensure contractual obligations	Information available in the document uploaded for signing	Necessity for performance of a contract	ZealiD acts as data processor and does not define retention period on its own*
Natural persons representing our Subcontractors	Ensure contractual obligations	Name, surname, position, phone number and email address, other information required for performance of a contract	Necessity for performance of a contract	In accordance with the relevant regulatory requirements
Complainants/ requesters	Investigate and take required action in line with our duties	Information provided by the complainant/requester; information included into our response to the complaint/request; date of the complaint/request submission and our response	Consent & necessity for compliance with a legal obligation	5 years from the complaint and request submission date (14 years - if complaint results in the revocation of the certificate)
Whistleblowers	Investigate and take required action in line with our duties	Personal data (if any) provided by the whistleblower	Necessity for compliance with a legal obligation	5 years from the case closing date

Data Subject categories	**Purpose for data processing**	**Personal data being processed**	**Lawful basis for processing**	**Retention period**
Candidates (job applicants)	Select and manage personnel	Name, surname; personal identity number (or date of birth); copy of ID document; citizenship; telephone number and email address; description of life and activity (CV); details of education and qualifications; date of application; other personal data provided by the data subject	Consent & legitimate interest	1 year from the rejection date
Employees & trainees (former and existing)	Manage personnel, manage records, ensure safety and health of employees, ensure compliance with the labor, social insurance and other legal requirements	Name, surname; personal identity number (or date of birth); copy of ID document; social security number; citizenship; address; telephone number; work and/or personal email address; description of life and activity (CV); position; data on recruitment (dismissal); education and qualification; training; incapacity for work; pay, benefits; information on incentives and penalties; performance appraisal data; current account data; private interest declaration data; special categories of personal data related to incumbency.	Consent, necessity for compliance with a legal obligation, necessity for performance of a contract	In accordance with the relevant regulatory requirements
Employees (Registration officers)	Ensure security of our Service	Video surveillance data of data subjects	Necessity for compliance with a legal obligation	30 days
Subscribers to the ZealiD newsletter	Contacting the subscriber	Email address	Consent	Until the consent is revoked
Visitors of ZealiD website	Analytics, cookies, ensure functionality and security of our Services	IP address; type of browser in use; number of sessions per browser on each device; type of device and operating system; referrer information; time zone; user preferences; pages visited, approximate geolocation	Consent & legitimate interest	26 months
Users of ZealiD	Improve ZealiD Mobile	Log records (connection ID), date of birth, language preference, ID	Legitimate	26 months

Data Subject categories	Purpose for data processing	Personal data being processed	Lawful basis for processing	Retention period
Mobile App	App	document issuing country, Customer name, issues in registration flow and ongoing usage of the ZealiD Mobile App	interest	
Users using ZealiD QR code/ deep link	Analytics, cookies, ensure functionality and security of our Services	IP address; type of browser in use; number of sessions per browser on each device; type of device and operating system; device unique ID referrer information; time zone;	Consent & legitimate interest	26 months

* When our Customers use certain Services, we generally process and store limited personal information on their behalf as a data processor. For example, in the context of document signing, when a Customer uploads contracts or other documents for review or signature, we act as a data processor and process the documents on the Customer's behalf and in accordance with their instructions. In those instances, the Customer is the data controller and is responsible for most aspects of the processing of the personal information. If you have any questions or concerns about how personal information is processed in these cases, including how to exercise your rights as a data subject, you should contact the Customer (either individual or entity requesting your signature). If we receive any rights requests concerning instances where we act as data processor, we will forward your query on to the relevant Customer.

3. Special categories of data

ZealiD processes ID photos (and all data therein) and selfie videos systematically for the purposes of unique identification and authentication of a natural person. This falls into GDPR article 9 that prohibits all such processing unless an exemption is provided by law.

ZealiD bases its processing on two legal grounds under GDPR Article 9:

- Article 9 (2) (a): the data subject has given explicit consent
    - Article 4 (1): 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- ZealiD services are regulated and the requirements to process ID documents are defined by law (e.g., copy of ID document required, birth date, birth place).

You specifically consent to ZealiD processing and storing personal data that allow us to uniquely identify you as a natural person. Such personal data includes unique identifiers such as personal code, citizen service number, social security number, etc. For example,

Dutch BSN (“burgerservicenummer”), Swedish personal number (“personnummer”) and Lithuanian personal code (“asmens kodas”).

Before using the ZealiD service you specifically consent to ZealiD automated processing and automated decision making of your personal data, such as age (verification of you being over 18 years old), ID document data (verification of ZealiD supported documents, ID document issuing and validity dates), facial features (for the verification of liveness), NFC Signature validation (if present). During the liveness check the Subscriber’s camera view of the three-dimensional face changes, observing perspective distortion and proving it is 3D. Relevant automated decisions are taken on the basis of a fully automated process without any human intervention.

The terms of use and privacy policies are in addition to the consent and information published in ZealiD service flows and on the zealid.com website.

ZealiD has implemented security measures to secure high risk ID document data. The measures are described in the ZealiD CPS and TSPS available at https://www.zealid.com/en/repository. They are also resulting from the relevant Data Protection Impact Assessments (DPIAs). This includes and is not limited to minimizing access, enforcing 2FA authentication for all actors accessing system that contain Special Categories and encrypting all evidence packages.

4. Documentation and maintenance of consent

ZealiD processes are built with GDPR in mind. Without active participation and consent to data subject facing information - including links to privacy and terms, the service cannot be used. No access to data of a data subject will be granted unless a standardized process involving information and consent is completed in the ZealiD Mobile App. All consumers have consented to the service they are going through.

4.1. Provision of consent

Our products are GDPR by design therefore we demonstrate to the Customer that enrolment/registration cannot be done without consent.

For general usage of the ZealiD Mobile App, the User is in control of the data at all times. No sign-in or e-signature can be issued without active use of the PIN or biometric authentication at the phone. Upon request provided to the DPO, we can provide timing and more in-depth details of when you have enrolled.

4.2. Revocation of the consent

The nature of our verification service is that a consent to process data cannot always be withdrawn because the data used is required by law, for example where ZealiD issues a qualified electronic certificate and maintains the remote signature creation capabilities for the subscriber. However, the certificate can be revoked. Please refer to https://www.zealid.com/en/revocation.

4.3. Underage users

ZealiD policy restricts Users younger than 18. This is checked as part of our Service registration. It is stated in Terms and Conditions Subscribers ZealiD TRA Service that we don't accept underaged (below 18).

5. Visitors and users of our Website and Platform

5.1. Analytics

When you visit www.zealid.com we use third-party services, Google Analytics, Hubspot and Hotjar to collect standard internet log information and details of visitor behavior patterns. We do this to gain information such as the number of visitors to the various parts of the site. This information is only processed in a way that does not directly identify a person. We do not make, and do not allow providers to make, any attempt to find out the identities of those visiting our website. We use the information to report on visitor numbers, and to make improvements to our service.

This information is collected only if visitors opt in. The information collected is classed as personal data because providers assign a unique identifier to each visitor. We do not make, and do not allow providers to make, any attempt to find out the identities of those visiting our website.

We have measures to protect the information collected, which include: limiting the amount of data collected (including not collecting full IP addresses), setting a retention schedule, restricting access to our Google Analytics, Hubspot and Hotjar data, and regularly reviewing our use of analytics.

We keep analytics data for 26 months from a visitor's last visit.

5.2. Cookies

Cookies do lots of different jobs, such as letting you navigate between pages efficiently, storing your preferences, and generally improving your experience of our Services. Cookies make the interaction between you and our Platform faster and easier. We use cookies to distinguish you from other users of the Platform and our Services. This helps us to provide you with a good experience when you use the Platform and also allows us to improve the Platform and Services. Cookies and other things like local storage also help us authenticate you to deliver personalized content.

We use a cookies tool on our website to gain consent for the optional cookies we use. At that time, you may also want to remove any cookies, which have been placed on any device used to access the Website, Platform and/or Services. Your withdrawal of consent will not affect the lawfulness of any processing carried out by us prior to such withdrawal.

Cookies that are necessary for functionality, security and accessibility are set and are not deleted by the tool.

Please refer to your device's documentation to learn what controls you can use to remove or block cookies. Please remember that if you do this, it may affect your ability to use the

Platform and/or the Services. As you use your device, you will encounter third parties that make use of cookies and similar technologies. We take no responsibility for those third parties or what they may place on your device or in your browser.

5.3. Security and performance

We use a third-party web application firewall by Hubspot to help maintain the security and performance of our website. The service checks that traffic to the site is behaving as would be expected. The service will block traffic that is not using the site as expected. To provide this service, these tools actively monitor real-time traffic at the application layer with the ability to alert or deny malicious behavior based on behavior type and rate. The rules used to detect and block malicious traffic are aligned to the best practice guidelines documented by the Open Web Application Security Project (OWASP), specifically the OWASP Top 10 and similar recommendations.

We host our website in Hubspot and keep traffic information for 26 months.

6. Mobile App

The ZealiD Mobile App service is a qualified certificate and signature service. The characteristics of the service is to allow the User to register, authenticate and sign documents with a qualified electronic signature. All transactions need to be stored for evidence purposes as they constitute a mechanism for contractual obligations for ZealiD Customers and their consumers (natural persons and data subjects). Please refer to the latest Certificate Practice Statement (hereinafter - CPS) and Trust Service Practice Statements (hereinafter - TSPS), available at https://www.zealid.com/respository.

Certificates for trust services are issued for longer periods and as minimum for 2 years. A certificate can be deleted but the evidence package that corresponds to the signatures produced by the User needs to be saved for as long as the signature is valid. This will be a long period typically up to 12 years.

7. Sharing your data

We use data processors who are third parties who provide elements of services for us. We have contracts in place with our data processors (e.g., accountants). This means that they cannot do anything with your personal information unless we have instructed them to do it (such as process and share our employees personal data to the social insurance authorities or tax inspectorates for the purposes of social insurance tax administration or tax administration). They will hold data securely and retain it for the period we instruct.

In some circumstances we are legally obliged to share information. For example, under a court order or where we cooperate with European supervisory authorities in handling complaints or investigations. We might also share information with other regulatory bodies or authorities in order to further requirements established by legal acts. In any scenario, we'll satisfy ourselves that we have a lawful basis on which to share the information and document our decision making.

We will not share your information with any third parties for the purposes of direct marketing.

7.1. Links to other websites

Where we provide links to websites of other organizations, this privacy notice does not cover how such organization processes personal information. We encourage you to read the privacy notices on such websites.

8. Data protection

We use a combination of technical, administrative, organizational and physical safeguards to protect your personal data. Access to your personal data is restricted to those who are necessary for the delivery of the services. These safeguards are tested as part of our annual audits and accreditations. For further details please see the Repository section available on our website.

9. Your data protection rights

Under data protection laws, you have rights we need to make you aware of. The rights available to you depend on our reason for processing your information.

Your right of access: You have the right to ask us for copies of your personal information. This right always applies. There are some exemptions, which means you may not always receive all the information we process.

Your right to rectification: You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete. This right always applies.

Your right to erasure: You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing: You have the right to ask us to restrict the processing of your information in certain circumstances.

Your right to object to processing: You have the right to object to processing if we are able to process your information because the process forms part of our public tasks, or is in our legitimate interests.

Your right to data portability: We do not process personal data that may allow the data subject to exercise the right to data portability in accordance with Article 20 of Regulation (EU) 2016/679.

10. Your right to complain

Please email dpo@zealid.com to make a request under these provisions. In order to help us deal with such a request please provide details of the product/service that the request relates to, the relevant ZealiD office or contact person and any other details (such as Customer number etc). Please note that we will perform steps to verify your identity before providing any information.

You also have a right to lodge a complaint with the appropriate Data Protection Authority if you believe that we have not complied with our legal obligations.